PETROBRAS	TECHNICAL SPECIFICATION	N°:	I-ET-3010.2Q-5412-800-P4X-001
	CLIENT: MARLIM LESTE E SUL		SHEET: 1 of 16
	JOB: BASIC DESIGN – REVIT I		
	AREA: MARLIM LESTE E SUL		
	TITLE: **FLARE/SLOP VESSEL GAS RECOVERY SYSTEM - RELIEF SYSTEM**		ESUP
			INTERNAL

MICROSOFT WORD / V. 365 / I-ET-3010.2Q-5412-800-P4X-001_B.DOC

INDEX OF REVISION

REV.	DESCRIPTION AND/OR REVISED SHEETS
0	ORIGINAL
A	REVISED WHERE INDICATED
B	REVISED WHERE INDICATED DUE TO CONSISTENCY ANALYSIS

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E
DATE	APR/09/24	JUN/14/24	JUL/16/24			
EXECUTION	U44D	CTTD	U44D			
CHECK	CTTD	U44D	DVOP			
APPROVAL	U361	U361	U361			

SUMMARY

1 INTRODUCTION

1.1 Objective

1.1.1 This specification describes the minimum requirements for the automation, instrumentation and control of the Flare/Slop Vessel Gas Recovery System - Relief System, to be installed at the UNIT (FPSO).

1.1.2 This specification also describes:

I. Interface with each system to be connected to Flare and Slop Vessel Gas Recovery System Relief Panel (PN-5412001).
II. Integration aspects regarding each Package type.

1.2 Definitions

1.2.1 Refer to I-ET-3010.00-1200-940-P4X-002 - GENERAL TECHNICAL TERMS.

1.3 Abbreviations, Acronyms and Initialisms

AEPR	Automation & Electrical Panels Room
BPV	Buckling Pin Valve
CCR	Central Control Room (located in the Hull Accommodation)
CSS	Control and Safety System
DOU	Diário Oficial da União (Official Gazette of the Federal Government)
FAT	Factory Acceptance Test
HFT	Hardware Fault Tolerance
HMI	Human-Machine Interface
HP	High Pressure
IACS	International Association of Classification Societies
I/O	Input/Output
IP	Ingress Protection Ratings
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
LP	Low Pressure
MTTF	Mean Time to Failure
MTTFS	Mean Time to Failure Safe
PES	Programmable Electronic System
PCS	Process Control System
PFD	Probability of Failure on Demand
PLC	Programmable Logic Controller
PSD	Process Shutdown System
QOV	Quick Opening Valve
RRF	Risk Reduction Factor
SAT	Site Acceptance Test
SIF	Safety Integrity Function
SIL	Safety Integrity Level
SIT	Site Integration Test
SOS	Supervision and Operation System
SRS	Safety Requirements Specification
UAM	Unit Alarm Malfunction
UAS	Unit Alarm Shutdown
UI	Unified Interpretation—A resolution issued by IACS
UR	Unified Requirement—A resolution issued by IACS

2 REFERENCE DOCUMENTS, CODES AND STANDARDS

2.1 External References

2.1.1 International Codes, Recommended Practices and Standards

API - AMERICAN PETROLEUM INSTITUTE

API	RP 14C	ANALYSIS, DESIGN, INSTALLATION AND TESTING OF SAFETY SYSTEMS FOR OFFSHORE PRODUCTION FACILITIES
API	STD 521	PRESSURE-RELIEVING AND DEPRESSURING SYSTEMS

IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC	60331	TESTS FOR ELECTRIC CABLES UNDER FIRE CONDITIONS – ALL PARTS
IEC	61508	FUNCTIONAL SAFETY OF ELECTRICAL/ ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS – ALL PARTS
IEC	61511	FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR – ALL PARTS
IEC	61892-4	MOBILE AND FIXED OFFSHORE UNITS - ELECTRICAL INSTALLATIONS - PART 4: CABLES
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)

2.1.2 2.1.3 Classification Society

2.1.2.1 The detailed design shall be submitted to Classification Society for approval.

2.1.2.2 The Unified Requirements (URs) and Unified Interpretations (UIs) of IACS, applicable and in force in the Detail Enginnering Design Phase, shall be observed and their requirements implemented.

2.1.2.3 The design and installation shall be updated following requirements, comments of Classification Society as well as URs and UIs mentioned in item 2.1.2.2. Internal references.

2.1.3 All Regulatory Standards (Normas Regulamentadoras-NRs) in force, published in the Diário Oficial da União (DOU), shall be followed.

2.2 Internal References

2.2.1 Project Documents

I-DE-3010.2Q-5412-944-P4X-001	HIGH PRESSURE FLARE K.O. DRUM
I-DE-3010.2Q-5412-944-P4X-002	LOW PRESSURE FLARE K.O. DRUM
I-DE-3010.2Q-5412-944-P4X-003	HIGH/LOW PRESSURE FLARE
I-DE-3010.2Q-5412-944-P4X-004	FLARE/SLOP VESSEL GAS RECOVERY SYSTEM - TRAINS A/C

I-DE-3010.2Q-5412-944-P4X-005	FLARE/SLOP VESSEL GAS RECOVERY SYSTEM - VESSEL
I-DE-3010.2Q-5412-944-P4X-006	HIGH PRESSURE FLARE COLLECTING SYSTEM
I-DE-3010.2Q-5412-944-P4X-007	LOW PRESSURE FLARE COLLECTING SYSTEM
I-DE-3010.2Q-5336-944-P4X-001	SLOP VESSEL
I-ET-3010.00-1200-800-P4X-002	AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS
I-ET-3010.2Q-1200-800-P4X-014	AUTOMATION INTERFACE OF PACKAGED UNITS
I-ET-3010.00-1200-940-P4X-002	GENERAL TECHNICAL TERMS
I-ET-3010.00-5140-700-P4X-002	SPECIFICATION FOR ELECTRICAL MATERIAL FOR OFFSHORE UNITS
I-ET-3010.00-5140-700-P4X-009	GENERAL REQUIREMENTS FOR ELECTRICAL MATERIAL AND EQUIPMENT FOR OFFSHORE UNITS
I-ET-3010.00-5140-700-P4X-007	SPECIFICATION FOR GENERIC ELECTRICAL EQUIPMENT FOR OFFSHORE UNITS
I-ET-3010.00-5140-700-P4X-003	ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS
I-ET-3010.2Q-5412-320-P4X-101	FLARE/SLOP VESSEL GAS RECOVERY COMPRESSOR PACKAGE SPECIFICATION (UC-5412001)
I-RL-3010.2Q-1200-940-P4X-001	GENERAL SPECIFICATION FOR AVAILABLE UTILITIES
I-RL-3010.2Q-5412-983-P4X-001	LOPA STUDY REPORT FOR CLOSED FLARE SYSTEM

3 ENVIRONMENTAL AND OPERATION CONDITIONS

3.1 General

3.1.1 All equipment, panels and instrumentation devices shall be suitable for the environmental and operating conditions described in I-ET-3010.00-1200-800-P4X-002 – AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS.

4 TECHNICAL REQUIREMENTS

4.1 General

4.1.1 All equipment, panels and instrumentation devices shall fully comply with requirements of I-ET-3010.00-1200-800-P4X-002 – AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS.

4.2 SIL / LOPA Study

4.2.1 Taking into account the safety-related aspects of the Flare and Slop Vessel Gas Recovery System comprised of PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel, PN-TA-5412001-01 - Flare Ignition and Monitoring Panel and PN-UC-5412001-01 - Flare and Slop Vessel Gas Recovery Compression Unit Panel, and the technical need to properly integrate the FGRS, the detailed engineering design shall guarantee that the overall required risk reduction factor (RRF) determined by the Safety Analysis (I-RL-3010.2Q-5412-983-P4X-001 – LOPA STUDY REPORT FOR CLOSED FLARE SYSTEM) can be achieved.

4.2.2 Regarding the interlocking related to HP flare:

4.2.2.1 It shall be a high demand mode SIF SIL 2, with the existence of two mechanical independent protection layers (IPLs), that is, two buckling pin valves (BPVs) providing a RRF = 1000 as a whole. The logic of this SIF, herein after named as SIF_HP, is: PSHH-5412002-1/3 (2oo3) commanding the opening of both EV-5412004 and EV-5412017.

4.2.2.2 The MTTFS of SIF_HP shall be equal or greater than 100 years. For the set of EV-5412004 with EV-5412017 shall be underestood as one EV, i.e, since the EVs are installed in parallel, any EV spuriously opening shall used to determine the MTTFS.

4.2.2.3 The test interval of SIF_HP shall be equal to or greater than 12 months.

4.2.3 Regarding the interlocking related to LP flare:

4.2.3.1 It shall be a high demand mode SIF SIL 1, with the existence of two mechanical IPL, that is, two BPVs providing a RRF = 1000 as a whole. The logic of this SIF, herein after named as SIF_LP, is: PSHH-5412007-1/3 (2oo3) commanding the opening of EV-5412010.

4.2.3.2 The MTTFS of SIF_LP shall be equal or greater than 100 years.

4.2.3.3 The test interval of SIF_LP shall be equal to or greater than 12 months.

4.2.4 Regarding the interlocking related to Slop Vessel:

4.2.4.1 It shall be a high demand mode SIF SIL 1, taking into account the existence of two mechanical IPL, that is, two BPVs providing a RRF = 1000 as a whole. The logic of this SIF, herein after named as SIF_SV, is: PSHH-5336501-1/3 (2oo3) commanding the opening of EV-5336005.

4.2.4.2 The test interval of SIF_SV shall be equal to or greater than 12 months.

4.2.5 Regarding the interlocking for backflow detection in HP Flare:

4.2.5.1 It shall be a SIF SIL 2. The logic of this SIF, herein named as SIF_HP_BF, is: EV-5412004 not closed OR EV-5412017 not closed OR ASHH-5412013 commanding the closure of SDV-5412008 (NOT ZSL-5412004 OR NOT ZSL-5412017 OR ASHH-5412013 commanding the closure of SDV-5412008).

4.2.5.2 The a test interval of SIF_HP_BF shall be equal to or greater than 12 months.

4.2.6 Regarding the interlocking for backflow detection in LP Flare:

4.2.6.1 t shall be a SIF SIL 2. The logic of this SIF, herein named as SIF_LP_BF, is: EV-5412010 not closed OR ASHH-5412012 commanding the closure of SDV-5412009 (NOT ZSL-5412010 OR ASHH-5412012 commanding the closure of SDV-5412009).

4.2.6.2 The test interval of SIF_LP_BF shall be equal to or greater than 12 months.

4.2.7 Safety integrity data for all devices shall be informed.

4.2.8 The SIL evaluation/assessment/rating of the Flare and Slop Vessel Gas Recovery System shall include all fundamental components of the system as mentioned above. All documentation in order to certify that SIL requirements were achieved shall be presented.

4.2.9 Any component associated with Flare and Slop Vessel Gas Recovery System that could influence or prevent the system from performing its primary function, either in normal operation or malfunction, shall be included in the SIL evaluation/assessment.

4.2.10 Safety integrity data/Reliability data for each component is required to perform the SIL evaluation and determine the overall system rating.

4.3 Functional Description

4.3.1 The PN-5412001 (Flare and Slop Vessel Gas Recovery System Relief Panel) shall be responsible for the proper and safe operation of the quick-opening valves (QOVs) actuation, valves in charge of HP/LP Flare and Slop Vessel gas flow rate relieving. This system shall be interconnected to PN-TA-5412001-01 (Flare Ignition and Monitoring Panel) and PN-UC-5412001-01 (Flare and Slop Vessel Gas Recovery Unit Panel). It shall also be interconnected to Topsides PLCs.

4.3.2 The HP flare header shall operate in a pressure range defined by the following:

I. At normal pressure level the relieving of HP Flare gas is lined up to UC-5412001 (Flare/Slop Vessel Gas Recovery Compression Unit).

II. At high pressure level the HP QOVs are opened, lining up the relieving to HP Flare, and also the lineup to UC-5412001 (Flare/Slop Vessel Gas Recovery Compression Unit) is interrupted by closing the inlet SDV.

4.3.3 The LP flare header shall operate in a pressure range defined by the following:

I. At normal pressure level the relieving of LP Flare gas is lined up to UC-5412001 (Flare/Slop Vessel Gas Recovery Compression Unit).

II. At high pressure level the LP QOV is opened, lining up the relieving to LP Flare, and also lineup to UC-5412001 (Flare Gas Recovery Compression Unit)) is interrupted by closing the inlet SDV.

4.3.4 The Slop Vessel shall operate in pressure range defined by the following:

I. At normal pressure level the relieving of Slop vent is lined up to UC-5412001 (Flare/Slop Vessel Gas Recovery Compression Unit).

II. At high pressure level the Slop Vessel QOV is opened, lining up the relieving to the Slop Vent, and also the lineup to UC-5412001 Flare Gas Recovery Compression Unit) is interrupted by closing the inlet SDV.

4.3.5 All these 6 (six) pressure levels shall be selected for proper and safe running of the Flare gas system.

4.3.6 QOVs shall be installed in the flare main header downstream the HP and LP flare knock-out drums. For the Slop Vessel, QOV shall be installed in its vent line.

4.3.7 Each QOV shall have Buckling Pin Valves (BPVs) protection in a bypass line. If the main QOV from each header is bypassed and the bypass valve is aligned, the BPVs shall still remain aligned. The blockage (only for maintenance) shall be made by full bore ball valves, installed upstream and downstream of the QOVs. Refer to I-DE-3010.2Q-5412-944-P4X-001 - HIGH PRESSURE FLARE K.O. DRUM, I-DE-3010.2Q-5412-944-P4X-002 - LOW PRESSURE FLARE K.O. DRUM and I-DE-3010.2Q-5336-944-P4X-001 - SLOP VESSEL for further information.

4.3.8 The QOV valves shall move from close to fully open in less than 3 (three) seconds (to be confirmed during Detail Engineering Design Phase).

4.3.9 Three pressure transmitters in a 2oo3 configuration shall be connected to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel in distinct I/O cards in order to monitor the HP flare header. PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel sets the opening of the QOVs EV-5412004 and EV-5412017, also connected in distinct I/O cards, to the associated HP Flare, according to process conditions, and requests the start of flare ignition to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel.

4.3.10 Three pressure transmitters in a 2oo3 configuration, shall be connected to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel) in distinct I/O cards in order to monitor the HP flare header. PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel sets the opening of the QOV EV-5412010 to the LP Flare, according to process conditions, and requests the start of flare ignition to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel.

4.3.11 Three pressure transmitters in a 2oo3 configuration, shall be connected to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel in distinct I/O cards in order to monitor the Slop Vessel. PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel sets the opening of the QOV EV-5336005 to the Slop Vent, according to process conditions.

4.3.12 Flare Gas Recovery System – Relief System package classification shall be in accordance with I-ET-3010.2Q-1200-800-P4X-014 – AUTOMATION INTERFACE OF PACKAGED UNITS. Package requirements shall be according to I-ET-3010.00-1200-800-P4X-002 – AUTOMATION, CONTROL AND INSTRUMENTATION ON PACKAGE UNITS. All parameters' data shall be available for monitoring from HMI at CCR.

4.3.13 In addition to the signals requested by I-ET-3010.2Q-1200-800-P4X-014 – AUTOMATION INTERFACE OF PACKAGED UNITS, which describe the interface between CSS and the FGRS panels, the following electrical signals shall be provided for interconnection of control/safety panels among themselves, at least:

I. **Ignition System Loading** – hardwired signal with line monitoring from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel (solenoid valve from sparking pellets type ignition system, energize to open), in order to activate the indexing cylinder and to rotate the magazine one step for loading of ignition pellet prior to opening of launching valve.

II. **Ignition Pellet Launching** – hardwired signal with line monitoring from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel (solenoid valve from sparking pellets type ignition system, energize to open), in order to open the launching valve.

III. **Request Flare Ignition** – fail-safe hardwired signal from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel (digital input – DI) requesting permission to start electric ignition.

IV. **Start Continuous Electric Sparking Type Ignition** – fail-safe hardwired signal from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-TA-5412001-01 - Flare Ignition and Monitoring Panel (digital input – DI), in order to activate the continuous electric sparking type ignition system.

V. **Flare Ignition Status** – fail-safe hardwired signal from PN-TA-5412001-01 - Flare Ignition and Monitoring Panel (digital output - DO) to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital input - DI).

VI. **LP QOV opening** – fail-safe hardwired signal from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-UC-5412001-01 - Flare and Slop Vessel Gas Recovery Compression Unit Panel (digital input – DI), in order to notify the compressor that the LP QOV has already been requested to open. Required actions from compressor side are not defined in this specification, but if it is required, they shall be implemented.

VII. **HP QOVs opening** – fail-safe hardwired signal from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-UC-5412001-01 - Flare and Slop Vessel Gas Recovery Compression Unit Panel (digital input – DI), in order to notify the compressor that the HP QOV has already been requested to open. Required actions from compressor side are not defined in this specification, but if it is required, they shall be implemented.

VIII. **Slop Vessel QOV opening** – fail-safe hardwired signal from PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital output – DO) to PN-UC-5412001-01 - Flare and Slop Vessel Gas Recovery Compression Unit Panel (digital input – DI), in order to notify the compressor that the Slop Vessel QOV has already been requested to open. Required actions from compressor side are not defined in this specification, but if it is required, they shall be foreseen.

IX. **UC-5412001 Shutdown** – fail-safe hardwired signal from PN-UC-5412001-01 - Flare and Slop Vessel Gas Recovery Compression Unit Panel (digital output – DO) to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel (digital input – DI). This signal shall request LP/HP and Slop Vessel QOVs opening and flare ignition.

4.3.13.1 All signals described above shall be confirmed during Detailed Engineering phase.

4.3.14 Interposition relays shall be foreseen for all signals interconnecting FGRS panels among themselves, that includes all signals listed in section 4.3.13 and any other required during Detailed Engineering phase. Buyer shall be informed by Seller in which panel interposition relays are being installed.

4.3.15 The following instruments shall be connected to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel:

I. Pressure transmitters:

a. PIT-5412002-1, PIT-5412002-2 and PIT-5412002-3.
b. PIT-5412007-1, PIT-5412007-2 and PIT-5412007-3.
c. PIT-5336501-1, PIT-5336501-2 and PIT-5336501-3.

II. QOVs with their respective limit switches (ZSL and ZSH) and solenoid valves (EY):

a. EV-5412004 and EV-5412017 with 04 solenoid valves (each) connected in series, with the first on being the one closer to QOV actuator: 1st connected to CSS – PSD, 2nd and 3rd ones connected to PN-5412001; 4th connected to PN-UC-5412001-01.
b. EV-5412010 with 03 solenoid valves connected in series, with the first on being the one closer to QOV actuator: 1st one connected to CSS – PSD; 2nd one connected to PN-5412001; 3rd connected to PN-UC-5412001-01.
c. EV-5336005 with 03 solenoid valves connected in series, with the first on being the one closer to QOV actuator: 1st one connected to CSS – PSD; 2nd one connected to PN-5412001; 3rd connected to PN-UC-5412001-01.

III. BPVs with their respective limit switches (ZSL and ZSH):

a. PSE-5412003-1.
b. PSE-5412003-2.
c. PSE-5412018-1.
d. PSE-5412018-2.
e. PSE-5336003-1.
f. PSE-5336003-2.

IV. Oxygen Analyzers

a. AIT-5412012.
b. AIT-5412013.

4.3.16 All safety functions shall be implemented following the interconnections among the control/safety panels and the design documentation. All safety function to be implemented shall be approved by Buyer.

4.4 Minimum Safety Requirements

4.4.1 Safety Instrumented Functions (SIFs) shall comply with requirements of IEC-61508 and IEC-61511 and shall comply with Safety Instrumented Level (SIL) and Risk Reduction Factor (RRF) required by safety analysis.

4.4.2 Safety requirements, including mandatory SIL 2 certifications, shall apply to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel as indicated below:

I. Safety sensors (initiators).
II. Logic solver, including I/O cards, network, power supply and processors.
III. Application program.
IV. All final elements, e.g., QOV/actuator sets, with respective solenoid control cabinets, if applicable, valve(s)/actuators between LP Flare header and HP Flare header.
V. All appurtenances necessary to build the system.

4.4.3 The required SIL 2 High Demand and SIL 1 High Demand, stated in sections 4.2.2 and 4.2.3, shall have the achieved SIL of each SIF confirmed/updated during Detail Engineering Design Phase, according to safety analysis (Layer of Protection Analysis – LOPA). All documentation in order to certify that SIL required by safety analysis were achieved shall be issued. The Safety Requirements Specification (SRS) shall include all SIF's.

4.4.3.1 As stated in items 4.2.5 and 4.2.6, the MTTFS of aforementioned SIFs shall be calculated in Detail Engineering Design Phase to verify whether interlocking that closes SDV-5412008 and the interlocking that closes SDV-5412009 shall be treated and transformed into a SIF.

4.4.4 The PN-TA-5412001-01 - Flare Ignition and Monitoring Panel shall be activated in a proper time and in coordination with QOVs actuations. Ignition shall be assured even in the case of QOV back-up actuation (BPV).

4.4.5 Each QOV back-up (Buckling Pin Valve-BPV) shall be an independent layer of protection with high reliability and shall comply with PFD equal to 10^{-2}. For the two buckling pin valves installed, the value of 10^{-3} shall be the PFD of the BPV set (two buckling pin valves).

4.4.6 Flare and Slop Vessel Gas Recovery System shall be fail-safe. During operation, power supply failures shall be investigated to guarantee the personnel safety, environment protection, and safety of process operating conditions and equipment.

4.4.6.1 It shall be presented a detailed study containing all the relief scenarios for the flare system, e.g. from PSVs, BDVs and PVs, including the dynamics of the total system.

4.4.6.2 Process design calculations shall be undertaken by Detail Engineering Design Phase in order to define the Flare Gas Recovery System response times that are sufficiently short to prevent unacceptable process conditions. Flare Gas Recovery System response times shall be defined in that phase and shall be used for selection of the QOV valves.

4.4.6.3 An alternative to achieve the safety integrity level required for the whole system may be proposed, subjected to BUYER evaluation and approval during bidding process.

4.5 Logic Solver Main Requirements

4.5.1 An independent safety Programmable Electronics (safety PE) shall be supplied to guarantee SIL 2 reliability, also designed and installed in compliance with safety integrity level SIL 2 requirements. The safety PE will be part of PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel.

4.5.2 Logic Solver shall consist of:

I. Redundant CPUs (processors) with suitable hardware features for functional safety, a suitable operating system and embedded functions for failures control, communication boards, I/O boards, memory boards, power suppliers, racks etc.
II. Library with approved safety function blocks.
III. Suitable configuration tool for SIF parameters.
IV. Tool to confirm that the download application software is identical to the source application software.
V. Safety users' manual describing instructions on how to use the equipment in order to build safety applications that comply with IEC 61508.

4.5.3 The Logic Solver to be used shall have been designed and tested in compliance with safety integrity level SIL 2 requirements, in accordance with IEC 61508.

4.5.4 Redundant controllers shall be used in PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel to obtain both characteristics of high availability and high reliability (safety).

4.5.5 Safety PE SIL 2 certification is mandatory, and preference shall be given to equipment assessed by an independent organization that has been approved by Brazilian accreditation body (INMETRO - Brazilian National Institute of Metrology, Quality and Technology). Equipment certified by TÜV, exida or similar are also acceptable.

4.5.6 It shall be supplied all Safety PES hardware, application software (including all passwords), programming, configuration, cabinets, wiring, parts and materials for a fully functional system, whether or not specifically itemized in this specification. A fully functional system in this specification also includes a fully functional, programmed and configured Safety PE interface available for communication to CSS. The interface with CSS shall be kept to the minimum necessary for CSS safety actions execution.

4.5.7 The Safety PES shall be able to communicate with CSS, without impact on the Safety PE logics.

4.5.8 Safety PE shall include hardware and software diagnostic facilities. Logic voted inputs and/or redundant outputs may be used to achieve SIL 2 reliability. Safety PE for SIL 2 applications shall demonstrate a minimum safe failure fraction of 90%.

4.5.9 Only certified software and hardware versions shall be used. New versions or versions for bugs' correction, which are directly related to the system safety or availability, shall only be implemented after proper certification.

4.5.10 Each analog input channel shall have resources for detecting signal failure when exceeds the 4-20mA range. It shall be used distinct modules to connect the redundant initiators and the actuators.

4.5.11 The components of Safety PES shall be provided with built-in redundancy or fault tolerance so that a single card failure shall not cause a loss on Flare and Slop Vessel Gas Recovery System functionality.

4.5.12 Component parts of the Safety PES shall be arranged such that a loss of signal or power leads system to a safe state.

4.5.13 For development of application software the activities shall comprise:

I. Application software specification.
II. Cause & effect diagram.
III. Individual safety function specification.
IV. Descriptions.
V. Associated tag list.
VI. Logic specification.
VII. Timing requirements.
VIII. Safety response times.
IX. Logic delay times.
X. Safety thresholds and limits.
XI. Bypasses requirements.
XII. Alarms, logs and events treatment specification.

4.5.14 Application software uploading/downloading shall be verified and documented.

4.5.15 All bypasses, overrides and inhibits of a Flare and Slop Vessel Gas Recovery System shall be alarmed/notified to the operators in the CCR HMIs. All Flare Gas Recovery System override facilities shall be carefully developed with the following requirements:

I. The need for restricted access, e.g. password protection.
II. Facilities for automatic recording of any override/bypass.
III. Definition of an upper limit for allowed override time to ensure that no override is forgotten.

4.5.16 All safety functionalities referring to logic solver failures shall be part of the system. In case of fail detection, it shall be alarmed in CSS HMI.

4.5.17 Flare and Slop Vessel Gas Recovery System hardware and software shall be designed to operate independently from the initiating causes identified during the hazard analysis, to minimize common cause failures (CCF).

4.5.18 Flare and Slop Vessel Gas Recovery System devices shall have self-diagnosis features to detect on-line failures to improve their availability. Input signals line monitoring and partial stroke test routine shall be available.

4.5.19 The PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel shall be installed indoor, in air-conditioned area, at AEPR.

4.6 Safety Requirements Specification

4.6.1 During the Detail Engineering Design Phase, an SRS shall be generated. The SRS shall define the technical requirements needed to SIF implementation, to guarantee tolerance against spurious fails and SIL reliability required in safety analysis.

4.6.2 The SRS shall include the following information:

I. Process description and summary of the documented hazard scenarios generated from the hazard analysis process.
II. Descriptions of functions performed by the SIF.
III. SIL calculations for each SIF.
IV. Related process measurements with their normal operating ranges and applicable trips points.
V. Safe state of the process for each identified SIF.
VI. Response time requirements for each SIF to bring the process to safe state.
VII. Requirements for overrides, inhibits and manual shutdowns, including how they will be reset.
VIII. Considerations for process common cause failures such as corrosion, plugging, power supply etc.
IX. Special start-up requirements and Flare Gas Recovery System restart considerations.
X. Interfaces to CSS – PSD.
XI. Requirements for proof test interval.
XII. Required testing frequencies, PFD and spurious MTTF.

4.7 Instrumentation minimum requirements

4.7.1 Main characteristics of QOV: pneumatic actuator, fail open and equipped with 2 (two) limit switches (open and close). It shall open in a time not superior to 3 (three) seconds (to be confirmed during Detail Engineering Design Phase).

4.7.1.1 LP QOVs, HP QOVs and Slop Vessel QOVs shall open according to item 4.1.

4.7.2 In order to meet SIL requirements, it shall be demonstrated that each QOV (including solenoid valve and actuator) and each pressure transmitter is suitable for use in the safety instrumented functions in accordance with the requirements defined in IEC 61508 and IEC 61511, including Minimum Hardware Fault Tolerance of final elements. Technical data of manufacturer and safety certificate issued by a recognized entity, such as TÜV, exida or similar, regarding QOV's and pressure transmitter reliability, failure data, and similar shall be presented in order to proof the adequacy of the specified instrument for the safety application.

4.7.3 Buckling pin valves shall not be taken into account as a Hardware Fault Tolerance for the QOVs.

4.7.4 For HP Flare, which is part of a SIL-2 High Demand SIF, the required HFT is 1, which means that the whole SIF shall have redundancy. This means that, even if SIL-2 is achievable with only one QOV, there shall be foreseen 2 QOVs, each with at least two solenoids each, in order to achieve the required HFT.

4.7.5 Actuators shall be properly sized to operate the valve under the maximum specified operating conditions. Actuator configuration and selection shall be such that the actuator is suitable to be applied in the SIL loop as defined.

4.7.6 Safety transmitters (initiators) shall have failure diagnosis features and be dedicated to Flare and Slop Vessel Gas Recovery System duty only and, therefore, separated and independent from other field devices.

4.7.7 Regarding Slop Vessel Pressure Transmitters (PIT-5336501-1, PIT-5336501-2, PIT-5336501-3), they shall be connected to PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel for the QOVs opening logic.

4.7.7.1 A 2oo3 PSHHH voting signal shall be sent to CSS, as hardwired signal, for safety purposes. This logic shall not cause any impact in the Slop Vessel QOV opening logic.

4.7.8 Minimum requirements for design, manufacturing, installation and tests of the instrumentation cables shall be in accordance with Classification Society rules.

4.7.9 Instrumentation cables shall follow IEC 61892-4.

4.7.10 All cabling associated with the fire and gas system shall be suitably protected against mechanical damage/hazardous events and diverse routing shall be foreseen to minimize the possibility of loss of system capability due to cable damage arising from fire or other physical causes. All cables shall be fire resistant in accordance with IEC 60331.

4.8 Requirements for Electric Systems and Power Supply

4.8.1 The PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel shall convert and distribute the different power supplies inside the panel, including where necessary a stabilized power supply unit for cabinet internal distribution of the 24 Vdc. See I-ET-3010.00-5140-700-P4X-003 – ELECTRICAL REQUIREMENTS FOR PACKAGES FOR OFFSHORE UNITS.

4.8.1.1 Electrical material and equipment shall comply with I-ET-3010.00-5140-700-P4X-002 – SPECIFICATION FOR ELECTRICAL MATERIAL FOR OFFSHORE UNITS, I-ET-3010.00-5140-700-P4X-009 - GENERAL REQUIREMENTS FOR ELECTRICAL MATERIAL AND EQUIPMENT FOR OFFSHORE UNITS, I-ET-3010.00-5140-700-P4X-007 - SPECIFICATION FOR GENERIC ELECTRICAL EQUIPMENT FOR OFFSHORE UNITS.

5 MANUFACTURING, DELIVERY AND OPERATION

5.1 Tests

5.1.1 All the required tests associated to the package automation, control and instrumentation of the package as a whole shall be performed, including FATs and SATs. FAT, SAT and SIT shall follow IEC 62381, IEC 62337 and Classification Society rules.

5.1.2 Prior to execution, it shall be submitted for Buyer approval the planning and test procedures for each FAT (compressor, ignition system, Flare and Slop Vessel Gas Recovery System and the package as a whole) as well as for SAT.

5.1.3 Testing, performance validation, verification and commissioning activities shall demonstrate that the Safety Requirement Specification designed for the Flare and Slop Vessel Gas Recovery System has been reached. This test shall be witnessed by a recognized entity, such as TÜV, exida or similar. This entity shall issue a certificate attesting the requirements on Safety Requirement Specification and the required SIL.

5.1.4 Flare and Slop Vessel Gas Recovery System shall be fully tested in specific period of time (proof test interval) in order to detect and correct dangerous failures so as to maintain the required performance and the required PFD. This period of time shall be confirmed during Detailed Engineering Desing Phase in conjunction with Operational team, however, for SIF design purposes it shall not be less than one year.

5.1.5 A detailed maintenance/inspection plan to be executed during UNIT (FPSO) lifetime to keep the SIL reliability shall be presented.

5.1.6 There shall be documented test procedures to verify the whole Flare and Slop Vessel Gas Recovery System, including the initiators and final elements.

5.1.7 Any component of hardware or software that fails during a test shall be re-tested as necessary to demonstrate that the rectification has been successfully completed.

5.1.8 The devices shall have self-diagnosis features to detect on-line failures. Input signals line monitoring and partial stroke test routine shall be available.

5.2 Spare Parts

5.2.1 It shall be provided a suggested list with components subject to be supplied in spare parts. The components shall be selected during Detailing Engineering Design Phase.

5.3 Warranty

5.3.1 This supply shall guarantee for all Flare Gas Recovery System components, even for equipment or devices furnished by others, according to contractual documents and EXHIBITS.

5.3.2 This warranty shall cover both fabrication and installation problems, as well as any service included in the scope of supply.

5.3.3 This warranty shall guarantee the supply of spare parts of PN-5412001 - Flare and Slop Vessel Gas Recovery System Relief Panel, at least, for up to 10 (ten) years after the acceptance test date, and technical assistance at installation site performed by qualified and certified maintenance staff, when requested.

5.3.4 During guarantee period, any defective device shall be changed for a new one, within 1 (one) week, after the problem has been reported.

5.4 Packing Requirements

5.4.1 On completion of testing at factory all equipment shall be prepared for shipment and storage.

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