ADNOC GROUP PROJECTS AND ENGINEERING

EMERGENCY SHUTDOWN (SIS) SYSTEM SPECIFICATION

Specification

AGES-SP-04-004

ص ب 898، أبوظبي، الإمارات العربية المتحدة
PO Box 898, Abu Dhabi, UAE
adnoc.ae

شركة بترول أبوظبي الوطنية
Abu Dhabi National Oil Company

GROUP PROJECTS & ENGINEERING / PT&CS DIRECTORATE

CUSTODIAN	Group Projects & Engineering / PT&CS
ADNOC	Specification applicable to ADNOC & ADNOC Group Companies

Group Projects & Engineering is the owner of this Specification and responsible for its custody, maintenance and periodic update.

In addition, Group Projects & Engineering is responsible for communication and distribution of any changes to this Specification and its version control.

This specification will be reviewed and updated in case of any changes affecting the activities described in this document.

INTER-RELATIONSHIPS AND STAKEHOLDERS

a) The following are inter-relationships for implementation of this Specification:

   i. ADNOC Upstream and ADNOC Downstream Directorates and

   ii. ADNOC Onshore, ADNOC Offshore, ADNOC Sour Gas, ADNOG Gas Processing. ADNOC LNG, ADNOC Refining, ADNOC Fertilisers, Borouge, Al Dhafra Petroleum, Al Yasat

b) The following are stakeholders for the purpose of this Specification:

   ADNOC PT&CS Directorate.

c) This Specification has been approved by the ADNOC PT&CS is to be implemented by each ADNOC Group company included above subject to and in accordance with their Delegation of Authority and other governance-related processes in order to ensure compliance

d) Each ADNOC Group company must establish/nominate a Technical Authority responsible for compliance with this Specification.

DEFINED TERMS / ABBREVIATIONS / REFERENCES

"**ADNOC**" means Abu Dhabi National Oil Company.

"**ADNOC Group**" means ADNOC together with each company in which ADNOC, directly or indirectly, controls fifty percent (50%) or more of the share capital.

"**Approving Authority**" means the decision-making body or employee with the required authority to approve Policies & Procedures or any changes to it.

"**Business Line Directorates**" or "**BLD**" means a directorate of ADNOC which is responsible for one or more Group Companies reporting to, or operating within the same line of business as, such directorate.

"**Business Support Directorates and Functions**" or "**Non- BLD**" means all the ADNOC functions and the remaining directorates, which are not ADNOC Business Line Directorates.

"**CEO**" means chief executive officer.

"**Group Company**" means any company within the ADNOC Group other than ADNOC.

"Specification" means this Emergency Shutdown (SIS) System Specification

CONTROLLED INTRANET COPY

The intranet copy of this document located in the section under Group Policies on One ADNOC is the only controlled document. Copies or extracts of this document, which have been downloaded from the intranet, are uncontrolled copies and cannot be guaranteed to be the latest version.

TABLE OF CONTENTS

GENERAL

1 PURPOSE

The purpose of this specification is to define the minimum mandatory technical requirements for design, manufacturing, testing, packing, installation and commissioning of Emergency Shutdown System (ESD)/Safety Instrumented System (SIS).

2 SCOPE

2.1 The scope of this specification is limited to Programmable Electronic System (PES) type ESD/SIS.

This specification excludes solid state ESD System, field input devices (transmitters, switches etc), and output devices (shutdown valves, electrical switchgears etc).

2.2 For project specific additional requirements, refer to ESD system requirements stated in respective project's Purchase Requisition documentation.

3 DEFINED TERMS / ABBREVIATIONS / REFERENCES

Abbreviations	
AMS	Alarm Management System
BMS	Burner Management System
CCR	Central Control Room
CPU	Central Processor Unit
EMI	Electromagnetic Interference
EDP	Emergency Depressurisation System
ESD	Emergency Shutdown System
EWS	Engineering Workstation
FAT	Factory Acceptance Test
FDS	Functional Design Specification
HART	Highway Addressable Remote Transducer
HVAC	Heating, Ventilation and Air Conditioning
HIPPS	High Integrity Pressure Protection System
HMI	Human Machine Interface
HSSD	High Sensitivity Smoke Detection
HSSS	Hydraulic Safety Shutdown System
IAMS	Instrument Asset Management System
ICSS	Integrated Control and Safety System

Abbreviations	
IP	Ingress Protection
I/O	Inputs/Outputs
LAN	Local Area Network
LCD	Liquid Crystal Display
LCP	Local Control Panel
LED	Light Emitting Diode
MCB	Miniature Circuit Breaker
MOS	Maintenance Override Switch
MTTF	Mean Time To Failure
MTTR	Mean Time To Restore
OWS	Operator Workstation
PCN	Process Control Network
PCS	Process Control System
PES	Programmable Electronic System
PFD	Probability of Failure on Demand
PLC	Programme Logic Controller
PST	Partial Stroke Test
RAM	Random Access Memory
RFI	Radio Frequency Interference
SAT	Site Acceptance Test
SER	Sequence Events Recording
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SIT	Site Installation Test
SOE	Sequence Of Events
SNTP	Simple Network Time Protocol
TETRA	Terrestrial Trunked Radio
TCP/IP	Transmission Control Protocol / Internet Protocol
TUV	Technischer Uberwachungs Verein
UPS	Uninterruptible Power Supply

Technical Definitions	
Term	**Definition**
ESD and SIS System	It is an Electrical / Electronic / Programmable Electronic safety-related System that provides the safeguarding of the process and equipment to protect personnel, assets and environment. It comprises of sensors/transmitters, the final control elements, and the logic solver.
PFD	A value that indicates the probability that a device or system will fail to respond to a demand in a specified interval of time.
Reliability	The probability that when operating under stated environmental conditions, the system will perform continuously, as specified, over a specific time interval.
Fail Safe	The capability to go to a predetermined safe-state in the event of a specific malfunction.
Fault-Tolerant System	A system incorporating design features which enable the system to detect and log transient or steady-state fault conditions and take appropriate corrective action while remaining on-line and performing its specified function.
MTTF	'Mean Time To Failure' is the expected time to failure of a system in a population of identical systems.
MTTR	Mean Time To Restore' is the statistical average of time taken to identify and repair a fault (including diagnosis).
Response Time	Total maximum time required to read all field inputs, program execution and change field output state at I/O card channel level.
Safety Instrumented Function (SIF)	Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.
Safety integrity	Average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time.
Safety Integrity Level (SIL)	Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented Systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.
SIL Validation	Activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification.
SIL Verification	Activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.
Watchdog	Combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of PES device and taking action upon detection of an incorrect operation.

References
ADNOC Group Companies ESD/SIS documents part of ESD/SIS Purchase Order shall be referred for design and supply of equipment.

SECTION A

4 NORMATIVE REFERENCES

4.1 International Code(s) and Standards

The following codes and standards, to the extent specified herein, form a part of this specification. When an edition date is not indicated for a code or standard, the latest edition at the time of order placement shall apply:

Standard	Description
American Petroleum Institute	
API RP 521	Pressure-relieving and Depressuring Systems
American National Standards Institute / The International Society of Automation (ANSI/ISA)	
ANSI/ISA 5.1	Instrumentation Symbols and Identification
ISA 5.3	Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic and Computer Systems
ISA 5.4	Instrument Loop Diagram
ISA S5.5	Graphic Symbols for Process Displays
ISA 18.1	Annunciator Sequences and Specifications
ISA 18.2	Management of Alarm Systems for the Process Industries
ISA 71.01	Environmental Conditions for Process Management and Control System, Temperature and Humidity
ISA 71.04	Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
ANSI/ISA-TR99.00.01	Security Technologies for Industrial Automation and Control Systems
The Engineering Equipment and Materials Users Association (EEMUA)	
EEMUA PUB No 191	Engineering Equipment and Material User's Association Alarm Systems - A Guide to Design, Management and Procurement
The International Electrotechnical Commission (IEC)	
IEC 60079	Explosive Atmospheres – All parts

IEC 60297-3-101	Basic dimensions of front panels, sub-racks, chassis, racks and cabinets
IEC 60332	Tests for Electric and Optical Fibre Cables Under Fire Conditions – All parts
IEC 60364	Electrical installations of buildings - All parts
IEC 60529	Degrees of protection provided by enclosures (IP code)
IEC 60445	Basic and Safety Principles for Man-Machine Interface, Marking and Identification - Identification of Equipment Terminals, Conductor Terminations and Conductors
IEC 61000	Electromagnetic Compatibility (EMC) – All Parts
IEC 61131	Programmable controllers– All Parts
IEC 61508	Functional Safety of Electrical/electronic/Programmable Electronic (E/E/EP) Safety Related Systems- all parts
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector – all parts
IEC 61326-3-1	Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
IEC 62402	Obsolescence Management – Application guide
IEC 62443	Industrial communication networks - Network and system security - All parts
IEC 17799	Information technology - Security techniques - Code of practice for information security management
IEC 60947-5-6	Control circuit devices and switching elements - DC interface for proximity sensors and switching amplifiers (NAMUR)
Institute of Electrical and Electronics Engineers (IEEE)	
IEEE 802.3	Standard for Ethernet
International Organization for Standardization (ISO)	
ISO 9001	Quality Management Systems - Requirements.
ISO 9004	Managing for the Sustained Success of an Organization – A Quality Management Approach

ISO 19011	Guidelines for Auditing Management Systems
Military Handbook	
MIL HDBK 217F	Reliability Prediction of Electronic Equipment
NATIONAL FIRE PROTECTION ASSOCIATION (NFPA)	
NFPA 70	Standard for the safe installation of electrical wiring and equipment
NFPA 85	Boiler and Combustion Systems Hazards Code
NFPA 86	Standard for Ovens and Furnaces
NFPA 87	Standard for Fluid Heaters
European Standards (EN)	
EN 298	Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
EN 746 Part 1 & 2	Industrial Thermo-processing Equipment – Safety Requirements
EN 50156	Electrical equipment for furnaces and ancillary equipment
NAMUR (Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der Chemischen Industrie)	
NAMUR NE 43	Standardisation of the Signal Level for the Failure Information of Digital Transmitters

4.2 ADNOC Specifications

Document Number	Title
AGES-SP-04-001	Process Control System Specification
AGES-SP-04-003	Fire and Gas System Specification

5 REFERENCE DOCUMENTS

5.1 Standard Drawings

Not Applicable.

5.2 Other References

Not Applicable.

6 DOCUMENTS PRECEDENCE

The Codes and Standards referred to in this specification shall, unless stated otherwise, be the latest approved issue at the time of Purchase Order placement.

It shall be the VENDOR'S and CONTRACTORS'S responsibility to be, or to become, knowledgeable of the requirements of the referenced Codes and Standards.

The VENDOR/CONTRACTOR shall notify the COMPANY of any apparent conflict between this specification, the related data sheets, the Codes and Standards and any other specifications noted herein.

Resolution and/or interpretation precedence shall be obtained from the COMPANY in writing before proceeding with the design/manufacture.

In case of conflict, the order of document precedence shall be:

(1) UAE Statutory requirements

(2) ADNOC Codes of Practice

(3) Equipment datasheets and drawings

(4) Project Specifications and standard drawings

(5) Company Specifications

(6) National/International Standards

7 SPECIFICATION DEVIATION/CONCESSION CONTROL

Deviations from this specification are only acceptable where the VENDOR has listed in his quotation the requirements he cannot, or does not wish to comply with, and the COMPANY/CONTRACTOR has accepted in writing the deviations before the order is placed.

In the absence of a list of deviations, it will be assumed that the VENDOR complies fully with this specification.

Any technical deviations to the Purchase Order and its attachments including, but not limited to, the Data Sheets and Narrative Specifications shall be sought by the VENDOR only through Concession Request Format. Concession requests require CONTRACTOR'S and COMPANY'S review/approval, prior to the proposed technical changes being implemented. Technical changes implemented prior to COMPANY approval are subject to rejection.

8 PROCESS SAFETY REQUIREMENTS

Sr.No.	Description
1	ESD/SIS Logic Solver shall be highly reliable and certified for safety integrity level of SIL3 as per IEC 61508 and IEC 61511.
2	ESD/SIS Logic Solver hardware architecture shall be redundant and fault tolerant to provide availability of 99.99%.
3	ESD digital output fail-safe state shall be the 'de-energized' unless otherwise specified. ESD digital output shall go to a '0' (deenergized) state on shutdown conditions, power failure and on component failure.
4	CONTRACTOR shall carry a Functional Safety Assessment (FSA) as per IEC 61511-1 clause 5.2.6.1.5 prior to the hazards that the SIF are designed to prevent.
5	A detailed safety integrity assessment review to establish SIF integrity targets (SIL) shall be completed by CONTRACTOR during FEED and Detailed Design engineering phase.

9 DESIGN CONSIDERATIONS

9.1 Operation & Design Life

The ESD system shall be designed for minimum life duration 15 years.

9.2 Environmental Requirements

Other than field local panels (Remote I/O, Electronic JB etc), all ESD system cabinets will be installed in climate controlled unclassified indoor locations. Use of field mounted Electronic JB/Remote I/O are subject to COMPANY approval based on proven track and compliance with SIL requirements.

The indoor installed ESD system shall be suitable for an air-conditioned environment to ISA S71.04, G3 classification. Normal indoor operating conditions will be 22°C ± 2°C and 50% Relative Humidity. The System shall continue to operate in HVAC upset conditions during which in the indoor location of installation temperature can fall to 0ºC or rise to 60ºC, and the humidity can vary between 5% and 95% non-condensing.

9.3 Electric Utility Data

Two separate power feeders from dual redundant UPS and one feeder from Utility power supply shall be made available for use by the VENDOR for powering ESD system cabinets.

The Electrical power supply details are as follows:

(a) 240V AC, Single Phase, 50 Hz, earthed

(b) Steady state Voltage variation ± 10% nominal voltage

(c) Steady state Frequency variation ± 5 %

9.4 Seismic Requirements

The system shall be designed to operate in the presence of a sinusoidal vibration of 2g at 10 - 500 Hz and withstand a shock of 15g for 11 milliseconds.

9.5 Hazardous Area Protection

Unless otherwise specified, ESD system cabinets shall be installed within a general purpose, non-classified electrical area.

If equipment is located in hazardous area, the Hazardous area classification and method of protection shall comply with IEC 60079. ESD/SIS Equipment located in certified Hazardous Area enclosures shall comply with maximum ambient conditions for continuous operation.

Instrumentation in hazardous areas shall be certified by recognised certifying body, IEC or equivalent.

For instrumentation installed in hazardous area, Ex i (Intrinsically Safe) design is the preferred method for hazardous area protection., exception is solenoid valves which should be Ex'd' or Ex'm' certified. Other protection standards for SOVs may be used where appropriate if specifically approved by COMPANY.

9.6 Ingress Protection

The degree of Ingress Protection (IP) for equipment enclosure shall comply with IEC 60529 and equipment data sheets. The equipment minimum IP rating shall be as follows:

(a) IP 42 for Indoor climate-controlled environments

(b) IP 65 for Outdoor field environments

9.7 Engineering Units

Reference shall be made to Project Engineering Design basis for Units of Measurements.

SECTION B

10 TECHNICAL REQUIREMENTS

10.1 General Design

The Emergency Shutdown Systems (ESD) shall provide an independent protection system to maintain the plant processes in a safe state when the plant Process Control System (PCS) is unable to keep the process within predetermined safe operating limits. The ESD shall perform its safety function by sensing abnormal process conditions and by actuating final elements to bring plant in a safe state. Safe state should be achieved by isolating sections of plant via isolation valves (Emergency Shutdown Valves / Emergency Inventory Valves), stopping rotating equipment machinery such as compressors and pumps, and blowdown / depressurising sections of plant.

The ESD System also called as Safety Instrumented System (SIS) shall have a high degree of availability, reliability and fault tolerance.

ESD System Logic Solver shall be Programmable Electronic System (PES) based certified for SIL3 as per IEC 61508.

ESD system shall be ‘off the shelf’ equipment with ‘Field Proven’ design in industrial safety applications and certified for intended use.

The ESD system VENDOR shall have a proven track record over a minimum 15 years in providing design, engineering, supply, and commissioning services for large scale Oil, Gas, Petrochemical and related process facilities.

The ESD system shall be engineered considering the full life cycle from design, installation, commissioning, start-up, operations and maintenance through to decommissioning as per IEC 61508 and IEC 61511 requirements.

10.1.1 System Architecture

The Process facilities will be controlled from CCR utilising an Integrated Control and Safety System (ICSS) architecture. This approach consists of a Process Control System (PCS), an Emergency Shutdown (ESD) system, and a Fire & Gas (F&G) system, with the PCS serving as the prime control and command system.

ESD system shall have ‘suitable modular redundant’ architecture (for example. Triple or Quadruple redundant) utilising two-out-of-three or two-out-of-4D voting or any other equivalent redundant system architecture with appropriate voting configuration to maintain SIL 3 integrity. ESD System architecture shall support hot mode (online) replacement of faulty modules without degradation of system functionality, SIL 3 integrity and high availability.

The ESD system shall have a robust, fault-tolerant, redundant architecture. A single fault shall not reduce the safety availability of the system and the safe failure rate shall remain below that of a simplex processor. Process shutdown shall not occur as a result of any single component failure in the ESD system.

For large process plants with multiple units, the ESD system architecture shall be geographically distributed. The individual ESD sub-system will be located in respective unit’s Instrument Equipment Room. Each ESD sub-system shall be capable of functioning independently and should automatically switch to ‘Island’ mode in the event communication failure with CCR or between any ESD nodes located in other Instrument Equipment Room. Communication failure between ESD Systems located at CCR and Instrument Equipment Rooms

shall not automatically lead to plant shutdown. 'Island' mode response to communication failure shall be programmable.

10.1.2 Reliability

The ESD system shall be highly reliable and certified to SIL 3 rating as per IEC 61508.

The system shall be designed for an availability of 99.99 percent or better. Availability is defined as:

$$\text{System availability \%} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

SIL and Availability figures must be provided by the VENDOR with method of calculation and all assumptions clearly stated. Data for failure rates shall be derived from FMEDA analysis by recognised bodies.

MTTR of eight (8) hours and Proof Test Interval of 10 years shall be used in PFD and SIL calculations.

10.1.3 Redundancy

The basic architecture of ESD shall utilize redundant processors, I/O modules, power supply, internal buses and communication interfaces so that failure of any single component shall not degrade system safety functionality.

In redundant hardware configuration, it shall be possible to replace and repair any faulty module without interrupting system operation. Faulty module replacement shall not disrupt system safety or functionality or impact operation of the controlled process. The transition to the healthy module shall be bumpless (for example no loss of process safety and protection. No operator action shall be required to restore the system to normal operation other than simple mechanical replacement of modules.

ESD hardware and software configuration shall be designed to eliminate or subsequently minimize common mode failures.

10.1.4 Performance

The response time (input change to output response) for ESD processing shall be less than 300 msec unless specified otherwise in project functional specification for shorter response time due to process licensor or package equipment manufacturer requirements.

Loading of controllers, processor memory capacity, operator interface stations, data communications devices and networks shall not exceed 60% of total operable capacity under maximum loading conditions including all spares capacity defined in this document. Maximum loading conditions shall be based on the heaviest alarm load possible.

10.1.5 Functional Requirements

ESD System hardware shall be allocated process area and unit wise to reduce impact of any hardware failure on production loss. Using this topology, each ESD system shall operate in a self-contained mode, minimising the potential impact of any inter-nodal communications loss.

ESD System I/O modules shall be segregated by process and risk areas to increase system and process availability. In general, one I/O card shall not contain the I/O of more than one process unit. Process unit I/O split unit wise is not required for Non-Fail safe output cards driving alarm lamps. Cards belonging to one logic group shall be located together and spare points shall be left within the I/O group for expansion. Distribution of I/O shall also be governed by Unit segregation, identification as Independent Protective Layer for a specific Safety Instrumented Function and avoidance of common mode failures.

Wherever voted logic (for example. 1oo2, 2oo3 etc) is required for multiple devices, each device shall be allocated to separate I/O cards. Critical duty and stand-by equipment such as boilers, turbines, compressors and pumps that are spared shall be segregated into separate I/O cards.

Hardware portions of ESD which shares different SIF functionalities, shall be rated for highest SIL among SIF functionalities contained within. This shall include main CPU's, communication modules, I/O cards, Barriers, Relays; and power supplies to ESD system and field devices. The operating system and programming software shall also be validated as suitable for the highest required SIL of SIF functionalities executed by ESD system.

Generally, a '1' logic signal on inputs is to be used for the normal (safe) state, and a '0' logic signal for an abnormal (trip or failure) state.

Any safety critical fault resulting in a system failure shall drive ESD/SIS outputs to fail safe state. The fail-safe state shall be the de-energized mode unless otherwise specified. The ESD system outputs shall be normally energized, de-energize to trip, except for alarm/status lamp outputs. Output signals should go to a '0' (deenergized) state on power failure or on component failure. Note that certain specific applications may be designed as energized to trip. All cases where the design is to be energize to trip shall be approved by the COMPANY.

The ESD logic solver shall be designed such that once it has placed the process in a safe shutdown state, the outputs shall be latched to fail safe state. They shall be restored to energise state only after process healthy condition is restored followed by interlock reset command by operator.

10.1.6 SIL Review

Each SIF shall be SIL Validated and then Verified during detail design by CONTRACTOR during FEED and EPC stage.

CONTRACTOR shall carry SIL Validation and Verification assessments as per IEC 61511.

VENDOR shall provide necessary support to CONTRACTOR for SIL Verification activity.

VENDOR shall provide following data and necessary support for SIL Verification activity:

(a) PFD and System Failure Rates.

(b) Safe Failure Fraction.

(c) Diagnostic Coverage factors.

(d) Mean Time Between Failures.

(e) Common cause failure factor as per method detailed in IEC 61508-6.

(f) SIL 3 Certificate as per IEC 61508 from Exida, TUV or equivalent.

(g) Safety Manual.

(h) Documentary evidence of suitability of equipment based on prior use as described in IEC 61511-1.

(i) Fault tolerance report, showing conformance to IEC 61511-1 requirements.

10.1.7 Emergency Depressurisation System (EDP)

The Emergency Depressurisation System is provided to reduce the pressure in a system below the normal operating pressure to achieve following:

(a) To reduce the risk of vessel or pipeline rupture during a fire.

(b) To minimize the hydrocarbon inventory which may expose to fire hazard.

(c) To minimize the uncontrolled release of flammable or toxic gas.

The Emergency Depressurisation facility shall be designed in accordance with API RP 521.

The Emergency Depressurisation Valves (EDV) located on piping will be opened from CCR to release gases to vent system during hazardous situation. Activation of emergency depressurisation sequence shall be automatic or manual as per respective plant shutdown philosophy. EDP functionality shall be implemented in plant ESD/SIS. EDVs and depressurisation activation Push Buttons shall be wired to plant ESD/SIS. The EDP activation Push Buttons with protected cover and lamp indication shall be located on ESD console in CCR.

10.2 Functional Specification (FS) and Functional Design Specification (FDS)

The Functional Specification shall be prepared by CONTRACTOR in consultation with COMPANY and shall form the basis for the VENDOR proposals and for the VENDOR to develop the ESD system design in Detail. shall be written specifically for each project.

The FS shall provide the following information:

(1) This specification

(2) Number and spacing of IES;

(3) Number and type of I/O (Analogue, Digital, SOV, ‘Soft’ serial, IS, Non-IS) and allocation to IES;

(4) Number of Safety functions and allocation to IES;

(5) I/O Criticality ratings

(6) Requirements for ‘island’ operation.

(7) P&IDs (to support segregation assessment).

Based on the FS and additional supporting documentation, VENDOR shall develop the detailed design of the ESD system and document it in the FDS.

The supporting information supplied to VENDOR to develop the FDS shall include:

(8) Logic Descriptions;

(9) Sequence Narratives;

(10) Updated P&IDS;

(11) Operating Philosophies;

The FDS shall detail the project specific architecture, system layout, hardware, software. It shall be written in conjunction with COMPANY/CONTRACTOR by VENDOR, based on the Functional Specification, provided in the requisition, and the additional supporting documents.

The system design and build will not be approved until the FDS is approved by COMPANY.

Operator interface requirements shall be included in FDS.

The FDS shall provide a detailed inventory and description of the equipment, functional definition and equipment data, including, as a minimum:

(1) Definition of data flows to achieve FS requirements

(2) Allocation of controllers to IES/units

(3) Allocation of I/O to controllers

(4) Number of ESD cabinets

(5) Allocation of I/O to cabinets

(6) General Arrangement (GA) of cabinets including, rack distribution and mounting, power distribution, terminations, trunking, cooling fans, temperature monitoring, cable entry arrangement and dimensional drawings

(7) Preliminary configuration database

(8) Function block definitions (Valve trip, Pump trip, etc.)

(9) HMI station details /GA and dimensional drawings

(10) Access control

10.3 ESD Hardware

10.3.1 Main Processors

Each ESD system shall contain redundant CPU operating synchronously and in parallel.

Hot replacement of a CPU or modification of a CPU's running application program shall not require process interruption or system re-initialization.

A locking mechanism (hardware switch) for each CPU shall prevent memory modification from an outside source.

For CPU with volatile (RAM) memory, battery backup on CPU module shall be provided to retain data for six months in memory. Batteries on CPU module shall replaceable online without degrading ESD system functionality.

Each processor loading shall not exceed 60% in all memory areas, to allow for future expansion.

10.3.2 I/O General

The VENDOR shall provide I/O cards of robust design and high quality. I/O cards shall be installed in I/O cabinets in I/O racks or on individual base plate depending on I/O card mounting design. I/O cards shall be manufactured to withstand the facility environment, the maximum ambient conditions.

All input and output cards used in SIF shutdown logic shall be redundant, fail safe design and SIL3 certified as per IEC 61508. All output cards which are driving noncritical alarm lamps should be approved for non-interaction and are not SIL rated. Redundant I/O cards shall be used for all inputs and outputs except for maintenance override inputs and annunciators / lamps outputs. For I/O cards installed in I/O racks, single I/O

cards with empty hot spare shall be provided for maintenance override inputs and outputs to annunciators/lamps.

'Single Component' hardware such as signal conditioners, I.S barriers, Signal converters, relays used for individual SIF must be arranged in voting scheme to meet the targeted SIL of each SIF. PFD values and architectural constrains must be taken in the consideration when evaluating the achieved SIL of each SIF.

The I/O system shall be of a modular design. The I/O modules will include an electronic design that allows ease of installation. The system shall permit any I/O module to be removed or inserted into the system backplane under power without causing a system upset. The system shall include diagnostics to prevent signal scan errors due to card removal or insertion.

Except for Universal type I/O cards, a mechanical keying facility shall be provided to prevent physical insertion and on-line activation of a module in a wrong location. No address links or switches shall be mounted on the I/O modules. The module type identifier shall be located in the firmware of the module and automatically recognised by the operating system.

Number of I/O channels per I/O card shall be limited to 32 nos.

I/O Modules should preferably be universal type for example each I/O Module can be configurable to Analogue or Digital input/outputs as per requirement.

All individual I/O channels shall be electrically isolated (opto-isolator) from the main CPU and provide galvanic isolation from field equipment. Failure in any I/O card shall not affect other I/O cards. Failure or fault in any I/O channel shall not affect other I/O channels. I/O cards shall be designed so that a short circuit or high voltage on one input (or output) shall not induce a fault on any other input (or output) on the same module. Ground/Earth fault shall be automatically detected and reported preferably per individual I/O card or per individual I/O channel.

All Input and Output cards/modules shall have built in capability of 'Line Monitoring' to detect I/O channels faults like open circuit, short circuit, earth fault, load failure, supply failure, circuit fault.

For digital inputs, end line resistors used for the line monitoring purpose shall be installed on the terminal of the field switches. When isolation barriers are used in safety critical applications, line monitoring thresholds shall be configured to detect barrier faults. This ensures that barrier faults do not inhibit safety critical functions.

Input faults like open circuit, short circuit, earth fault etc which are not safety critical shall be configured with a default 2 second delay to avoid alarm chattering and spurious trips.

For the purpose of standardisation, ESD system digital outputs shall provide power to the field devices for example. solenoids, relays etc, while digital inputs shall provide 24 VDC to input switches.

All input and output points shall be individually provided with current limiting and isolation circuity.

All discrete I/O modules should include local status indicators (LED) to monitor the status of each input and output and any communication and I/O faults. Spare I/O points, which are pre-configured within the ESD system shall be shorted or terminated according to manufacturer's recommendations to avoid nuisance faults or diagnostic alarms.

Unless otherwise specified by the CONTRACTOR during detailed design, the ESD System VENDOR must assume that all Field devices, both Inputs and Outputs are located in potentially hazardous atmospheres. Inputs shall provide intrinsic safety isolation through the use of appropriately certified, galvanically isolated intrinsically safe interface units. The barriers may be either inherent in the System I/O cards or termination assemblies, or in separate field termination blocks mounted within the marshalling cabinets.

Field Cable Termination Board design shall ensure that all active components used for signal conditioning and for loop power to input/output signals are redundant. Failure of any component inside them shall not generate fault in redundant I/O signal channel simultaneously.

10.3.2.1 Analogue Inputs

The ESD system shall support following analogue inputs:

(a) 4-20mA, HART compatible, 24VDC powered by the System and load resistance 600Ω nominal.

(b) 1 to 5 V DC

(c) Range of Thermocouple and RTD inputs (Note- Temperature transmitters with HART 4-20 mA output shall be used for RTD and Thermocouple sensors unless specified otherwise)

(d) Pulse Inputs for Rate measurement

The ESD System shall be capable of interfacing with 2, 3 and 4 wire instruments with or without powering from system.

Analogue input card characteristics shall meet or exceed the following requirements:

(a) Analogue to digital conversion shall exhibit high common mode line frequency noise rejection.

(b) Normal mode rejection shall meet or exceed 60 dB at line frequency and harmonics.

(c) Common mode rejection shall meet or exceed 120 dB at line frequency and harmonics.

(d) Common mode voltage rejection shall be 500 V DC or peak AC.

(e) Automatic gain and zero shift compensation are preferred.

(f) Minimum acceptable resolution is 12 bits (1 in 4096).

(g) Accuracy, including linearity shall be 0.1% of full scale or better.

a. Open loop/thermocouple burnout (either direct or via an appropriate interface) feature is required.

HART signals connected to ESD shall be directly accessible from the Asset Management System. It is preferred to use HART compatible Field Termination Assemblies and HART enabled AI/AO instead using HART multiplexers and modems for HART interface. Exceptions shall require prior approval from COMPANY. ‘Smart’ transmitters HART data must be configured to ‘read only’.

Analogue inputs shall have open circuit, short circuit and out of range detection capability as per NAMUR NE43 standard.

History/trending data storage functionality shall be available for all Analogue I/Os.

10.3.2.2 Analogue Outputs

The ESD system shall support analogue output of 4-20 mA with HART protocol for PST of Shutdown Valves.

10.3.2.3 Digital Inputs

The ESD System shall support discrete inputs as follows:

(a) Input type- Volt free Contact and NAMUR Proximity switches.

(b) Inputs powered from ESD by 8–24 VDC wetting voltage and capable of detecting status changes with loop impedance (including contact resistance) of at least 1000 ohms.

(c) Digital input signals shall be conditioned by a low-pass filter, typically up to 15 msec, to reduce the effects of noise and bounce.

(d) A minimum of 1000 VDC opto-isolation shall be provided between each input signal and microprocessor.

10.3.2.4 Digital Outputs

The ESD System shall support discrete outputs as follows:

(a) Digital Output shall power Solenoid Valves, Interposing Relays and Alarm Lamps of voltage rating 24V DC, 48V DC or as specified in purchase order.

(b) Digital outputs shall be current rated for minimum 0.5 amp for an inductive load per point at 60°C. Output circuits shall be provided with protection against reverse EMF and voltage transients caused by the switching of inductive loads and protection against current overloads.

(c) Voltage loop back circuitry shall automatically verify that the commanded state is equivalent to the field state.

(d) Digital output modules shall operate within ±10% voltage variation, provide a minimum of 1000 VDC opto-isolation between each output signal and microprocessor, accept surge current on each point of 12A per cycle for AC voltage and 10A for 24 VDC voltage for 10 msec and 5A for 48 VDC voltage for 10 msec.

(e) Output modules shall be automatically tested for stuck-on and stuck-off components at a regular interval not exceeding 1 second.

10.4 Electromagnetic Compatibility

ESD system equipment shall comply to IEC 61000 and IEC 61326-3-3 for immunity to Radio Frequency Interface (RFI), Electromagnetic Interference (EMI) and electrostatic discharge.

The systems shall be capable of accepting various signal inputs for its direct use while preventing noise errors due to electromagnetic or radio frequency interference including hand-held or mobile communications equipment, nearby radio stations, electrical storms, solenoids, relays or contactors carrying heavy currents.

The most probable source of radio frequency interference (RFI) at the site is the use of handheld radio transceivers with nominal radiated power of 5 watts. VENDOR shall state any frequencies in the VHF and UHF and TETRA bands for which they cannot comply.

10.5 Surge Protection

VENDOR shall provide protection for the ESD system equipment against surges and transient over-voltage/currents that may be induced via the power supply, communications and signal cabling Systems. ESD system Surge protection shall be comply to IEC 61000-4-5. Protection shall be built to withstand 2kV surges on power supply cabling and 1kV on communications and signal cabling.

10.6 ESD Software

10.6.1 Programming

The CONTRACTOR shall develop Logic diagrams from ESD Cause and Effect Diagrams in line with standard formats during FEED stage and shall be further detailed during EPC stage. VENDOR shall develop application programs to implement safety logics based on Cause and Effect/Logic Diagrams, and safety requirements documentation provided by CONTRACTOR.

The application program shall be user friendly. This means that detailed comments and descriptions shall be included throughout all function block elements which identify elements by tag numbers and intended functionality.

Application software shall be designed in conformance to IEC 61511-1, clause 12.

Standard Function blocks that are pre-tested and certified by a recognized external organization like TUV shall be used be to develop the application programs.

Maximise use of standard function blocks for all frequently used functional logics. This reduces software configuration time, results in standardised application logic which simplifies operation, maintenance and future projects configuration work.

The program development software shall be capable of supporting both on-line and off-line programming. On-line programming or making on-line application program changes while an ESD system is operating, (for example., configuring new I/O points, tags and addresses, revising or adding logic and changing dynamic element parameters) shall be possible without having to reset or re-initialize application programs currently running within the CPU. Off-line program emulation shall be provided unless specified otherwise.

Program editing and saving shall incorporate automatic time-dated and revision level file saving functionality. To monitor software changes, there shall be a software utility for comparing two revisions (present and past) of application program which shall report all changes in a high level readable format to evaluate result of changes and identify extent of testing required. Verification of application software by software tool shall be possible on-line.

VENDOR shall issue Functional Design Specifications which should clearly define all standard Function Blocks (non-custom ones) developed to implement ESD functional requirements along with VENDOR's Hardware, Software, Firmware and Network solution for the Project. The methodology of preparing this documentation shall comply with IEC 61508 for software development and implementation. COMPANY approval of Functional Design Specification is mandatory prior to commencement of manufacture.

Each ESD system shall be programmed using IEC 61131 compliant software. The configuration software shall be capable of implementing all logic and safety functions required by the application. VENDOR shall state the programming method used, and the operating system required for the programming system. Additionally, the VENDOR shall advise where the programming/monitoring software resides, and the various licensing agreements for single and multiple uses of the software.

Where separate ESD functional logic groups are implemented within the same ESD, the software for each shall be kept fully segregated. As a minimum, dedicated areas within the ESD program shall be applied for each ESD functionality. These dedicated areas shall be clearly documented within the program using program comment capability. Spare internal bit and register addresses shall be maintained for each ESD functionality program or program area.

Software shall be protected from unauthorized changes by the use of both passwords and key lock switches. VENDOR shall advise what methods are available in his system for such protection.

ESD CPU shall support following software utilities for logic implementation:

(a) Math functionality with both integer and real numbers.

(b) Relay logic including transitional inputs and latching outputs.

(c) Time delays and counters.

(d) Median Select and Median Deviation function for analogue input voting.

The EWS and Logic Solver operating system, application and configuration software shall be supplied by VENDOR with the latest up-to-date software revision and associated patches till SAT. In addition, VENDOR shall make available all the software updates and patches during entire life cycle of ESD system as part of Long-term technical support contract.

10.6.2 System Log

To monitor changes in configuration, a system log shall be maintained by VENDOR from the FDS approval date till FAT, SAT and Commissioning is completed.

The system log is to record the date of changes or occurrence of problems, the cause / originator of the change or problem, summary of the change or problem, an assigned change or problem report number and action taken relating to the change or problem correction. The list shall be maintained in chronological log report number order in a format such as MS Excel (.xls) that can be easily uploaded into a database. Application program changes requested shall be kept filed by functional logic group. Each change shall be filed marked with the assigned system log report number. Maintenance of these records is required to comply with IEC 61508.

10.6.3 Engineering Workstation

Engineering Workstation shall be provided to allow the user to enter, add, delete, or modify logic program, fault diagnostics, system monitoring, and application documentation.

Access to Engineering Workstation for configuration purposes shall be restricted to users with appropriate credentials. The user access to ESD system shall be restricted by means of User Ids and Passwords or other suitable technologies for identification and authentication of users. Two factor authentication and password protection shall be provided for each user. The system shall be capable of defining user groups as per roles Engineer, technician. System access privileges shall be configurable for each user group.

The Engineering Workstation shall be capable of monitoring the status of application programs in real-time. Manual forcing of input or output states and visible power flow on logic diagram shall be possible.

All programming shall be done using alphanumeric tag name references and allow on-screen comments for functional description of application program.

Off-line programming shall provide run emulation capability for testing and troubleshooting of the application program. Software changes shall be done off-line, tested, and then compiled into the running application.

The VENDOR shall detail in the ESD FDS the methods of version control and storing of master and backup copies of application programs for all the ESDs located at different geographical locations. Each change shall have the detail of the change, the time and the personnel who performed the change logged.

VENDOR shall fully describe and quote as an option any offline and remote diagnostic tools that are available for use with the system.

Additionally, for process plants with multiple ESD systems located at various Instrument Equipment Rooms, it shall be possible to connect PC-laptop based EWS at each ESD location, for purposes of monitoring or programming. The VENDOR is responsible for providing all necessary hardware, communication ports and internal cabinet wiring to support this EWS connectivity requirement at each ESD system location.

VENDOR shall provide an EWS software backup and restore system.

10.7 Communication

ESD System shall consists of following two networks for communication:

(1) Safety Network (SN)- this shall be a SIL 3 rated, redundant network used to communicate safety critical signals such as inter-trips between various ESD system nodes.

(2) Process Control Network (PCN) - used for interfacing with PCS for ESD I/O display, alarming of shutdowns and diagnostics, invoking of operational and maintenance overrides from PCS OWS.

The SN and PCN communication networks shall be dual redundant and support IEEE-802.3 Ethernet interface capability. The communications modules shall include an internal program (self-diagnostics) and transmission error detection mechanism to locate hardware malfunctions and aid in locating coding errors in the configurations and software programs.

Connections to networks and devices outside of the ESD system shall be performed through dedicated firewall devices. ESD communication networks shall be 'Achilles' certified for cyber security and robustness.

Communication interfaces shall be off-the-shelf, using existing, industry standard media and communications protocols such as Modbus or Ethernet as identified in project specifications.

All communications ports shall permit connection or disconnection of cabling without interrupting or jeopardizing ESD system operation.

Error checking schemes shall include Cyclical Redundancy Checking (CRC), Longitudinal Redundancy Checking (LRC) in conjunction with bit parity checks, fail safe transmission time-out, message fault words, and loss of communication path alarms.

No adverse effect shall occur on communications networks during transients when many variables are changing rapidly or by data queries from the maintenance station. Data highway broadcast 'storms' shall not cause the ESD system to lock up or operate improperly.

The communication interface shall be sufficiently robust to withstand electromagnetic interference including power surges without causing a dangerous failure of safety functions.

The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

VENDOR is responsible for the correct design of the Communication Network interface to affect bi-directional transfer of all ESD information and maintain ICSS screen update of 1 to 3 seconds maximum.

Loss of data communication to PCS PCN shall not result in trips or status changes of the ESD communication points. Recovery of communication shall be automatic. The VENDOR shall indicate the type of output (hardwired) will be made available for annunciation of communication failure at PCS OWS.

For connecting ESD Systems located at different locations, the SN and PCN communication networks shall use redundant fibre optic cables and components, installed by others across various plant units, utilising segregated path routing to minimise common mode failure of redundant links. Fibre Optical cables shall be terminated directly to ESD communication module or through Network switch/media converter. Communication system components including Network Switches, Media Converter, power supplies shall be redundant.

10.8 Human Machine Interface

10.8.1 Operator Interface

The ESD system shall be designed to operate on a stand-alone basis. Under normal conditions, the ESD system shall utilize the PCS OWS to display status of all ESD I/O's and alarm notifications.

From PCS OWS, Operators shall be able to view all data related to ESD for example process parameters current values, states of all ESD inputs and outputs, alarms, maintenance overrides, resets.

ESD system data shall be displayed on the PCS Process Graphic displays in the same way as native PCS data. Though ESD system I/O's are not directly connected to the PCS, same shall be transparent from the PCS OWS to the maximum extent possible.

The PCS shall be utilised to display ESD system shutdown hierarchy, architecture and ESD shutdown logics in Cause and Effect diagrams format.

The PCS OWS shall display various faults and process alarms generated in ESD system for analogue and digital I/Os. Fault alarms shall include Open circuit, Short circuit, Earth fault. Process alarms shall include measuring parameter High High, High, Low, Low Low alarms for example. LAHH, LALL.

To transfer display and alarm data, ESD shall communicate with the PCS OWS seamlessly as with any other PCS nodes on the PCN Communication Network.

Separate ESD hardwired Mimic or Matrix panel is not required unless specified otherwise in purchase order.

10.8.2 ESD Console

ESD Console shall be provided in CCR to install Push Buttons (Shutdown, De-pressurisation, Reset), key Switches for Input Overrides (MOS), and Visual and Audible Annunciator for critical alarms.

Where applicable, in addition to CCR, the Emergency Shutdown and Depressurisation Push Buttons shall be provided on ESD console at Local Control Rooms near to process units. If ESD Processor cabinets are installed in remote Instrument Equipment Room, then ESD console Digital I/O data shall be transferred to ESD Processor on dual redundant SIL3 certified Safety Network.

To avoid spurious trips, the Total Plant and Unit Shutdown, De-pressurisation and Critical equipment shutdown activation Push Buttons shall be triplicate contacts (provide 3 separate contacts) for 2oo3 voting.

Shutdown and Depressurisation push buttons shall be fitted with mechanical protection to avoid accidental initiation.

10.8.3 Maintenance Override Switch

The Maintenance Override Switch (MOS) functionality shall be provided only for ESD inputs to bypass inputs during plant start-up and maintenance operations. The application of ESD Input Overrides during maintenance shall be controlled at supervisory level via Master Inhibit Enable key switch with lamp indication on ESD console. When it is in the 'Override On' position, a limited number of individual maintenance overrides from PCS HMI can be applied. Turning the key to the 'Off' position shall remove all overrides and extinguish the warning lamp.

Start-up overrides from PCS HMI shall be granted if Master Start-up Inhibit Enable Key Switch is in 'Override On' position. Timers shall be used on start-up override, to remove these after a pre-defined time.

The MASTER Inhibit Enable key-switch shall be of 'stay put' type with key reset. The key shall be removable in the 'Off' position.

ESD system shall support following functionality for MOS Management:

(1) Two factor authentication and password protection to activate individual input override in addition to hardwired MASTER Inhibit Enable key-switch on ESD console

(2) MOS activation incident shall be logged and generate alarm in PCS.

(3) MOS timeouts shall be configurable to remove input overrides either automatically or manually

(4) Alert operator if input is in override state for long time than timeout limits

(5) The history of MOS activities for example enabled, removed, timeout etc shall be available in SOE and displayed in dedicated MOS display in EWS and PCS OWS.

(6) In order to maintain adequate protection, multiple overrides enable at a time shall be limited. The input overrides shall be organised in groups (process system wise) and limits on number of overrides per group shall be configured (typically 2 input override per group maximum).

(7) For 2oo3 voting logic, it shall not be possible to override more than one input at the same time. During override condition, the 2oo3 logic shall automatically degrade to 1oo2 unless otherwise specified.

10.9 Diagnostics

The system shall incorporate comprehensive self-diagnostics such that all permanent and transient faults are identified, alarmed and reported.

ESD system shall have ‘Watchdog’ functionality to monitor healthiness of hardware and software.

ESD system shall be capable of identifying, locating and reporting the following faults as a minimum:

(1) CPU faults

(2) Communication faults.

(3) I/O module faults.

(4) Scan failure of main or I/O processors.

(5) Memory faults.

(6) I/O interface or addressing faults.

(7) Application program and hardware layout inconsistency.

(8) Voted signal discrepancy on inputs and outputs.

(9) Voted discrepancy on calculated values within application program.

(10) Load power or fuse faults on field circuits.

(11) Power supply faults including battery back-up monitoring and output voltage verification.

(12) Over temperature conditions.

(13) Transmitters Bad Quality (BQ) status as per NAMUR 43.

(14) System cabinet high temperature.

(15) MCB fault.

(16) Fan failure/Temperature alarm of CPU system rack.

(17) Watchdog failure.

(18) I/O forcing status.

(19) Common fuse blown indication for I/O cards and power supply units.

(20) Incoming feed power supplies failure status.

(21) Earth fault of I/O Channel.

(22) Open Circuit fault for Normally de-energized I/O loop.

(23) Short Circuit fault.

(24) Safety Network status.

I/O module diagnostics shall be able to detect and alarm I/O point faults of the following types:

(i) 'stuck-on' - short circuited failure of a discrete input or output.

(ii) 'stuck-off' - open circuit failure of a discrete output.

The Diagnostic Test Interval for faults monitoring of ESD System and its I/O's shall not exceed 1 second. This self-testing for fault monitoring shall not affect performance of the ESD system.

The diagnostics of the system shall allow identification of all faults that a system component can alarm on the network up to and including the module level for all types of components. For I/O modules, the diagnoses, in addition, should be available up to channel level. The diagnostics shall be presented through PCS graphics depicting the cabinet and locating the faulty component. The status of the component shall be green if healthy and red if an alarm condition is present.

Status indicators shall be provided to indicate normal operation or fault conditions on each replaceable module. In addition, each fault shall initiate a hard alarm contact or an internal fault flag for communication to a PCS host computer or other operator interface.

Diagnostic Reports should be generated by the system with clear and interpretable diagnostic information. It is not acceptable to generate report files which can only be analysed at VENDOR'S facility. The ESD shall provide reports detailing active overrides and inhibits that are generated on shift changes.

10.10 Alarm Management

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

An Alarm Management System (AMS) shall be implemented in ICSS.

Alarm Management shall comply with the EEMUA Publication 191 and the ISA 18.2 requirements.

The alarm management software for ESD system shall have the following AMS capabilities:

(a) Alarm and event logging

(b) Storage of alarms and events for retrieval

(c) Sorting of alarms and events in chronological order

(d) Sorting of alarms by priority

(e) Providing statistical analysis of alarms and events

(f) Alarm reports (shelved alarms, filtered alarms, masked alarms, statistics)

(g) Alarm change management (alarm threshold modification, alarm priority change)

(h) Printing and reporting.

(i) First out alarm.

(j) Alarm masking and dynamic suppression

The alarm and event history shall be periodically backed onto another central server for permanent storage.

Refer to ADNOC Group Company AMS specification for further details.

10.11 SOE Requirements

SOE application shall accurately record the sequence of events in the order of their occurrence and enable rapid root cause analysis of trips after multiple events have occurred.

SOE shall be configured to perform both event logging and first-out reporting, for example, the time-tagged discrimination of trip events as well as first out event capture, that will allow the determination of the first event which caused individual or collective process equipment to trip.

First-out alarm/event sequence configuration shall comply to ISA 18.1. First-out (first alert) alarm/event functionality shall be used to indicate which one alarm in a group of alarms operated first. To accomplish this, the HMI indication for the alarm point that operates first must be different from the visual display indication for subsequent alarm points in that group. Only one first out alarm indication must exist in any one first out group.

The SOE and SER shall be a standard feature of ESD system. The SOE shall utilise time stamping carried out at ESD Processor and I/O module level to log events. Along with basic process alarms and trips, the system faults, device health, operator actions shall be captured.

VENDOR shall verify feasibility of using EWS as SER without loss of SOE functionality while EWS is being used for configuration.

SER shall be capable of storing 100,000 time stamped events in a circular file. The time stamp shall equal the respective ESD-PLCs clock time at the time the trip alarm is generated with a resolution equal to or better than the smallest scan time of ESD. Cater to processor communication failure, at least the last 1000 events per processor shall be stored in internal non-volatile memory.

ESD system master clock shall have 1 ms resolution. Events (faults and alarms) shall be time stamped at I/O module level. The minimum time resolution between SOE events shall be 1 ms. No events shall be missed, and all events shall be recorded on each scan.

Each ESD CPU shall be synchronize with all other nodes on the PCN communication network via a time signal broadcast on the PCN from an SNTP Time server. As with all nodes of the ICSS, the time synchronization of the ESD and SOE clocks shall be kept within 10 - 25 msec.

Combined SOE reporting of PCS and ESD events via the PCS shall be provided. ESD SOE information should be passed to the PCS via a direct PCS highway node communication module resident in the ESD. The SOE data together with time stamp information should be transferred from the ESD to the PCS. The ESD must buffer SOE data in memory until the interface communication module successfully completes transmission of the data to the PCS. Software resident in the PCS shall then assimilate and store all ESD SOE data with PCS generated SOE data, as well as SOE data transmitted to the PCS by other subsystems.

10.12 Cabinets

10.12.1 Construction

ESD system and marshalling cabinets shall be rigid and self-supporting. Cabinets shall be constructed of sheet steel with a rigid internal steel frame. Cabinets shall be braced for shock and vibration normally encountered during transport and construction.

The cabinet's structure thickness shall be minimum 1.5 mm for cabinet steel plate sides, roof and bottom, and minimum 2 mm for doors and plinths.

Unless otherwise specified in Purchase order, the dimensions of the cabinets shall be 2000 mm (H) (excluding plinth) x 800mm (W) x 800 mm (D) (front access). If cabinets are permanently bolted to form sections, the length of these sections shall not exceed 2400 mm.

All cabinets shall have the same exterior and interior finish and colour. Cabinet colour shall be RAL 7035. Plinth colour shall be RAL 7022.

The cabinet Internal layout shall be designed to provide safe and unimpeded access to all electronic modules, power distribution, fuses, terminals and cables termination areas, cables and wiring routings and replacement of defective parts with the minimum amount of dismantling or removal of associated equipment.

Cabinets shall have redundant ventilation fans at cabinet top section for heat removal. Alarms shall be provided for cabinet high temperature and fan failure. Cabinets shall be equipped with ventilation louvers with dust filters units. Inlet louvers shall be installed at the bottom of cabinet doors. Filter screens shall be readily accessible and easily removable.

At the top of cabinet, a hole shall be provided to connect air sampling tube from High Sensitivity Smoke Detection (HSSD) System. Tube connection hole size shall be as per Purchase Order requirements.

Cabinet and inside equipment support shall be designed to dampen effects of external vibration.

Eyebolts shall be mounted on each cabinet to facilitate handling during unloading and permit transportation of the enclosure by crane.

All unused I/O module slots shall be fitted with removable cover plates.

Cabinet shall have lockable hinged doors. Hinges shall be the lift off type for example doors shall be easily removable from cabinet. All door locks shall be provided with the same lock and key combination. Keys shall be removable with the doors either locked or unlocked.

Internal lighting lamp at the top of the cabinet shall be controlled by a door switch or movement detector and incorporating a manual on/off/auto switch.

A pocket shall be provided on the inside of the door to keep cabinet drawings.

Each Cabinet and all its major components shall be clearly labelled and identified with a Tag Number. Cabinet nameplates shall be by engraving on three-layer plastic. Material layers shall be red-white-red for ESD system and shall be attached with stainless steel screws. Nameplate engraving shall be subject to CONTRACTOR review and approval.

VENDOR shall assemble a typical cabinet for approval by COMPANY prior to commencing assembly of all cabinets. Final cabinet layouts shall be a part of Functional Design Specification and will be subject to COMPANY approval.

10.12.2 Wiring

In case of conventional system (I/O cards installed in CPU cabinets), VENDOR shall provide Field Termination Assemblies (FTA) in ESD Marshalling cabinets for wiring field signals to I/O cards. VENDOR shall provide all interconnection cables from marshalling to CPU cabinets and between CPU cabinets. All wiring except power wiring between cabinets shall utilize VENDOR standard multicore cables with pluggable pre-assembled terminators/connectors. For Solenoid or similar higher loads cabling shall utilize terminal boards suitable for 2.5 mm2 or higher size conductor cables. I/O cards shall not be split over more than one cable connector and shall not contain I/O of more than one process unit.

All wiring shall be segregated according to type (input or output) and voltage levels.

Colour coding for wiring shall be as follows:

Power 24V DC positive - RED negative - BLACK 240V AC phase - BROWN neutral - LIGHT BLUE
Input and output signals - WHITE (or BLUE if a colour is to be used to indicate Intrinsically Safe signals)
Safety Earth - GREEN/YELLOW Signal Earth - GREEN Intrinsic Safe Earth - GREEN/BLUE

All interconnecting cables shall be tagged at both ends with cable number and cabinet number. Wiring core shall be tagged at both ends with terminal and module number using shrink sleeve type markers or equivalent.

All internal wires shall be stranded copper except for thermocouple type where it should match the thermocouple type.

Internal wiring shall be laid in PVC close slotted ducting (raceway) with a covering lid colour coded blue for Intrinsically Safe and Grey for non-Intrinsically Safe wiring. Ducting (raceways) shall have at least 40% spare capacity after commissioning.

Internal cabinet wiring, cables and wire ways shall be minimum flame retardant in accordance with IEC 60332.

Cable entries shall be from the cabinet bottom and provide facilities for sealing (such as gland plate) to prevent ingress of moisture, contaminants and rodents from entering the cabinet.

All internal and external wiring shall be connected to terminals. Splices are not permitted in wiring. Terminal blocks shall be Push-in Spring type (cage clamp type) and non-hygroscopic type. Terminals shall be tinned and clearly identified. The size of the terminal blocks shall be consistent with the wire size. Segregation of IS and Non-IS marshalling is required. Terminal colour for Non-IS wiring shall be Grey and Intrinsic Safe wiring shall be Blue. Terminals utilized for voltages higher than 48 volts shall be protected against accidental contact with removable cover plates which carry high voltage warning labels. Terminal blocks shall be labelled and numbered.

All panel cabinet tagging for cabinets, racks, TBs, Distribution boards, Terminal blocks, shall be engraved tagging fixed in a permanent manner. Sticker or temporary tagging is not acceptable.

10.12.3 Power Supply

Unless otherwise specified in the Purchase Order, each cabinet will be powered from redundant 240 VAC, 50 Hz UPS dual redundant feeders by the CONTRACTOR. For each incoming power feed, a double pole isolation switch shall be provided. Individual alarms will be generated for each of these when turned to the off position or on any fault.

System power supply located inside ESD cabinets shall be dual redundant and each shall be capable of supplying 100% system power if other fails. All power supplies, without considering redundancy shall include a spare capacity of 25 percent of the maximum load considering all spare I/O slots were filled.

Power supplies shall be replaceable on-line without disrupting the process and without affecting functioning of ESD System. Distribution of all power levels to all system chassis and modules shall also be completely redundant as a minimum. This is to be inclusive of all voltage levels required for logic processors, all chassis requirements, I/O modules and communication modules. This means that the failure of a power supply or incoming line shall not take out a leg of I/O or a main processor. Cabinet power supplies shall have over-temperature protection, integral fuse protection, and status LEDs to indicate power supply faults.

Miniature circuit breakers (MCB) and fuses shall be employed to provide electrical protection and isolation for all powered components. The distribution circuit shall ensure that at no point of single MCB failure will result in other consequences or cascade effect. MCB fault contacts shall be wired in series to generate a common fault alarm. Selection of fuses and MCB ratings shall be carefully coordinated with upstream fuses / MCBs including UPS distribution, taking into account power up inrush currents.

Additionally, separate 24 VDC redundant power supply for powering field instruments shall be provided. The VENDOR shall be responsible for designing the 24 VDC power distribution with circuit protection for all system I/O. All 24VDC –ve terminals shall be connected to Instrument earth (floating earth is not allowed). Power supply +ve outlet shall have diode.

Failure of any power supply must be signalled via a dry normally open (N/O) contact which shall be wired in series to a common discrete input point for alarm indication for each self-contained suite of cabinet(s). Each power supply shall be provided with primary and secondary overload protection. The secondary overload shall be self- resetting or have a time overload delay to prevent an instantaneous fault from tripping the system off. Over voltage protection must be provided if it is necessary for the protection of the connected loads. All individual fuses shall be considered with fault LED indication and common fault alarm for monitoring by PCS. No hidden fault is allowed without remote common alarm.

The VENDOR shall wire cabinet lighting and utility outlets to a separate breaker which will be fed from a single phase 240 VAC 50 Hz utility non-UPS power supply.

VENDOR shall provide the power consumption including inrush currents and crest factors for each cabinet to size incoming power feeders.

10.12.4 Earthing

There shall be three separate isolated Earthing Systems within the ESD cabinets as follows:

(1) Safety Earth: Each cabinet shall have a M10 brass earth stud, complete with nuts and washers for dedicated safety earthing. All metal racks, internal panels, cable tray, doors and detachable panels shall be earth bonded together to this safety earth with a flexible copper braid strap of at least 10mm2 to ensure effective earthing.

(2) Instrument Earth: Each system and marshalling cabinet shall be provided with one 5mm x 15mm copper galvanically isolated instrument earth busbar across the full width of, and insulated from, the

panel for earthing System electronics and electrostatic screens of field cables. In general, field instrument shields shall be grounded to instrument earth within the Marshalling Cabinet.

(3) Intrinsically Safety Earth – IS Earth: Marshalling cabinets with non-isolating IS barrier (for example Zenner barrier) circuits shall be supplied with an additional isolated IS earth busbar clearly labelled.

10.13 Partial Stroke Test

Valve Partial Stroke Test (PST) shall be carried to verify Shutdown valve performance during plant operation as per IEC 61511 requirements to maintain valve PFD within acceptable limits and to avoid frequent proof (full stroke) test.

PST facility shall be designed such that shutdown valve shall be always available to respond to a process demand during test period.

Preferably, PST shall be through Asset Management System via ESD System. PST diagnosis software shall be installed on IAMS PC. To carry PST, the ESD Output with HART protocol shall be wired to valve SMART E/P (Electro Pneumatic) Positioner. IAMS shall retrieve this HART PST data from ESD System over PCN Network to carry diagnostics. PST initiation shall be from PCN OWS using IAMS client interface.

Refer to project function specification for Shutdown Valves for further PST implementation requirements.

10.14 Cyber Security

Cyber Security implementation shall comply to IEC 62443 for safety level SL2. ESD system shall be ISASecure certified for cyber security.

ESD shall integrate securely into ICSS PCN communication network through firewall. VENDOR shall implement a ‘Safety domain’ separated from the ‘Control domain’ either by firewalls or by implementation of a localised safety communication network that is separate from the Control Domain. ESD Engineering Workstation and Controller shall sit on SN in ‘Safety domain’. PCN and SN shall not terminate on the same switch to ensure that two separate networks are maintained.

ESD Controller and Engineering Workstation shall be cyber secure by design for example it shall have built in firewall functionality to restrict access to authorized protocols and devices. It shall be able validate communication with devices using encryption and digital signatures. It shall have software whitelisting so that only authorized programs or applications are executable and malware or unauthorized programs are blocked.

Cyber Security design shall comply with the ADNOC Group Company’s Digital Security policies.

A cyber security risk assessment as per IEC 62443-3-2 shall be performed by COMPANY/CONTRACTOR. VENDOR shall provide all required support for this assessment.

The cyber security risk assessment shall be performed by CONTRACTOR as follows and shall be seen as an iterative and continuous process from hardware freeze to FAT and SAT:

1. Define the risk analysis methodology (for example architecture based)
2. Identify major items (organization, systems, subsystems, networks)
3. Identification, evaluation of the threat scenarios with their impact and likelihood
4. Reduce the risks by designing adequate countermeasures
5. Summarize the results in a Risk Register.

The cyber security risk assessment findings and recommendations shall be implemented by VENDOR.

VENDOR shall provide firewalls to enforce data transfer between ESD and PCS/ICSS.

The ESD system software patch update and security programs requirements shall comply to COMPANY Cyber Security guidelines/policies.

All unused ports on switches and routers of ESD system shall be disabled to assist in preventing unauthorized access to the ICSS network infrastructure.

VENDOR shall provide Firewall and Malware protection for Cyber Security in line with COMPANY Cyber Security guidelines/policies.

10.15 Spare Capacity/Expandability

10.15.1 Installed I/O and Cabinet Space

Each Marshalling and System cabinet shall be provided with 20% installed and wired spare for each type of I/O card. Each I/O card shall have at least 20% spare I/O channels available. The installed 20% spare shall include all associated terminations, terminal block, cable ducts, trays Field cable spare cores shall be terminated on terminal blocks.

In addition to wired spares there shall be an average 20% empty space inside cabinets for future use.

10.15.2 Memory/Processing

Spare memory for application program and database shall be at least 40%. CPU loading shall not exceed 60% of its maximum capacity at full system loading.

10.15.3 Communication Interfaces

Communication interfaces shall not be loaded more than 50% at maximum loading after plant start-up.

11 ESD REQUIREMENTS FOR SPECIAL PACKAGE UNITS

Refer to Appendix 1 for ESD System requirements for Special Mechanical Packages.

SECTION C

12 SCOPE OF SUPPLY

Detailed engineering and design of the ESD system in accordance with all specifications, standards, datasheets and other statements of requirement include with or referenced in the requisition.

The VENDOR shall have single point responsibility for all aspects of the works, inclusive of all components sub-contracted or purchased from other parties. These shall include, but not be limited to:

(1) Total system engineering definition of the ESD system in the form of a Functional Design Specification (FDS) based upon the Functional Specification (FS), datasheets and COMPANY specifications provided by CONTRACTOR. FDSs shall be written by the VENDOR and approved by COMPANY during the Design Phase to detail the VENDOR scope of work.

(2) The agreed FDS

(3) ESD System Topology

(4) Design and supply of the ESD system Console, including the integration design and resulting facilities for all free issued materials to be mounted thereon

(5) Design and supply of the ESD System Cabinets

(6) Design and supply of the ESD Marshalling Cabinets

(7) Design and supply of the ESD Auxiliary Cabinets

(8) Design of the ESD system communications network and supply of all communication equipment and cables up to and including firewalls at interface to Process Control Network.

(9) Supply of ESD hardware, software, cabinets, consoles, EWS, printers, power supply units, peripherals,

(10) All System Interconnecting cables, network switches, licenses and all other equipment required for a fully functional, operable, reliable and maintainable ESD System.

(11) Supply of operating system software and firmware.

(12) Supply of system configuration and application software including design and configuration of database, and reports

(13) Supply of specialist integration services for third party equipment forming part of the ESD system scope

(14) Supply of System test procedures, all necessary test equipment and personnel for all tests. Perform tests for witness by the Contractor’s representative

(15) Human Machine Interface for local access.

(16) Data communications

(17) Documentation

(18) Documentation and certification in accordance with the material requisition, this specification and the standards referenced herein.

(19) Special tools required installation, operation and maintenance of the equipment;

(20) Painting, Preservation and Packing;

(21)Insurance spares;

(22) Spares (commissioning and 2 year);

(23) Design and supply of power distribution system within the ESD system

(24) Certified calculations shall form part of the scope of supply as follows:

i. Sizing Calculations;

ii. Power Calculations;

iii. Heat loading calculations.

(25)Commissioning; start-up and long term support.

(26)Site assistance for ESD system installation and commissioning

In addition to the above requirements, design, fabrication, configuration, testing and installation shall also be compliant with cyber-security requirements.

13 QUALITY CONTROL AND ASSURANCE

Equipment shall only be purchased from Vendors approved by ADNOC Category Management. This approval indicates that the VENDOR has an approved Quality management system and a proven track record in supply of this equipment type.

COMPANY/CONTRACTOR reserves the right to inspect materials and workmanship at all stages of manufacture and to witness any or all tests.

VENDOR shall comply to Criticality Rating for Equipment outlined in respective ADNOC Group Company's Quality System Specifications for requirements of production checks, shop inspection, testing and material certification.

The VENDOR shall provide equipment inspection and test reports as per approved Inspection and Test Plan by CONTRACTOR.

14 CERTIFICATIONS

VENDOR shall provide SIL 3 certificates for offered ESD system from Exida, TUV or equivalent.

VENDOR shall provide all Test Certificates as per Supplier Document Register and Schedule (SDRS) provided in Purchase Order.

15 INSPECTION & TESTING REQUIREMENTS

15.1 General

The VENDOR shall be responsible for workmanship, testing and quality assurance of the material supplied.

Inspection and Testing will be carried out by VENDOR and it will be witnessed by the CONTRACTOR and COMPANY representatives at various stages and locations as follows:

(1) Pre-Factory Acceptance - conducted at the system assembly/manufacturer location.

(2) Factory Acceptance Test - may be conducted at the system assembly location as a standalone ESD test and then again at the PCS location as an integrated test, or entire testing may be done at the PCS location.

(3) Integrated Factory Acceptance Test – conducted following FAT at the PCS location.

(4) Site Installation Test- conducted at the job site once system is installed and powered up.

(5) Site Acceptance Test - conducted at the job site as a system operating test after commissioning.

VENDOR shall provide all test procedures to CONTRACTOR and COMPANY for review and approval at least two months prior to the proposed test schedule.. Each formal acceptance test must be signed by a VENDOR, CONTRACTOR and COMPANY representative at the successful completion of the test(s).

15.2 Shop Inspection

CONTRACTOR'S representative will periodically visit the VENDOR'S shop facilities and inspect system progress from a hardware and software perspective.

15.3 Pre-Factory Acceptance Test

VENDOR shall detail all physical tests and inspections which will be performed in the Pre-FAT procedure. As a minimum these tests shall include complete physical inspection of all cabinetry, system components, wiring, labelling, Additionally, the procedure shall list all internal VENDOR test/inspection records which can be provided to the CONTRACTOR during the Pre-FAT. As a minimum, project related QA inspections covering bought out components and internal inspections of assemblies are to be included.

The system equipment will be inspected by CONTRACTOR representative at the Pre- Factory Acceptance Test for satisfactory quality and workmanship. In addition, COMPANY or CONTRACTOR shall have the right to inspect the work in progress at any stage.

The VENDOR is responsible to maintain a punch list during the Pre-FAT. The Pre-FAT punch list shall list the problems discovered, include the date discovered, the name of the person reporting the problem, the date corrected, the name of the person who performed the correction, the date retested and accepted, and the name of the individual accepting the retest. This entire Pre-FAT punch list shall be given one System Log report number and maintained as part of the ESD system log. Unless otherwise agreed by COMPANY, all items on the Pre-FAT punch list shall be cleared before the commencement of FAT.

The entire Pre-Factory Acceptance Test (Pre-FAT) procedure must have been successfully exercised on the system by the VENDOR prior to the FAT.

15.4 Factory Acceptance Test

The FAT shall include the complete testing and acceptance of both hardware and software.

The VENDOR shall be required to submit FAT procedures for approval prior to FAT. These shall cover, but not be limited to:

(a) Complete hardware testing including simulation of all input and output channels, testing of all system redundancy (CPU's, power supplies, I/O buses, I/O comm modules, highway communication modules,), observation of fault reporting via hardware indicators and data transfers, and hot swap component replacement.

(b) Complete simulation of all functional logic groups. This testing is to be inclusive of I/O simulation through the marshalling cabinets and system cables to ensure healthy HW and SW configuration for all I/O. Functional test shall be performed through software simulation for all tested I/O. It is intended that this testing be performed with the ESD system data linked with the PCS. In this case all PCS/ESD data transfers associated with each functional logic group shall be exercised and observed during the function logic validation testing. If schedule or other requirements necessitate testing of the ESD functional logic prior to a PCS integration test, all data transfer bit sets and register values will be exercised/observed for correct operation by means of a test computer simulating a PCS while testing the functional logic. In this case, later Integrated testing with the PCS shall include PCS highway interface of the ESD processors with the project application software loaded. At least 10 percent of all interface data points shall again be simulated, and correct results observed. Additionally, full redundancy testing of the communications interface shall be performed. CONTRACTOR and COMPANY approval to perform the ESD FAT first separately, and then integrated as described above must be obtained in writing by the VENDOR.

(c) As the functional logics are checked, proper recording of SOE data shall be verified. Additionally, the SOE sorting and reporting capabilities shall be demonstrated and certified correct.

During FAT the system shall be made available to CONTRACTOR and COMPANY for sufficient periods to verify satisfactory performance.

COMPANY and CONTRACTOR'S representative will witness the entire FAT. The FAT procedure/checklist will be signed off by the VENDOR, CONTRACTOR and COMPANY representative at the successful conclusion of testing. A copy of the signed off FAT procedures/checklist and related printouts shall be furnished to CONTRACTOR and COMPANY representative. Each punch point shall be categorised to define criticality and time frame for completion. This is applicable to all tests & punch lists.

All process inputs and outputs must be simulated during the FAT. The purpose of this simulation is to provide a facsimile of the production process, with all points of an individual loop or interconnected loops hooked up for test simultaneously.

All system programs must be complete and resident in the system prior to the start of FAT. All program listings must be free of pencilled (patched) corrections. The system software loaded must be the final version encompassing all required changes incorporated after VENDOR internal testing. Any changes which were made as a result of internal testing shall be documented as part of the ESD system log.

The VENDOR is responsible to maintain a punch list during the FAT. The FAT punch list shall list the problems discovered, include the date discovered, the name of the person reporting the problem, the date corrected, the name of the person who performed the correction, the date retested and accepted, and the name of the individual accepting the retest. This entire FAT punch list shall be given one System Log report number and maintained as part of the ESD system testing log.

Diagnostic programs which are tested during FAT shall be shipped to IFAT with system.

15.5 Integrated Factory Acceptance Test (IFAT)

Following FAT, IFAT shall follow and include testing of communication interface between ESD and PCS. Data transfer between ESD and PCS shall be checked. ESD graphics implemented in PCS OWS shall be 100% tested.

IFAT testing procedure shall be furnished by VENDOR for CONTRACTOR and COMPANY approval.

15.6 Site Installation Test (SIT)

After the system has been installed on site and site QA as well as VENDOR inspection of the mechanical and electrical installation has been successfully completed, a Site Installation Test will be conducted by the VENDOR when directed by the CONTRACTOR.

SIT shall include as a minimum:

(d) An audit and inspection of equipment as installed. A deficiency report shall be written, and appropriate action taken to rectify any problems.

(e) All alarm status, analogue and pulse inputs, and controlled end devices shall be disconnected by means of isolating terminals.

(f) Each system shall be powered up and system and application software will be loaded. System diagnostics shall be run and checked to ensure the system is error free.

(g) Communications shall be established between all components of the system and from the ESD to the PCS.

(h) Redundancy testing of processor, power supply systems, I/O buses and communication modules shall be performed.

(i) At least one point from every input/output module shall be verified by signal simulation/monitoring from the associated marshalling cabinet.

(j) A random sampling of data transfers between the PCS and ESD shall be performed to ensure proper operation of the data links.

(k) All MOS enable switches shall be checked for proper operation by exercising the enable switches, implementing PCS soft MOS functions, checking the ESD implements the MOS and then observing the ESD clearing imposed soft MOS functions when the MOS enable switches are switched to the off position.

(l) Random sampling of SOE data shall be conducted.

Full details of all tests to be performed shall be defined in the SIT procedure.

The VENDOR is responsible to maintain a punch list during the SIT. The SIT punch list shall list the problems discovered, include the date discovered, the name of the person reporting the problem, the date corrected, the name of the person who performed the correction, the date retested and accepted, and the name of the individual accepting the retest. This entire SIT punch list shall be given one System Log report number and maintained as part of the ESD system test log.

COMPANY and CONTRACTOR representative will witness the entire SIT. The SIT procedure will be signed off by the VENDOR, CONTRACTOR and COMPANY representative at the successful conclusion of testing. A copy of the signed off SIT procedures and related printouts shall be furnished to CONTRACTOR and COMPANY representative.

Upon completion of the SIT, the system shall remain powered on and loop checks shall be conducted as loops are made ready. System status shall continue to be monitored and all detected faults and/or changes/modifications to system hardware and software shall be recorded in the System test log. During commissioning, loop checking shall include the whole loop, from the control room to the field device.

15.7 Site Acceptance Test (SAT)

After the system has been commissioned and put in service the Site Acceptance Test period commences. The purpose of the site acceptance test is to verify that all hardware and software is correctly installed and functioning according to the specifications in the real environment and verify integrated performance of the ESD with the ICSS system.

The SAT shall be conducted as per SAT procedure/checklist approved by COMPANY. The SAT procedure/checklist shall fully detail all acceptance tests criteria. The SAT shall only be deemed as completed only after all loops, logics, hardware, software, functional requirements and ICSS integration checks are thoroughly completed.

This test shall include monitoring the system data transfer and update times. SOE data capture and time synchronization between the PCS and ESD shall be verified. Transmission and display of correct first out alarm notifications as well as secondary alarms shall be observed. System diagnostics shall be routinely checked. The SAT procedure shall fully detail all acceptance test criteria. Duration of SAT shall not be less than 72 hours.

The VENDOR is responsible to maintain a punch list during the SAT. The SAT punch list shall list the problems discovered, include the date discovered, the name of the person reporting the problem, the date corrected, the name of the person who performed the correction, the date retested and accepted, and the name of the individual accepting the retest. This entire SAT punch list shall be given one System Log report number and maintained as part of the ESD system test log.

The SAT procedure/checklist will be signed off by the VENDOR, CONTRACTOR and COMPANY representative at the successful conclusion of testing. A copy of the signed off SAT procedures and related printouts shall be furnished to CONTRACTOR and COMPANY representative.

Successful completion and approval of the SAT will constitute system acceptance by the CONTRACTOR and COMPANY.

15.8 Certificates of Acceptance

At the satisfactory conclusion of the FAT, IFAT, SIT, and SAT a Certificate of Acceptance shall be provided by the VENDOR for signature by the CONTRACTOR and COMPANY.

Following documents as minimum shall be attached to Certificate of Acceptance dossier:

(1) Signed and Approved FAT, IFAT, SIT and SAT test reports

(2) Electric Equipment Test Certificates

(3) SIL Certificates

(4) Hardware Test Certificates

(5) Software Test Certificates

(6) Approved As-Built Drawings

15.9 Services by the VENDOR

The VENDOR shall supply necessary manpower and specialist personnel and all necessary tools and equipment to support testing at Vendor's shop and at site as defined above sections.

16 SUBCONTRACTORS/SUBVENDORS

The VENDOR shall assume unit responsibility and overall guarantee for the equipment package and associated equipment.

The VENDOR shall transmit all relevant Purchase Order documents including specifications to his SUBCONTRACTORS.

It is the VENDOR'S responsibility to enforce all Purchase Order and Specification requirements on his SUBCONTRACTORS.

The VENDOR shall submit all relevant SUBCONTRACTOR drawings and engineering data to the CONTRACTOR.

The VENDOR shall obtain and transmit all SUBCONTRACTOR warranties to the CONTRACTOR/COMPANY, in addition to the system warranty.

17 SPARE PARTS

17.1 Spares

The VENDOR shall identify the following spares:

(1) Pre-commissioning, commissioning and start-up spares

(2) Recommended spares list for two years operation

Spares shall be itemised and priced in VENDOR quotation.

VENDOR shall support supply of spare parts for 15 years.

The VENDOR shall complete the Spare Parts Interchangeability Record (SPIR) Form to be supplied by the CONTRACTOR. The CONTRACTOR shall agree Spares to be included in Purchase Order.

17.2 Special Tools

The CONTRACTOR shall agree the Special Tools to be included in Purchase Order.

The VENDOR shall identify all necessary standard and special tools, test software, and test and calibration equipment required to perform routine maintenance and any other recommended tools for specialised procedures.

The VENDOR shall provide design and performance specifications for all special tools, test software, and calibration equipment.

The list of the standard tools shall state the following:

(a) Description of its service

(b) Manufacturer and Catalogue No

(c) Quantity recommended.

Special tools shall be itemised in VENDOR quotation.

18 PRESERVATION & SHIPMENT

18.1 Packing and Shipping

Preparation for shipment shall be in accordance with purchase order Preservation and Export Packing requirements. VENDOR shall be solely responsible for the adequacy of the preparation for shipment provisions with respect to materials and application, and to provide equipment at the destination in ex-works condition when handled by commercial carriers. Adequate protection shall be provided to prevent mechanical damage and atmospheric corrosion in transit and at the jobsite. Preparation for shipment and packing will be subject to inspection and rejection by COMPANY'S/CONTRACTOR'S inspectors. All costs occasioned by such rejection shall be to the account of the VENDOR. Equipment shall be packed, securely anchored, and skid mounted when required. Bracing, supports, and rigging connections shall be provided to prevent damage during transit, lifting, or unloading. Separate, loose, and spare parts shall be completely boxed. Pieces of equipment and spare parts shall be identified by item number and service and marked with CONTRACTOR'S order number, tag number, and weight, both inside and outside of each individual package or container. A bill of material shall be enclosed in each package or container of parts. One complete set of the installation, operation, and maintenance instructions shall be packed in the boxes or crates with equipment. This is in addition to the number called for in the Purchase Order.

All kinds of regulatory / non-regulatory approvals and procedures required for shipping shall be in the scope of CONTRACTOR / VENDOR.

18.2 Preservation and Storage

Equipment and materials shall be protected to withstand ocean transit and extended period of storage at the jobsite for a minimum period of 18 months. Equipment shall be protected to safeguard against all adverse environments, such as humidity, moisture, rain, dust, dirt, sand, mud, salt air, salt spray, and seawater. All equipment and material shall be preserved, and export packed in accordance with project specifications.

The VENDOR shall provide preservation plan to protect and ensure the integrity of ESD equipment during the period that starts when the ESD equipment is prepared for the first shipment from the point of origin and ends at the completion of project commissioning and start-up. The plan shall identify protective measures to be implemented during each phase of the project, inclusive of maximum ambient conditions. The completion plan shall be submitted to COMPANY for review and comment no later than 90 days prior to the first shipment of ESD equipment from the factory.

19 COMMISSIONING

19.1 Installation

VENDOR shall provide supervision assistance for Installation and Commissioning of ESD System at site. Installation will be carried out by the CONTRACTOR with supervision assistance from the VENDOR. The VENDOR shall notify the CONTRACTOR of any special tools required for installation and supply these if necessary, to the CONTRACTOR.

19.2 Life Cycle/Long Term Support

VENDOR must provide assurances that system equipment will not be obsolete in the next 15 years. In the belief that portions of the system will eventually be withdrawn from sale, a firm commitment by the VENDOR that for his standard products there will be either repair capability or equivalent parts and/or products available for a minimum of 15 years from the withdrawal date is required.

The ESD design shall consider the requirement that the system will require to be upgraded during the design life of the facilities. ESD supply shall be given specific attention to ensure all systems, components, software and individual elements and the respective running tools, test equipment, software and human skills can be maintained or replaced such that the original function and integrity of the whole ESD can continue in an uninterrupted manner for the field life.

The entire system shall be in ‘Active life’ for a minimum period of minimum 15 Years. Vendors shall provide life cycle commitment including:

(a) Start of Active life

(b) End of active life

(c) Start of limited support

(d) End of limited support

(e) Start of Obsolescence

Active life: Denotes the system is active and available for sale for new projects and revamp projects, full support from R&D, continuous support in terms of upgrade, patch update, bug fixing

Limited Support: Product has limited support with local maintenance and engineering support; bug fixing, continue to supply of spares (refurbished or new parts).

Obsolete: Out of sale and support is discontinued.

Between active to support phase, vendor shall provide a minimum support period of 7 years for company to plan for a smooth upgrade or replacement.

19.3 Maintenance

During warranty period, VENDOR shall provide service personnel for periodic fault finding, repair and replacement of all faulty hardware, firmware and software.

During bidding stage, Vendor proposal shall include the details and costs of all standard maintenance services available after SAT. COMPANY shall be under no obligation to select all or any of the agreements detailed and shall be free to negotiate a unique maintenance agreement with the VENDOR.

20 TRAINING

20.1 General

The following training courses are proposed for the selective attendance of suitable personnel such as Engineers, Supervisors and Technicians. The purpose of these training courses will range from gaining practical experience and functional knowledge on ESD system, its software and associated hardware, to acquiring an in-depth knowledge for administration and system configuration and software development purposes:

(a) System Architecture (all)

(b) Systems Software and Maintenance (System Administrator)

(c) System Administration (System Administrator)

(d) Network/Cyber Security (System Administrators, Supervisors)

(e) Application Programming (Engineers, Supervisors)

(f) Advance Programming Techniques (Engineers, Supervisors)

Above training shall be included nominally for 10 Engineers / Supervisors and 6 Technicians.

20.2 Training Course Documentation

For each trainee who will attend a training course, a copy of the complete training course, notes, and drawings shall be provided to COMPANY eight weeks prior to the commencement of the training course. The copies shall be retained by the trainees on completion of the training course and shall be the property of COMPANY.

In addition, five copies of the training course documentation shall be available on site prior to the installation and pre-commissioning for reference purposes.

20.3 Maintenance Training Course

The purpose of the course is to train Engineers/Supervisor/Technicians for first line fault diagnosis, and repair by replacement.

20.4 System Engineering Course

The purpose of this course is to enable COMPANY Engineers/Supervisors to be able to modify system I/O and system application software including interfaces to the PCS. The course shall include:

(a) System Hardware.

(b) System operating software.

(c) Review of project specific typical application software modules, data formats, data table allocations.

21 DOCUMENTATION

VENDOR shall submit the type and quantity of drawings for COMPANY/CONTRACTOR authorization or information as per Supplier Document Register and Schedule (SDRS) provided in Purchase Order.

The VENDOR shall provide all standard and project-specific documentation and software required for system definition, installation, initialisation, operation, maintenance, troubleshooting and training. This information shall provide complete documentation for the ESD in sufficient scope and detail to permit programming and maintenance of the equipment.

Mutual Agreement on document list and documents issue dates shall be an integral part of Purchase Order.

Comments made by COMPANY/CONTRACTOR on drawing submittal shall not relieve VENDOR of any responsibility in meeting the requirements of this specification. Such comments shall not be construed as permission to deviate from requirements of the Purchase Order unless specific and mutual agreement is reached and confirmed in writing.

All drawings, documents, information, correspondence, test reports, operating and maintenance instruction manuals shall be in the English language.

All documents and drawings issued by the VENDOR shall be produced in an electronic format compatible with Microsoft Office computer software. Documentation shall also be provided in Native format, in order to allow company to update during operational upgrade and future projects. VENDOR shall provide final documentation on DVD-ROM with search and retrieval capabilities.

ESD safety related documentation shall conform to IEC 61511-1, clause 19.

All system drawings shall be prepared and submitted in accordance with recognized standards. Every effort shall be made to minimize the total number of drawings prepared by use of common drawings, where practicable without loss of clarity.

Before SAT, VENDOR shall issue As-Built drawings incorporating all changes that have taken place during installation, testing and commissioning at site. Each drawing shall be clearly marked ‘As-Built’ and dated.

The below list of documents required is intended to define the minimum technical documents to be provided by the VEDNOR. This list is not exhaustive and additional documentation necessary for the work execution be provided by VENDOR. ESD system documentation to be supplied by VENDOR shall include, but not be limited to:

(1) System Architecture Diagrams

(2) System Block Diagrams and interface schematic

(3) Functional Design Specifications for Hardware and Software, Cabinets, Networking, Interfaces, Cyber Security etc

(4) System Configuration Specifications including Logic and Application Program Design

(5) Reliability/Availability Calculations and Reports

(6) SIL Calculations as per IEC 61508

(7) SIL and Safety System certification dossiers

(8) Loading Calculations (CPU, memory, networks, power supplies, spares)

(9) Cabinet and Console General Arrangement drawings

(10) Cabinet internal wiring diagrams

(11) Inter-panel Cable Connection Schedule

(12) Interconnection Wiring Diagrams

(13) Input/Output Assignment List

(14) Configuration database

(15) Functional Logic diagrams

(16) Loop Diagrams

(17) Software licenses

(18) Power supply, distribution and earthing drawings

(19) Power and Heat Loading calculations

(20) Electrical Load Schedule

(21) I.S. certification dossier (if applicable)

(22) Bill of Materials

(23) Comprehensive data sheets for all major items, including completed data sheets included in the enquiry/purchase order

(24) Inspection Test Plan (ITP)

(25) QA/QC Procedures

(26) Internal Testing and Pre-FAT Report

(27) FAT Procedure & Report

(28) SIT Report

(29) SAT Procedure& Report

(30) List of all spare parts, tools, test equipment and installation materials

(31) Spare Part Interchangeability List

(32) Packing, Marking and Shipping Procedure

(33) Preservation and Site Storage Procedure

(34) Complete catalogue sheets of all furnished items

(35) System Hardware Manuals

(36) Programming Manual

(37) Application software manuals

(38) System Security Manual

(39) Functional Safety Manual

(40) Operation and Maintenance Manuals

(41) Installation and Configuration Manuals

(42) Quality Manuals

(43) Third Party Manuals

21.1 Specific Requirements

VENDOR shall issue Software Functional Design Specification which details application software, configuration procedures and compliance to IEC 61508 & IEC 61511 programming requirements for safety applications.

Application program files in function block format including all pertinent embedded comments describing logic functionality shall be provided. Descriptors for logic element/blocks shall include completed I/O addresses and tag numbers, set points, logic element parameter identification. Flow charts and Logic diagram drawings shall be produced for all safety interlocking functions and they shall comply with the IEC 61131-3.

This document will be reviewed jointly by the CONTRACTOR and COMPANY and technical review meetings will be held to finalize and freeze the hardware and software prior to the FAT. COMPANY approval of the FDS is mandatory prior to System build and FAT.

The system software functional design specification shall be complete and follow the format given below:

21.2 Typical Program Macros

Typical program macros which are used repeatedly shall have written descriptions of the objectives and functions that are provided. It shall be in sufficient detail to allow a person familiar with individual programming elements of the system to determine the function of each module.

21.3 Detailed Logic Application Diagrams with Full Description

Each separate functional logic group shall be shown as ISA or IEC standard logic symbology, which is fully annotated and described, including all I/O tag numbers. A complete listing of all I/O points with tag numbers, descriptions, point configuration parameters (ranges, engineering. units,) and cross references shall also be included. This documentation may be generated by the actual programming software if the format is reviewed and approved by the CONTRACTOR and COMPANY. It shall include all logic functionalities, equations, calculations, scaling required for each functional logic group. Clear demarcation of each functional logic group shall be provided within the documentation.

22 GUARANTEES & WARRANTY

VENDOR shall provide warranty support for a period of two years, commencing on the date of COMPANY written acceptance of the system following the site acceptance test. Warranty shall apply to defective material workmanship and facility design, and/or facility software. Warranty work shall be done at COMPANY local facilities. The cost of diagnostics and/or correction of any warranty items shall be borne by the VENDOR.

The VENDOR will not be required to provide resident maintenance personnel during the warranty period but shall have competent technical personnel available from the local facility within 24 hours, if required by COMPANY.

The VENDOR shall guarantee that the software to be supplied shall be free from errors, for example software/firmware failure to perform function(s) as specified in this specification or COMPANY documentation.

23 PROJECT ADMINISTRATION

23.1 Project Personnel

The VENDOR shall insure that sufficient qualified personnel are always allocated to the project. The VENDOR shall utilize a project team structure to achieve continuity and accuracy of implementation. The VENDOR shall submit for CONTRACTOR'S approval the résumés of all personnel engaged in the project.

It is anticipated that the project team shall comprise at least the following disciplines:

(a) Project Manager (Commercial/Technical) (shall be nominated representative of the VENDOR with responsibility and authority to fully implement the project with technical correctness, on schedule and within the budget).

(b) Senior System Designer (Technical).

(c) Hardware Design (Technical Hardware).

(d) Software Designer (Technical Software).

(e) Test Technician (Technical Testing).

(f) Site Engineer (Installation/Commissioning).

23.2 Project Schedule

The VENDOR shall include with his quotation, a detailed Project Schedule showing the VENDOR'S best estimate of the achievable major schedule milestones.

The Project schedule shall be used as the main progress control document during the implementation of the project. The Project Schedule shall clearly show any 'float' or 'slack' time available together with any freeze dates required by the VENDOR and major milestones for equipment design, manufacture and delivery. The schedule shall clearly indicate required dates for each of CONTRACTOR supplied design data.

The VENDOR may include in the proposal any additional material which clarifies the procedure for implementing the Project Schedule.

23.3 Progress Reporting

The Project Schedule shall be used as the basis for monthly progress reporting, schedule controlling and schedule forecasting. At regular intervals, the VENDOR shall revise the Project Schedule to include the effect of changes and to reflect actual Project Progress.

23.4 Coordination Meetings

Coordination meetings shall be held as required between COMPANY, CONTRACTORS and VENDOR. The agenda for each coordination meeting will be prepared by the VENDOR prior to each meeting. Detailed meeting minutes will be taken by the VENDOR and submitted for COMPANY and CONTRACTORS for approval. An 'action item' log shall be prepared and continuously updated by the VENDOR.

Coordination meetings, to be held either in Abu Dhabi or home office, will be a part of the purchase order scope.

SECTION D

24 DATA SHEETS TEMPLATES

Not Applicable.

25 STANDARD DRAWINGS

Not Applicable.

SECTION E

APPENDIX 1 ESD SYSTEM REQUIREMENTS FOR SPECIAL MECHANICAL PACKAGES

1. INTRODUCTION

For keeping consistency in design and ease of integration, the Mechanical Package Suppliers should preferably use the same safety system hardware as that of the main plant ESD. This design standardisation of Package Safety Systems has following benefits:

(a) Integrated operating interface.

(b) Integrated peer control.

(c) Integrated diagnosis.

(d) Fast data exchange due to direct communication.

(e) Minimize the quantity of spare parts.

(f) Easier and less expensive engineering and maintenance.

(g) Reduce the number of operating personals.

(h) Reduce training requirements and time.

To achieve above, Package Safety System shall utilise PCN and SN of plant PCS and ESD for data transfer and system integration.

Package Units ESD system shall comply to this specification and additional functional requirements specified in the following sections.

2. HIGH INTEGRITY PRESSURE PROTECTION SYSTEM (HIPPS)

The function of HIPPS is to prevent over pressurisation in equipment or pipeline by shutting off the source of the high pressure before operating pressure exceeds design pressure and thus preventing rupture of equipment or pipeline for personnel and environment safety.

The HIPPS is an instrumented safety system consists of:

(a) Redundant pressure sensors, typically in a 2oo3 arrangement, that detect the high pressure.

(b) Final control element (fail safe shutdown valves or relays in case of tripping compressors and pumps).

(c) The Logic Solver in a redundant architecture.

The HIPPS shall be designed to:

(a) Standalone SIL 3 certified system as per IEC 61508 and IEC 61511.

(b) Entire system Response time shall be less than 0.5 x process safety time.

(c) Be as simple as possible, complex design shall be avoided.

(d) Be fail safe, therefore sensors, signals, logic solvers and final elements shall be designed to be fail safe.

(e) Permit on-line testing without reduction of trip integrity.

(f) Provide Fault diagnostic capability.

2.2 HIPPS Logic Solver

The following minimum requirements:

(a) Logic solver shall PES or Solid-state type and SIL 3 certified as per IEC 61508.

(b) 2oo3 voted HIPPS process pressure sensing elements shall be connected to three separate HIPPS logic solver input cards.

(c) Discrepancy monitoring and alarm between the three (3) analogue sensor values shall be implemented.

(d) Separate HIPPS logic solver input cards from other inputs that influence 2oo3 voting for example process sensor isolation valve limit switches.

(e) Where a SIF has more than one final element or dual trip circuits (for example two solenoid valves) these shall be allocated across 2 or more HIPPS logic solver output cards.

(f) Trip thresholds (set points) shall be locked to prevent adjustment through human error.

HIPPS Logic Solver shall be installed in a dedicated cabinet. In general HIPPS cabinets shall be installed inside equipment room or shelter in environmentally controlled atmosphere. For limited cases where locations are remote and equipment room is not available, the cabinet can be installed in field with prior approval from COMPANY.

For outdoor installation, panel design shall be such that it is:

(a) Suitable for the required hazardous area classification.

(b) Easily accessible.

(c) Suitable for the environmental conditions.

(d) Safe to operate.

Following status monitoring shall be available on HIPPS Logic Solver cabinet:

(a) Transmitter fault.

(b) Transmitter in test mode.

(c) Transmitter deviation.

(d) HIPPS shutdown activated.

(e) Valve open permissive.

(f) Shutdown valve open/close.

(g) Powers supply fault.

(h) Common fault.

(i) Valve testing activated

Following control facilities shall be available on HIPPS Logic Solver cabinet:

(a) System Reset.

(b) Lamp Test (Ongoing/Completed/Failed).

(c) Valves open/close.

(d) Valve Test.

HIPPS trip and fault signals shall be hardwired to PCS and ESD. HIPPS monitoring data shall be transferred to PCS on Modbus TCP/IP data link.

2.3 HIPPS Pressure Sensors

The field sensing side shall employ 2oo3 architecture to activate pressure isolation.

Pressure sensors shall be analogue 4-20 mA loop powered. HART communication protocols shall be used for diagnostic purposes. Transmitters shall have hardware switches or jumpers to lock the write protection.

Each HIPPS transmitter can be tested individually by means of a transmitter test interlocking with limit switches on the Double Block & Bleed Valve located in the field. If one of the three transmitters are in maintenance mode with block valve closed, the 2oo3 voting will degrade to 1oo2 voting.

2.4 Other Requirements

The HIPPS valves shall be highly reliable, fast acting and fail close type. Valve shall be SIL rated as per SIL class specified in Valve Data Sheet.

The HIPPS design shall enable the periodic testing of individual sensors and final elements. This shall include methodology and test facilities to achieve HIPPS activation and repeatable response time measurement with adequate resolution and automated recording of results to provide test traceability.

The complete HIPPS design, manufacturing, installation and testing shall be subject to third party verification to demonstrate compliance to SIL 3 reliability and availability requirements as per IEC 61508 & IEC 61511. The SIL Verification program is in VENDOR scope, performed by a specialised independent third party approved by COMPANY.

3. BURNER MANAGEMENT SYSTEM (BMS)

The objective of the BMS is to ensure the safe operation of fired equipment like boiler, furnace or fired heater. The system design shall include all those factors that contribute to the start-up, operation and shutdown of the unit in accordance with EN 298 & 746 and NFPA 85, 86 & 87 as well as applicable local, national or international codes.

The major checks to be carried by BMS shall include checking fired equipment self-protection during start-up, pre-purging, pilot ignite, main burner ignite, verify air/fuel ratio according to the load demand, trip burner on abnormal conditions and post-purging after burner stop.

BMS design shall provide the functional sequences and timing logic necessary for furnace safe start-up and shutdown.

BMS shall perform following functions as a minimum:

(a) Prohibit start-up of burner unless all permissive are healthy.

(b) Prevent firing unless furnace purge has been completed.

(c) Control fuel valves opening and closing during start and stop sequences.

(d) Ignition of pilot and main burners at light-off.

(e) Control air/fuel ratio according to heat load demand.

(f) Take Shutdown of furnace if flame loss or any abnormal condition detected.

(g) Execute Master Fuel Trip (MFT) upon certain adverse process operating conditions.

(h) Interface with Local Control Panel adjacent to fired equipment.

(i) Interface with plant PCS to control BMS operations via PCS OWS.

The BMS control, safeguarding and sequential functional logic shall be implemented using PLC based fault-tolerant, fail safe and SIL 3 certified system identical to Plant ESD System.

BMS will be integrated into the COMPANY's Integrated Control and Safety System (ICSS) so that it will have seamless interface with PCS for displaying and controlling BMS start/stop sequences from PCS OWS. Additionally, BMS cabinet shall be also provided with integral HMI which shall be used during BMS testing, commissioning and subsequent maintenance of the BMS PLC.

BMS interface with plant PCS and OWS shall be on dual redundant Process Control Network (PCN).

BMS interface with plant ESD shall be on dual redundant fault tolerant SIL 3 certified Safety Network (SN).

If BMSs are in duty/standby arrangements, they shall have segregated processors, I/O systems and cabinets/chassis, allowing each system to have individual turnaround. If major equipment has any parallel equipment downstream it shall be assigned to different nodes/chassis of the same controller.

Following conditions as minimum shall initiate a Master Fuel Trip burner shutdown:

(a) Loss of all flames.

(b) Burner fuel gas/oil header pressure low low or high high.

(c) Furnace pressure high high or low low.

(d) Main gas or oil fuel header valve position fault.

(e) Combustion air flow low low.

(f) Instrument air header pressure low low.

(g) Draft Fan(s) tripped.

(h) Actuation of manual Master Fuel Trip from Local Panel or CCR Console pushbutton.

In the event of Master Fuel Trip condition, BMS shall execute following actions:

(a) Close all fuel gas/oil header safety shutoff valves and open vent valves, as applicable.

(b) Close all burner fuel gas/oil safety shutoff valves and open vent valves, as applicable.

(c) Close ignitor gas header safety shutoff valves and open vent valves.

(d) Illuminate appropriate shutdown lamps and initiate alarms.

(e) Return system to the pre-purge state.

(f) De-energize all ignitors.

BMS design and control requirements shall be solely Package Supplier responsibility to meet Fired Equipment guarantee for safe operation, however following functional requirements shall be considered as a minimum:

(a) Provide push buttons on CCR console and LCP to initiate Master Fuel Trip (MFT) burner shutdown.

(b) Provide burner stop pushbuttons on CCR console and LCP for manual shutdown of burners.

(c) The interlocks shall be such that it is possible to relight the pilot without shutting down the main flame.

(d) The main flame shall have its own flame failure detector. This device shall be capable of differentiating between the pilot and the main flame. In the event of main flame failure on a single burner heater, both the fuel supply to the main flame and the pilot flame shall be shut off. Where heaters are fitted with more than one burner, failure of the main flame shall result in the isolation of the fuel supply to that burner. All the pilots shall remain a light.

(e) If a burner fails to ignite within the prescribed period, then the main burner shut off valves should close and a period sufficient to disperse any accumulation of un-burnt gas shall elapse before a further ignition attempt is made (on any burner in the heater).

(f) If the failure to ignite is the result of the loss of combustion in air, then a furnace pre-purge should be carried out in order to obtain a minimum of 5 volume changes in the furnace.

(g) Individual burner and pilot flame failures shall be indicated on the local panel with repeated alarms to control room. The re-start of the pilot and main flame shall be initiated locally by the operator. Automatic restart is not permitted.

(h) Fuel gas valves shall be of a fail-close design with local electrical reset and shall have a closed position proving switch. Failure of valve to close shall operate an alarm only.

(i) The LCP near furnace shall provide the operator with all the necessary pushbuttons and indicators required to control various operations like purge, pilot/burner light-off, shutdown.

4. HYDRAULIC SAFETY SHUTDOWN SYSTEM (HSSS)

The wellhead control panel shall be used to control the oil or gas producing well Surface Safety Valves (SSV), Downhole Valve (DHV), Wing Valve (WV) and open lift gas Shutdown Valve (if applicable) by applying pressurized hydraulic oil (pressure to Open). The oil pressure shall be generated by an electric motor pump combination with hydraulic oil reservoir generating the required pressure for opening above valves.

The control panel shall be designed as a stand-alone single wellhead control system and shall be totally independent of the flow line fluid using clean hydraulic oil as the operating medium in a closed, leak tight circuit.

The HSSS shall be housed in a completely enclosed stainless steel cabinet with front and back access doors in order to ensure total maintainability of the control system equipment. The front door shall be fitted with a framed window that encloses the operators control panel. All doors and windows shall be provided with handles having padlock arrangement. The Panel shall be mechanically protected to IP 65 according to IEC 60529 as minimum.

The hydraulic control and safety circuits shall be completed with filters, regulators, relief valves, pilots, accumulators, non-return valves, Flow line pilot trip indicators, pressure gauges and other accessories as required for the smooth, trouble free and safe operation of the well. All valves, fitting, tubing, pipe and pipe fittings, and reservoir fabrication shall comply to COMPANY ‘Instruments Tubing, Fittings & Valves Specification’. Control Panel shall be stainless steel 316L and provided with a breather.

When HSSS utilises PES for logic execution, the PES shall be identical to platform ESD System so that it can be easily integrated into platform ICSS. The PES in HSSS shall be SIL 3 certified as per IEC 61508.

For PES based HSSS, one of the following options should be considered for PES location:

(1) **Packaged HSSS:** In this Option, PES shall be installed in separate compartment within the HSSS panel. The Packaged HSSS cabinet shall be the SIS of the Wellhead Tower and it shall have external hardwired interfaces for remote shutdown signal and redundant serial interfaces with PCS for remote monitoring and control. Design of the Control panel and PES shall address outdoor installation related issues such as area classification, ingress protection, harsh environment, H2S presence,

(2) **Separated HSSS:** In this option, PES shall be installed remotely in separate cabinet. All instruments of the HSSS shall be wired to terminal strips inside the cabinet which shall be connected at site to the PES panel by means of multi-core cables.

For Separated HSSS, logic solver could be implemented in plant/Wellhead Tower SIS system as separate SIF function provided that SIL assessment does not consider HSSS and SIS as two independent protection layers.

HSSS shall be configured to carry out the following functions as a minimum:

(a) Hydraulic Pump start/stop based on oil pressure and oil tank level.

(b) Logic for Open / Close wellhead valves.

(c) Remote monitoring (all panel parameters) / control to PCS.

(d) Provide facility to allow local testing of hydraulic pump operation.

Shutdown Push button (Panic Mushroom-button valve Type with red plastic handle) with mechanical protection against accidental access shall be provided in panel front to enable immediate shutdown of the well in case of emergency situation. Remote mounted shutdown Push button shall be provided at adequate distance from the panel for the same function.

On activation of the shutdown command (local shutdown button, Remote shutdown button or remote command from ESD system), hydraulic supply pressure to all valves shall be immediately exhausted through block/bleed circuit and oil shall return to the main reservoir. The return line for the safety valves shall be different from the return line from the control valves (for example choke valves).

The wellhead control system shall allow manual operation of SSV and DHV, wing valves and lift gas shutdown (if applicable) Valves. The controls shall be designed for the fail safe operations.

Opening of the valves shall always be a manual operation either locally or remotely. Under no circumstances shall any of the valves open automatically. The operating sequence shall be designed such that the valves can be opened only in the following order. Control system design (logic) shall ensure that opening sequence is always maintained. Change in the opening sequence shall not be permitted:

(a) DHV

(b) SSV

(c) WV

(d) Open Lift Gas Shutdown Valves (SDV)

Control system design (logic) in the wellhead control system shall ensure that closing sequence of the wellhead towers is always maintained through the following sequence:

(a) WV

(b) SSV

(c) DHV

(d) Close Lift Gas shutdown valves (SDV)

The panel shall incorporate start-up bypass requirements to bypass the low pressure trips. The bypass systems shall be auto reset when the low pressure pilot / trip points have been cleared. Indicators shall be provided at the panel front as well as remote indication at PCS for the status of the High/Low pilots / trips.

HSSS logic shall be designed to ensure that it shall not be possible to open the valves when SIS circuit is unhealthy.

SSV shall close immediately, without time delay. The requirement of the closure of this valve is governed by the following:

(a) ESD push button on the control panel.

(b) Remote ESD actuation.

(c) Fusible plugs actuation.

(d) High or Low pilot actuation on sensing flow line pressure relative to the pressure set points.

(e) Manually closed from the well head control panel.

The DHV shall close only under ESD condition (ESD push button mounted in front of the panel, remote ESD actuation or fusible plugs actuation).

HSSS panel components internal and external shall be tagged and labelled. The exterior name plates shall be colour laminated.

The panel shall be designed to be lifted from the top, by providing four lifting eyes for this purpose.

Electronic compartment shall be totally isolated from accumulation of oil/dust/

The hydraulic control and safety circuits drawing shall be printed on the back-access doors from inside for technician guidance during maintenance.