EMPLOYER	PMC/ CLIENT REPRESENTATIVE	MAIN CONTRACTOR	EPC SUBCONTRACTOR
Ecomar Storage Solutions FZC LLC	MUC Engineering	Intrakat S.A Technical & Energy Projects	Hiap Seng Engineering Limited FZC ENGINEERING SUBCONTRACTOR MOTT MACDONALD

PROJECT: Ecomar Storage Terminal - Phase 1

JOB NO: 220201	DOCUMENT TYPE: REPORT	Page 1 of 30
Date: 15-02-2024	DOCUMENT NO: ESS01-ENG-ICA-RPO-0003	Rev-A

EMERGENCY SHUTDOWN PHILOSOPHY

Rev No.	Date	Description	Prepared by	Checked by	Approved by
A	15-02-2024	Issued for Approval	Anup Sera EM MOTT MACDONALD	Bharat EM HIAP SENG	Sandip GM -PROJ. HIAP SENG

CONTENTS

1 GENERAL

1.1 Introduction

Ecomar Storage Solution FZC LLC is planning to construct a petroleum product storage terminal on the western side of Port of Fujairah and intends to utilize the Port of Fujairah MM2 and VLCC jetties. Intrakat S.A Technical & Energy Projects, the Main Contractor, has appointed Hiap Seng Engineering Limited FZC(HSEL) as the EPC subcontractor for the project "Ecomar Storage Terminal – Phase I" in Fujairah, UAE. HSEL has appointed Mott MacDonald (MMD) as the Engineering subcontractor to provide detailed engineering services.

The Terminal is planned to have a capacity of around 1.3 million cubic meters. Twenty (20) atmospheric product storage tanks will be constructed as part of Phase -1 of the project.

1.2 Purpose of this Document

This document covers the project-specific Emergency Shutdown (ESD) philosophy that is proposed to be implemented in Ecomar Storage Solution FZC LLC and aligns with EMPLOYERS's Major Accident Hazard (MAH) risk management approach.

This document covers the philosophical intent and is not intended to address engineering aspects of hardware systems needed to implement the philosophy.

Instrumentation and control functions shall be developed on the basis of this philosophy and defined on P&IDs, Instrument Index and Cause and Effect Charts for main facilities and package units.

The purpose of Emergency Shutdown (ESD) is to prevent process fluid release, prevent the ignition of that fluid if it is released and to initiate measures to reduce the potential for escalation of fire.

This is achieved by quickly ceasing process operation and by isolating incoming and outgoing flows. ESD achieves these by a combination of actions:

a. Stopping process flow to prevent loss of containment by isolating the storage equipment.
b. Shutting down equipment and systems to bring them to a predefined safe state by executing a set of remedial actions, upon manual or automatic triggering.
c. Preventing ignition by eliminating potential sources of ignition.
d. Isolating and de-energising potential ignition sources that are not classified for continuous operation during any hazardous event, non-Ex rated, or located away from the area of the hazard, but which could be impaired by a major accident hazard.

By carrying out these actions, the ESD system aims to protect personnel, provide protection to the facility, and prevent or reduce the environmental impact from a major accident hazard.

1.3 Definitions

The following definitions are applied for the purpose of this specification:

Abbreviation	Definition
Employer	ECOMAR Storage Solutions FZE
Main Contractor	Intrakat S.A Technical & Energy Projects
PMC / Client Representative	MUC Engineering
Project	ECOMAR Storage Terminal- Phase 1. Fujairah, UAE
EPC Sub-Contractor	Hiap Seng Engineering Limited (HSEL)
Engineering Sub-Contractor	Mott MacDonald Limited (MMD)
Vendor/Manufacturer/ Supplier	The party, which manufacturers/supplies equipment or services for the project.
Shall	is to be understood as mandatory in relation to the requirements of this Specification
Should	is a strong recommendation to comply with the requirements of this Specification

1.4 Abbreviations

The following abbreviations are applied for the purpose of this document:

1oo1	One out of One
2oo2	Two out of Two
2oon	Two out of 'n'
AC	Alternating Current
ACS	Access Control System
AC	Alternating Current
API	American Petroleum Institute
ATG	Automatic tank gauging
AMS	Alarm Management System
ASME	American Society of Mechanical Engineer

ASD	Automatic Shutdown
BS	British Standards
CR	Control Room
DCS	Distributed Control System
ESD	Emergency Shutdown
F&G	Fire and Gas
FACP	Fire Alarm Control Panel
FAT	Factory Acceptance Test
HAZOP	Hazard and Operability study
HSE	Health Safety Environment
IEC	International Electrotechnical Commission
IEEE	Institution of Electrical and Electronic Engineers
IP	Ingress Protection
ICSS	Integrated Control and Safety System
ISA	Instrumentation Society of America
ISO	International Organization for Standardization
LAN	Local Area Network
MCC	Motor Control Centre
MOV	Motor Operated Valve
PLC	Programmable Logic Controller
PIV	Process Interrupt Valve
ROSOV	Remote Operated Shutoff Valve
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SIL	Safety Integrity Level

TCP/IP	Transfer Control Protocol/Internet Protocol
UPS	Uninterruptible Power Supply
WAN	Wide Area Network

2 REFERENCE DOCUMENTS

2.1 Project Reference Drawings and Documents

Document Number	Title
ESS01-ENG-PRS-RPO-0003	Operation Philosophy
ESS01-ENG-ICA-RPO-0002	Control Narrative
ESS01-ENG-PRS-CHA-0001	Process Cause and Effect Matrix
ESS01-ENG-ICA-CHA-0001	ESD Cause and Effect Matrix
ESS01-ENG-ICA-RPO-0001	Instrumentation and Control Design Basis
ESS01-ENG-ICA-DWG-4001	Overall Control system architecture diagram
ESS01-ENG-ICA-DWG-4004	Control room Equipment layout
	All P&ID's

2.2 Codes and Standards

Latest design and engineering of the works shall conform to the requirements of the latest issue of the following standards and documents. In the absence of a relevant code or standard, or when conflict occurs, other equivalent specification or standard may be referred in agreement with ECOMAR.

American Petroleum Institute (API)	
API 520 P1	Sizing, Selection, and Installation of Pressure-Relieving Devices in Refineries Part 1 - Sizing and Selection
API 520 P2	Sizing, Selection, And Installation of Pressure-Relieving Devices in Refineries - Part 2 - Installation
API 521	Pressure relieving and De-pressuring Systems
API RP 551	Process Measurement Instrumentation
API RP 552	Transmission Systems
API RP 554	Process Control Systems- Functions and Functional Specification Development
API RP 555	API RP 555 Process Analyzers
API 670	Machinery Protection Systems

International Electro Technical Commission (IEC)	
IEC 60079-0	IEC 60079-0 Electrical Apparatus for Explosive Gas Atmospheres General Requirements
IEC 60079-1	IEC 60079-1 Electrical apparatus for Explosive gas atmospheres – Flame proof enclosure “d”
IEC 60079-7	IEC 60079-7 Explosive atmospheres Equipment protection by increased safety "e"
IEC 60079-10	IEC 60079-10 Classification of Areas – Explosive Gas Atmospheres
IEC 60079-11	Electrical apparatus for Explosive gas atmospheres – Intrinsic Safety “i”
IEC 60079-14	Electrical apparatus in Explosive gas atmospheres – electrical Installation in Hazardous Area (Other than Mines)
IEC 60079-29-1	Explosive Atmospheres – Part 29-1: Gas Detectors – Performance requirements of detectors for Flammable Gases
IEC 60227	Specification for PVC Insulated Cables of Rated Voltages up to and Including 450/750 V
IEC 60381 Part-1 & 2	Part-1 & 2 Analogue Signals for Process Control Systems
IEC 60529	Degrees of Protection Provided by Enclosures (IP Code)
IEC 61000	Electro Magnetic Compatibility
IEC 61508	Functional Safety of Electrical/ Electronic /Programmable Electronic Safety Related Systems
IEC 61511	Functional Safety-Safety Instrumented Systems for Process Industry Sector
IEC 60331	Fire Resisting Characteristics of Electric Cables.
International Society of Automation (ISA)	
ISA - 5.1	Instrumentation Symbols and Identification
ISA - 5.2	Binary Control Logic Diagrams for Process Operations
ISA - 5.3	Graphic Symbols for distributed Control / Shared Display
ISA - 5.4	Instrument Loop Diagrams
ISA - 51.1	Process Instrumentation Technology
ISA 84.91.01	Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry

3 ENVIRONMENTAL CONDITIONS

Please refer to below table for the seismic/climatic data.

S. No.	Element Description	Value
1	Site Location	Fujairah Oil Industry Zone (FOIZ) - near Port of Fujairah, UAE
2	Altitude at Terminal	+22m for Tank farm 1 & 2 +19m for the Buildings / Shelters area
3	Relative Humidity	Average 60-80 % Maximum being 100 %
4	Ambient Temperature	Maximum 50 °C Minimum 12 °C
5	Design Ambient Temperature	Maximum @80 °C for equipment directly exposed to solar radiation. Maximum @50 °C for equipment protected from direct solar exposure. Minimum @7 °C Sub-soil temperature at 1 m depth for underground pipes: Summer 38°C and Winter 13°C
6	Atmosphere	Sulphureous, often contain fine dust and pollutants
7	Rainfall	Rare but possibly heavy Design Maximum intensity of 60mm/hr
8	Wind	45 m/s (3 second gusts at 10m height); typical for general design
9	Seismic Zone	Zone 2A as per UBC Volume 2 1997, Zone factor Z = 0.15 Horizontal acceleration = 0.15g Vertical acceleration = 2/3 of Horizontal acceleration
10	Power Supply	MV Supply 6600V, 50 Hz, 3 Phase LV Supply 400V , 50 Hz, 3 Phase UPS 230 V a.c, 50 Hz

4 UNITS OF MEASUREMENTS

The following units of measurement will be used in the documents.

Parameter	Unit	Abbreviation
Acceleration	Meter per sec per sec	m/s^2
Amount of Substance	Kilogram mole	kg-mol or kmol
Area	Square meter	m^2
Density	kilograms per cubic meter	kg/m^3
Energy - electrical	kilowatt hour	kWh
Flow - liquid	cubic meter per hour	m^3/h
Flow - gas and vapor	normal cubic meters per hour	Nm^3/hr or m^3/h
Heat	kilowatt	kW
Length	Kilometer Meter Millimeter	km m mm
Mass	kilogram	kg
Mass	Tonne	Te or T
Molecular weight	kilogram per kilogram mole	MWT or MW
Pressure	Bar-gauge (or absolute) or kilopascal	barg (or bara) or kPa
Speed (linear)	meters per second	m/s
Speed (rotating)	revolutions per minute	RPM
Temperature	degree centigrade	°C
Time	hour	hr. or Hr or h
Viscosity (dynamic) Viscosity (Kinematic)	Centipoise Centistoke	cP cSt
Volume	cubic meter	m^3

5 EMERGENCY SHUTDOWN – DESIGN CONSIDERATIONS

5.1 Safety Integrity Level (SIL)

The SIL Study and SIL review are proposed to be performed and implemented in line with the latest edition of IEC 61508. The requirements of IEC 61511 will also be considered.

Pipe to pipe SIL analysis is proposed to be done for all ESD loops including the ESD systems, field devices, MOVs and ESD loops of package equipment. The outcome of the SIL study will be considered to assess risks, set safety targets, and define requirements for safety functions.

Logic development will then be carried out.

5.2 Objective

An Emergency Shutdown System shall be provided for facility. The system shall be designed to provide safe emergency shutdown of process and equipment in order to prevent the development of a hazardous condition which may be caused by process upset or an external event, such as fire or gas detection.

For external events such as fire or gas detection emergency shut down is generally initiated by operator except in certain areas specified on PID's where ESD is automatic.

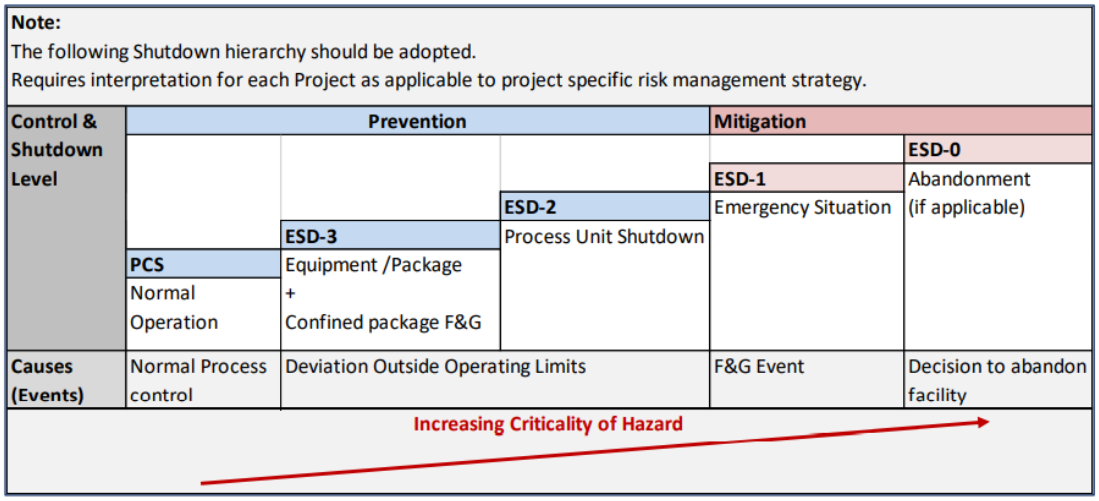
Initiating Contact from other subsystems shall be hardwired to the ESD System.

The purpose of shutdown is to make the elements of the facility safe by isolating a risk (Hydrocarbon inventory).

5.3 Shutdown levels

The overall control and shutdown arrangements shall as per hierarchy indicated in below diagram.

Figure 5.1: Hierarchy of Control and Emergency Shutdown Requirements



The following hierarchy of shutdowns shall be implemented in this project.

- ESD-1: Overall shutdown (Emergency Situation)
- ESD-2: Zone shutdown
- ESD-3: Equipment/Package/Unit or Local shutdown

The highest level shall be ESD-1 should typically be used in response to outdoor fire or gas release events or be initiated manually if emergency action of this scale is required for other accidents. ESD-1 may also be initiated in the event of overall utility failure, to bring the facilities to a known pre-defined safe condition. ESD-1 shutdown shall be initiated by a hardwired manual pushbutton located on the hardwired ESD console in the Terminal Control Room (CR). The corresponding ESD-1 actions are executed by the ESD system, except for the activation of the firefighting system(s) which is through the F&G system.

Emergency Shutdown levels ESD-2 and ESD-3 correspond to process upset conditions or other unconfined (sufficiently well contained) events not immediately a threat to the safety of the facility or of the personnel. These shutdown levels are complimentary barriers to the Basic Process Control System (BPCS).

The main F&G system deals with all fire and gas detection. ESD-2 and ESD-3 shutdowns generally provide protection against equipment or process upset conditions and should normally only be automatically initiated by plant monitoring devices.

ESD-2 shutdowns provide protection against certain critical process or utility upset conditions and might be automatically initiated by process monitoring devices.

Manual initiation shall be available for ESD-2 and ESD-3 shutdowns from the ICSS operator workstations in the control room (CR) and automatically when required by the Cause and Effect (C&E) and the system architecture. Shutdowns can also be activated manually when specified on the P&ID's and according to the Cause & Effect by:

- Local field switches located near the equipment or in the unit.
- Switches located on the package panel in the field.
- Pushbuttons on the Hardwired ESD console matrix panel

5.4 Shutdown Logic

5.4.1 ESD-1 (Emergency Situation) Overall Shutdown

ESD-1 shutdown is defined as the highest level and is initiated manually in the event of a major emergency requiring isolation of all potential electrical sources of ignition.

ESD-1 shutdown shall be initiated from

- Manual push buttons located at the main control point for the facility (Hardwired ESD Console matrix panel)
- Manual push buttons located at the POF area (Hardwired)
- Soft push button on the HMI in the ICSS (may be on separate screen to avoid inadvertent ESD)

Actions

ESD-1 shutdown should initiate the following actions:

- Shutdown and isolation, of all facilities and MOVs & Boundary MOVs, POF boundary MOV's, Manifold Boundary MOVs, Berth Valves and stop all rotating equipment's
- Shutdown all Package equipment's
- Provide audio visual annunciation (field and terminal control room)
- Fire pumps which are already running should continue to operate.
- Alarm to POF Control room.

5.4.2 ESD-2 Zone Emergency Shutdown

The purpose of ESD-2 is to contain any Major Accident within the 'Fire Zone' of the initiating event. This shall be done by appropriate isolation of process sections relevant to the affected Fire Zone.

There is one ESD-2 for each fire zone within the restricted area and it is the highest level of shutdown within the Fire Zone.

All hydrocarbon flows within the Fire Zone shall be stopped and hydrocarbon inventories blocked in. As fire and gas detection leads to different actions, the ESD-2 shall be further split into ESD-2/F for a fire detection case and ESD-2/G for gas detection cases covering ESD-2 within the Fire Zone.

The ESD-2 shutdown shall be initiated by:

- Cascade activation by ESD-1
- Manual push buttons located at new terminal control room (Hardwired ESD Console matrix panel)
- Manual push buttons located at strategic points around the facility.
- Automatically from the F&G system, as determined by the risk assessment.
- Automatically on loss of selected essential utilities (e.g. electrical power)
- Automatic overfill prevention system (AOPS) activation.

Note that confirmed gas detection outdoors in a given Fire Zone may not require immediate isolation of essential equipment in the non process area building (Substation & VFD building, Administration and Control building), if HVAC systems are designed to have gas tight dampers.

Gas detection in the HVAC inlet shall isolate the dampers and put the HVAC system into shutdown/ recirculation mode if feasible to avoid ignition by unclassified equipment.

If re-energisation is required, this shall be achieved by complete isolation from the power feeder, including battery charger.

Actions

ESD-2 shutdown should initiate the following actions:

- Activates ESD-3 of all units, process, and utilities systems, within the fire zone.
- Close all Fire Zone boundary MOV's.
- Close Berth Valve.
- Initiate the ESD-3 of the hydrocarbon units located outside the ESD-2 fire zone, which send hydrocarbons to the ESD-2 fire zone.
- Activation of audible alarm and visual signals for personnel to escape from fire zone and to assembly point.
- Provide audio visual annunciation (field and terminal control room)
- Provide audio visual annunciation to POF control room.

5.4.3 ESD-3 Equipment/Package/Unit or Local shutdown

The aim of this ESD-3 is to shut down an individual equipment or package within a given unit in response to process upsets and local F&G events related to equipment /package.

ESD-3 shall put the relevant equipment in a safe state and provide an opportunity for manual intervention to prevent escalation to a higher shutdown level (ESD-2 or ESD-1)

In some cases, equipment can have different ESD-3 sequences depending on the tripping fault. Where fire and gas detection lead to specific and different actions, ESD-3 of an equipment may be further split into ESD-3 (Fire) for fire case and ESD-3 (Gas) for gas detection.

There shall be one ESD-3 for each process or utility equipment within a unit.

Typical initiation methodologies are:

- ESD-2 of the unit.
- Manual initiation through push button
- For prime movers and machinery, manual initiation (push button) from a local panel.
- Trip of a process or utility operating parameter (excursion outside operating limits).
- Fire or gas detection inside an equipment enclosure.

Actions

- Close specific ESDVs for isolating the equipment.
- Stop motors.
- Initiate package shutdown
- Provide audio/visual annunciation (field and control room)

Upon fire detection inside an enclosure, activates firefighting means in the equipment enclosure and closes dampers.

6 EMERGENCY SHUTDOWN SYSTEM

6.1 ESD system for the terminals

An Emergency Shutdown System (ESD) is proposed to be provided in the terminals to take independent action and to maintain the plant processes in a safe state when the plant Basic Process Control System (BPCS) 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 such as Motor Operated Valves (MOV) , ESD MOVs etc. and stopping rotating equipment machinery such as pumps of plant.

ESD System Logic Solver shall be Programmable Electronic System (PES) based and certified for SIL2 as per IEC 61508. All logic solver hardware components, system software and application software shall be TÜV (or Equivalent) certified for SIL 2 applications.

The ESD system panels/cabinets are proposed to be located inside Marshalling room at new terminal in the Administration and Control building.

Alarms and actions shall be displayed on the common ICSS Operator workstations. Emergency shutdown (ESD) push button stations are proposed to be provided for the entire facility at strategic locations as identified in the P&ID's and layouts. These ESD pushbuttons shall be hardwired to the ESD system. Audio visual indications will be provided for operator attention thought out the plant including remote locations such as POF & existing Ecomar Terminal, Tank farms, manifolds, pump stations and in Control room.

An Emergency shutdown Matrix console will be provided inside the Control room which will have emergency pushbuttons, illuminated lamps, reset push buttons, bypass, Maintenance override switches (MOS) etc as required.

6.2 Automatic Overfill Prevention system

The Automatic Overfill Prevention System (AOPS) for the storage terminals is proposed to be implemented in the ESD system.

Independent level switch at AOPS level as initiator will be considered and will be hardwired to the ESD system. In case activated will close the MOV's of the respective tank and shutdown corresponding running pumps.

The level switch shall be SIL rated in accordance with the SIL study and verification report.

6.3 Terminal to Ship/shore communication

Communication between new Terminal ICSS and POF control system shall be via dual redundant fiber optic cable. However all operations e.g. ship loading/unloading, stripping, and pigging etc. shall be performed based on manual communication between Terminal and POF operator.

6.4 Typical ESD Cause and Effect

The following typical Emergency Shutdown (ESD) cause and effect chart is being proposed for the terminals.
Refer Annexure-1.

7 BASIC ENGINEERING INFORMATION

7.1 System Overview

The ESD System shall comprise of the following elements:

- Dedicated plant mounted initiating and actuating devices.
- Dedicated ESD system and marshalling cabinets in Marshalling room at new Terminal control building.
- Operators Interface via ICSS Operator Consoles in the new terminal Control Room (CR)
- Engineering Consoles in the new terminal Control Room (CR)
- Alarm Management integral to the ICSS

Measurement devices shall be placed in strategic locations within the plant and package units and equipment's to provide shutdown initiation when process and utility system parameters have reached a status from which they may create a hazardous or inoperable situation if the measured parameter is allowed to deviate further out of an acceptable range.

TUV (or equivalent) min SIL2 certified field devices shall be used for safety function.

Segments of the plant shall be isolated by Electrically driven Motor operated emergency shutdown valves. This should reduce the extent of the plant at risk in the event of upset conditions.

The ICSS Operator Interface shall be housed in the main Control Room (CR). It shall provide manual shutdown of the facility, as well as detailed annunciation of system status on the ICSS Operator Interface. Automatic shutdowns shall be provided as per P&ID's and Cause and Effect charts. Dynamic Cause and Effect including overrides and resets of the ESD System shall be displayed on HMI.

Redundant field initiating and actuating devices shall be provided based on the SIL Study result. Where redundant initiating devices are required, two or three independent instruments shall be provided at the same location, with independent impulse piping and manifold with isolation.

ESD logic shall be arranged for a 2oo2 or 2oo3 voting to initiate a trip. Operation of a single instrument in the group shall cause an alarm only to be displayed. A discrepancy alarm will be initiated if any one of the three devices are in different status and system logic shall automatically degrade to 1oo2. If only two instruments are used for redundancy, a discrepancy alarm shall be implemented to detect that there is a discrepancy; the 2oo2 logic will act as two out of two when there is no discrepancy alarm and as one out of two if there is a discrepancy alarm.

If redundant controlling devices are required, such as two MOVs, the controlling output signals to the valves shall be diversely routed and originate from separate cards.

7.2 General Requirements

Initiating devices and actuators shall be hardwired directly to the ESD System, which shall contain the required monitoring, and control equipment, and shutdown logic. The ICSS Operator Interface shall provide audible and visual annunciation of the status of the ESD System, and manual controls to enable Operator intervention for control, maintenance, and testing.

All ESD initiating devices and actuators, process hook up and their associated connections and circuits shall be dedicated to the ESD System and arranged to operate independently of other monitoring control and alarm systems. Redundant field devices shall have dedicated process tapping point with main isolation valve and process hook up. The ESD System shall be totally stand-alone and shall not rely on communication links for shutdown.

Inputs to the ESD Control logic shall be either analog or digital. Analog outputs shall not be allowed.

Analog inputs will be used as initiating device on process measurements (including permissive differential pressure around On-off valves). Permissive for Reset and Reset Signals between DCS and ESD shall be hard-wired.

Digital inputs are used for ESD Zone shut down switches, sub-system shut down commands from ICSS to ESD, valve limit switches and for shut down signals from package units.

Under normal operating conditions, contacts from initiating devices shall be closed, opening to alarm. Actuating devices shall be normally energized, de-energies to trip.

Analog inputs to the ESD system shall be designed in compliance to the requirements of NAMUR NE43.

In order to maintain safe state for the plant, transmitter fault shall be treated as trip condition. Redundancy/ voting shall be implemented to increase the availability based on the safe failure robustness analysis carried out during the SIL review.

Line monitoring is to be provided for ESD I/O's where the design is energies to trip or not fail safe.

End of Line resistors shall be installed at the field device.

For analog inputs, signal validation requirements as per NAMUR NE43 shall be complied.

Any ESD command will be monitored by the ICSS:

- A field push button is connected to the ESD and its initiation is alarmed in the ICSS.
- ICSS commands such as ESD resets and maintenance overrides shall be sent to the ESD via the Integrated communication network.

7.3 Cascading Effects

Cascade effect occurs when a shutdown in one piece of equipment results in a process upset, causing immediate shutdown of other equipment/systems.

Cascading emergency shutdowns shall be avoided, i.e. any shutdown signal should trip all affected equipment/systems, so that an abnormal situation does not escalate due to the intervention of the ESD System. However, a control instrument may take action to prevent an abnormal situation occurring because of a shutdown.

7.4 ESD Reset

On activation of a shutdown, the logic within the ESD System will latch in the shutdown (de-energized) condition. Zone reset shall be provided on the Matrix panel. There shall be a reset push button (software) for each subsystem and for each. Simple automatic shutdowns will not have resets unless these are identified in the Cause-and-Effect Charts.

The manual reset of the logic only, shall be made at the ICSS Operator Interface in the Control room. This logic reset will only be performed if the shutdown conditions are healthy or by-passed by a start-up override (e.g. low flow trip of a pump).

Manual reset of the field device shall only be provided when specified on the P&IDs. When a local reset is required on a package unit, the alarm message in the ICSS shall indicate this requirement (shut down local reset required).

The ESD reset shall not operate a valve. The local command will not be active if an ESD condition is present. For selected valves, the reset of the logic shall reset the valve operation without involvement of field operator.

7.5 Provision of Trip Initiators and Actuators

Locations of shutdown initiators and actuators shall be as shown on the P&IDs.

7.5.1 Cables

Cables used for ESD service shall be fire resistant as per IEC 60331.

7.5.2 Identification

All initiating and actuating field devices including junction boxes shall be clearly and distinctly identified from other field devices by color and tagging.

7.5.3 Emergency Shut Down Valves

Emergency Shut Down Valves (ESD) are electrically actuated motor operated valves. These MOVs for shutdown application shall have provision to receive hardwired shutdown commands from the safety systems.

The MOV shall be able to close in case of shutdown command from ESD system or loss of emergency signal. MOVs shall be stay put upon loss of power supply.

Valve shall Close under below conditions:

- Automatic initiation when the ESD detects an abnormal condition from a field sensor signal.
- Manually from the ICSS when the control room operator initiates ESD command.
- Manually from a local or a local panel push button.
- Manually from the control room if an operator initiates a Zone shut down.
- Manually from the field when the operator initiates the local shut-down switch mounted on the valve; this switch generally acts only on the valve on which it is mounted.

Valve Return to Normal Position

MOV valves in general shall have reset from ICSS except valves identified during P&ID and HAZOP review shall have local reset/open/close push buttons in the field. Interlock logic reset shall be included in the design for MOVs within the group. All MOV shall have provision to open/close from the ICSS if operating philosophy required and permitted after evaluating proper risk analysis.

7.6 Reliability and Availability

The ESD system design shall aim to maximize reliability and availability of 99.99% with and 8 hours MTTR without introducing a high degree of complexity into hardware or software configuration.

ESD system hardware design shall be modular wherever possible to enable first level maintenance replacement of failed components and to prevent as far as practical the shutdown of a unit when software is changed for another unit.

Making changes to the software shall not lead to shut down of other units and should be possible while the Unit is running.

7.7 Redundancy

In order to maximize system availability without compromising reliability, redundancy arrangements shall be incorporated within those elements of the ESD System which may be subject to common mode failure. For example, the ESD logic control system represents a single point of failure which, in the event of failure, could render the ESD System inoperative, or cause unnecessary shutdowns. No single component failure shall lead to a total system failure.

Where the logic system is based on PLC technology, then as a minimum, redundancy shall be provided. Redundancy within the ESD System shall apply to processors, memories, communication with ICSS and power supplies.

Any failures within the ESD System, which leave the ESD System unable to respond to a valid shutdown, shall be alarmed immediately.

Any failure of the system shall be alarmed with details in the ESD system diagnostics and with common alarm at the ICSS maintenance workstation.

7.8 Interfaces with Other Systems

ESD Interfaces Emergency Shutdown arrangements typically interface or rely upon several other Systems, where the integrity of those systems is critical to the overall management of major accident hazards. Typically, the interfaces include:

- Integrated control and safeguarding system (ICSS)
- Fire and Gas Detection System (F&G). Note that the Fire & Gas system shall be independent of the ESD system and shall not have common components with it, except for the final element, which could have common components e.g. ESD Valve, Equipment Trip, etc.)
- Package Unit Control Panel (if any)
- Motor Control Centre
- MMS (if any)

All interfaces of this nature shall be via discrete volt-free contacts. The ESD System shall monitor normally closed output contacts from the other systems and instruct shutdown via its own normally closed output contacts i.e. all contacts shall be closed in the healthy condition, open to trip.

Additionally, an ESD/ICSS redundant communication link shall be provided. This link shall be for diagnostics, first-out alarm, shut down alarms, reporting from the ESD to the ICSS and for selected commands from the ICSS to the ESD (resets, start-up & maintenance overrides).

Faults or malfunctions within systems, which the ESD System is interfacing to, shall not have an impact on the operation of the ESD System.

7.9 Operator Facilities

Initiation of manual trip for top level outputs (typically Zone shutdowns) from the ESD system shall be from individual push buttons. Push-button contacts (normally closed) shall be hard wired in the ESD System. Push buttons shall be guarded type with a flap in the front side to avoid accidental trips. Push button/switch shall have integrated illumination feedback indication in same PB/Switch as confirmation of action from ESD system.

Start-up bypass switches shall be provided if required for selected groups of inputs, which are in the abnormal state until the process has started. This facility is provided at the ICSS Operator Interface and transmitted to the ESD by the ESD/TAS link. Logic shall only be inhibited for a pre-set time, which will be sufficient to allow process to stabilize. If normal condition is not achieved within this time, the inhibit shall be automatically cancelled, and the ESD logic executed.

7.10 Logic Structure

The ESD logic shall be based on a modular structure comprising of several discrete sub-systems, each one defining the shutdown logic of a discrete section of the process.

7.11 Fault Monitoring and Testing

The ESD System shall include self-test and fault detection systems.

As a minimum the fault detection system shall have at least one method of monitoring and annunciation a basic fault in each of the following:

1. Power Supply
2. Input/Output Circuits and Interfaces
3. Logic controllers, including memories.
4. Voting Circuits

Monitoring hardware shall be kept to a minimum and as simple as possible. Any failure in the monitoring circuit shall be alarmed.

It shall be possible to monitor and test the components comprising the ESD panel while the system is in normal operation.

7.12 First Up Alarm and SER

Overall SER shall be done in the ICSS that shall discriminate alarms with a resolution of one second. Critical subsystems like ESD shall have their own high-resolution SER with native time stamping 1ms or better. The subsystem alarms shall be time stamped and transmitted to ICSS.

A first up alarm for each shutdown logic for each unit shall be provided in the ESD system and displayed in the ICSS. GPS time synchronizing facility shall be provided for the ICSS and subsystems for time stamping of alarms and events. Plant units/ equipment shall be divided into logical groups to arrive at optimum and meaningful SER presentation.

7.13 Maintenance Override Switches (MOS)

MOS facilities shall be provided only for those safeguarding sensors where a back-up indication and an associated means to stop the process are available. Subject to this condition, MOS shall be provided for analog, digital inputs.

MOS shall NOT be provided for:

- MOV limit switches (except where used as permissive and the operator has alternate means to confirm the valve position)
- Rotary equipment protection function inputs received from MMS (if any)

- Rotor equipment with single sensor protection (e.g. vibration switches, temperature elements)
- Outputs
- Manual ESD inputs

For voted inputs (e.g. 2oo2 or 2oo3) a MOS on any one sensor shall force the associated signal into trip (safe) state so that the logic is effectively degraded as negative MOS (to 1oo1 or 1oo2) to maintain the required safeguard.

Maintenance overrides shall be implemented using MOS enable key switches for each process unit/subunit. Individual maintenance overrides shall then be implemented in the ICSS as soft switches and accessible through the ICSS maintenance console. A general password shall limit the access to the use of the maintenance override switch to authorized persons. Only one initiator per equipment or subunit shall be overridden at any time. The ICSS Operator displays shall allow the identification of the inputs that are by-passed for maintenance.

The ESD system shall only by-pass the executive action. MOS override shall not inhibit the alarm function. All bypass status alarms shall be available on the ICSS console.

Once a day at a given time (e.g. 08h00, 12h00 etc.), the ICSS shall generate an alarm for each point for which the maintenance by-pass is on, an alarm record showing all active maintenance overrides shall be printed. COMPANY policy shall be observed regarding the length of time that an initiator can be overridden without a temporary PCR, in any event if this time is exceeded an urgent alarm shall be generated at the ICSS Operator console.

ESD system vendor shall implement the MOS logic as per TÜV-approved.

For the fan vibration switches, requirement of second switch shall be reviewed during the SIL review in view of the equipment availability and criticality.

7.14 Start-up Overrides

Start-up overrides, where required for inputs that are in the trip state until the process has started shall be initiated from ICSS. The command transferred via a Communication link shall initiate an appropriate timed override within the ESD system, which will feedback a start permissive to the ICSS. The logic shall automatically trip the process if the process fails to achieve healthy status within timed period.

7.15 Operational Considerations for Overrides

Operations personnel shall be responsible and authorized to operate MOS functionality. A MOS shall not be used as an Operational Override and theses shall be separate. Before a MOS is activated, all work and permit procedures shall be recorded. The permit procedure shall include a ‘mitigation procedure’ to mitigate the risks while the MOS is activated. The ‘mitigation procedure' shall include checking of a functional back-up measurement, monitoring by the operator in case of pre-alarm from the backup measurement and need for

manual trip. Any overrides carried over from one shift to other shift shall be authorized by a level higher than shift controller.

8 CONSTRUCTION REQUIREMENTS

8.1 ESD System

The ESD system shall be independent by ensuring it is segregated from the process control system, F&G system, and other monitoring systems.

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 SIL2 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 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 61511requirements.

Refer project specific Specification for Emergency Shutdown (ESD) system for detailed information.

8.2 Initiating Devices

Input signals to the ESD System shall be primarily from Smart transmitters monitoring pressure, level, flow, and temperature. Where switches are used in the field, they should be snap acting type arranged such that shutdown initiation is caused by opening contacts.

Where initiating inputs to the ESD system are from other systems, these shall be configured as normally closed contacts that open to initiate shutdown to achieve fail safe design.

Shutdown initiating signals from other systems shall generally be controlled by output circuits from those systems.

- Overall and Zone shutdowns shall be initiated manually using pushbutton(s) located in a hardwired ESD console on the control desk in the main Control Room (CR) and pushbutton(s) located on the front of the ESD system cabinet. Zone shutdowns shall also be initiated by Emergency pushbuttons located in the field.
- System and/or Sub-System shutdowns shall be automatically initiated from the ESD system or manually from hardwired pushbuttons located in the field.
- Each ESD hardwired pushbutton shall have two pairs of contacts. Each pair of contacts shall be wired to the ESD and configured as a 1oo2 voting logic.
- Equipment or Local shutdown shall be able to be initiated automatically by the ESD system or manually via pushbuttons local to the equipment in the field.
- Design of ESD initiators shall be as per the applicable SIL class. Necessary TUV certification shall be provided as required by the SIL class.

8.3 Valve Design

Design of MOV shall be as per the applicable SIL class. Necessary TUV certification shall be provided as required by the SIL class.

8.3.1 Final Elements/Actuators

Outputs from the ESD control circuits shall operate shutdown valves installed in the process piping or trip other equipment (either directly or via relevant control panels).

Shutdown valve actuators are electrically actuated Motor operated valve. The MOVs in shutdown application shall have provision to receive hardwired shutdown commands from the safety systems. The MOV shall be able to close in case of shutdown command from ESD system or loss of emergency signal. MOVs shall be stay put upon loss of power supply.

All on-off shutdown valves shall be fitted with status switches monitoring both open and closed positions wired to the DCS and communicated for status indication at the ICSS Operator facility. Local indication on on-off valve body shall also be provided.

Valve operation shall only be possible if ESD System logic has been reset at the Control Room, and the initiating condition is either healthy or inhibited by Start-up Override in operation.

Interfaces with other electrical equipment/systems shall be via volt-free contacts on interposing relays. Contacts shall be closed during normal operation, opening to trip.

Interface with MCC when powered by the ESD will be 24V DC (relays for outputs and contacts for inputs) and when powered by the MCC will be at MCC voltage.

Control valves shall not be used for ESD Service.

8.3.2 Protection of MOV

MOVs (e.g. battery limit isolation, Fire zone isolation etc.) shall be “fire safe” design as per API 6D, API 609 or API 607 as applicable. Any additional MOV requiring operations under fire condition need to be fire safe and shall be identified during project HSE reviews.

For fire protection and blast resistant requirements are not envisaged for this project.

8.4 Interface with MCC

Signals that need to be exchanged between ESD and MCC are interfaced through interposing relays located in the ESD Cabinet.

Signal from MCC to ESD used for any executive action shall be hardwired and serial communication is not acceptable for this purpose.

8.5 Junction Boxes

Junction boxes associated with the fire safe MOVs shall be either fire proofed or located outside the fire zone.

8.6 Required Utilities for ESD

ESD system performance is dependent on:

- Uninterruptible power (UPS): UPS shall keep the ESD system operational upon loss of main electrical power. In accordance with ISO 13702, the UPS autonomy period shall be a minimum of 1 hour for the Emergency Shutdown (ESD) systems.
- Power supply for Motor operated shutdown valves shall be 400 V, 50hz, 3 Phase with back up DG supply.
- Heating, Ventilation and Air Conditioning (HVAC): HVAC shall be provided to ensure positive pressurization and temperature control of Marshalling room where ESD cabinets shall be placed. HVAC Unit shall be located in a safe area, as any gas leak scenario cause complete shutdown of the HVAC unit.

Annexure-I : Typical ESD Cause and Effect for the terminal

Sr no	ESD initiator	Tank Farm MOV close	Pumps stop	Individual Zone Boundary Valves	Berth ESDV close	Package equipment's	CR Annunciation	Field annunciation
	ESD-1 Level Overall Shutdown							
1	CR Master ESD (Console /HMI) at New Terminal	ALL TF Inlet/outlet /Recirculation MOVs	ALL PUMPS	Yes	ALL MLA	Yes	Yes	Yes
2	Master ESD at POF	ALL TF Inlet/outlet /Recirculation MOVs	ALL PUMPS	Yes	ALL MLA	Yes	Yes	Yes
	ESD-2 Level Zone Isolation							
1	ESD PB at Tank Farm-1 or Control room	Respective TF	Pumps at respective pump station	Respective valves	Yes		Yes	Yes
2	ESD PB at Tank Farm-2 or Control room	Respective TF	Pumps at respective pump station	Respective valves	Yes		Yes	Yes
3	ESD PB at Manifold or Control room	No	All except Diesel Pump	Respective valves	Yes		Yes	Yes
4	ESD PB at POF Manifold or at Berth	Respective TF	Pumps at respective pump station, Ship Pumps [1]	Respective valves	Yes		Yes	Yes
5	Loading arm shutdown signal from Berth	Respective TF	Pumps at respective pump station, Ship Pumps [1]	Respective valves	Yes		Yes	Yes
6	AOPS Level switch High High	Respective TF	Respective Pumps	Yes	Yes		Yes	Yes
7	F&G detection	Respective TF	Respective Pumps	Yes	Yes		Yes	Yes
8	ESD PB at respective package	No	Respective pumps	No	No	Yes	Yes	Yes
9	PLR Low Low Pressure	Respective TF	Ship Pump [3]	No	No		Yes	Yes
	ESD-3 Level Unit/Local Shutdown							
1	Pump Temperature High High	No	Individual Pump	No	No		Yes	No
2	Pump discharge Pressure High High	No	Individual Pump	No	No		Yes	No
3	Pump suction Pressure Low Low	No	Individual Pump	No	No		Yes	No
4	Flow switch on pump discharge- No flow	No	Individual Pump	No	No		Yes	No
5	Tank Level Low Low (actuation is from tank gauging and level switch)	No	Individual Pump	No	No		Yes	No
6	ESD PB at respective packages	No	Respective pump	No	No	Yes	Yes	Yes
7	Pump vibration high high trip	No	Respective pump	No	No		Yes	

CR Central Control Room; PS Pump Station; TF Tank Farm; MLA Marine Loading Arms

[1] For ship unloading operation using on-board pumps of ship, a level 2 ESD on POF or Terminal area will result in closure of Tank inlet MOV and boundary MOV's at terminal and POF area. Ship unloading pumps shall be stopped manually by the operator by Radio communications.

[2] Side entry mixer shall be stopped once the level goes below level at which side mixer is installed and during overload condition, This shall be covered in Process Cause & Effect (Doc No. ESS01-ENG-PRS-CHA-0001).

Also side entry mixer shall be tripped on ESD-1 & F&G scenarios this has been covered in ESD detail cause & effect(Doc No. ESS01-ENG-ICA-CHA-0001)

[3] Ship unloading pumps shall be stopped manually by the operator by Radio communications.