Comment Resolution Sheet (CRS)

Project Name:	**EPC FOR SALT DOMES EXPLORATION (LEACHING FACILITY) AT JEBEL DHANNA AREA**	**Project No:**	**P03430**	**CONTRACT No.**	**4700017112**
Transmittal Ref.:	**TR-P03430-4700017112-IC-0620**	**Comment Code:**	**Approved with comments - resubmit**		
Document Class	**Document No**	**Revision No.**	**Document Title**		
N/A	**03-99-39-1603**	**Rev.B**	**Specification for Integrated Control and Safety System**		

SN	Reference Page/Section	COMPANY Comments Received	EPC CONTRACTOR Response	COMPANY Response / Remarks
1	Rev A CRS Sl. No. 5	1. refer comment in the 12.21 section. 2. Also refer comment in section 16.3	1. Noted & incorporated, refer section 12.21 2. Noted & incorporated, refer section 16.3	
2	Rev A CRS Sl. No. 7	Add requirements and details related to asset management System in ICSS	Asset management system is not in project scope.	
3	Section 12.14.1 & 12.14.3	27" may be considered	Noted & incorporated as 27" LED, refer section 12.14.1 & 12.14.3	
4	Section 12.21.1	Redundant IO to be connected in separate IO cards and in separate racks/chassis. Any pumps or process equipments having configured as A & B process equipments i.e. one in standby mode and other in running mode, then it will be considered as redundant process equipments and hence its IO's to be in separate cards, etc same as redundant IO's.	Noted & incorporated, refer section 12.21	
5	Section 12.34.1	specify at least 09 numbers. ESD-1 for all area and Area wise ESD-2, ESD-3. With area wise rest puh buttons. ESD matrix panel will have lamps (RED and Green) just below each individual push button to show the status	Noted & incorporated, refer section 12.34.1	
6	Section 12.35	cabinets. Redundant server to be placed in separate cabinets	Noted & incorporated, refer section 12.35	
7	Section 16.1	Criticality Rating, Inspection Class and Materials Certification shall be idenfied as Per Doc # 30-99-00-8517-1, Rev-0 for ICSS.	Noted & incorporated, refer section 16.1	
8	Section 16.3	Condition monitoring MMS, System 1 server, FACP, EDG, SCMS, HIPPS, HVAC, etc	Noted & incorporated, refer section 16.3. Please refer design review report (03-99-91-1614), HIPPS requirement is not identified.	
9	Section 16.4	Add a small section on Integrated SAT (ISAT) requirements. ICSS functionality will have to be tested with complete operational interfaces with all other systems and 3rd party systems	Noted & incorporated, refer section 16.5	
AL ASAB Comments Received				
10	-	No comments	Noted	
11			OWS requirement in operation facility is updated based on COMPANY comment on ICSS system architecture, refer section 12.14.4	
			All comments incorporated & document is issued as Rev 1 Issued for construction.	
Rev A Comments				
1	Section 3.3	This document to be added as Appendix	Noted & incorporated, refer Appendix-3	Noted

SN	Reference Page/Section	COMPANY Comments Received	EPC CONTRACTOR Response	COMPANY Response / Remarks
2	Section 3.3	Delete, below showing AGES	Noted and removed, refer section 3.3	Noted
3	Section 3.3	Add: AGES-SP-13-001 Criticality Rating Specification	As per project scope For criticality rating we will follow ADNOC specification Equipment / Material Criticality Rating Doc.30.99.00.8517-1. Instead of AGES, refer section 3.3	Noted
4	Section 3.4	Remove	Noted and removed, refer section 3.4	Noted
5	Section 12.1	Add following details in design requirements :- CPU loading, Memory Loading, Network Loading, Redundancy requirements, Spares Requirements, Cabinet Power Supply Loading, IO segregations, ESD Safety Network requirements	1. CPU loading - added in section 12.1 2. Memory loading - already indicated in section 12.10 3. Network loading - added in section 12.10 4. Redundancy requirement - already indicated in section 12.9 5. Spare requirement - already indicated in section 12.10 6. Cabinet power supply loading - already indicated in section 12.4 7. IO segregation - already indicated in 12.21 8. ESD safety network requirements - already indicated in section 12.22	1. Noted 2. Noted 3. Noted 4. Noted 5. Noted 6. Noted 7. refer comment in the 12.21 section, Also refer comment in section 16.3 8. Noted
6	Section 12.1	ANNEXURE 1_TECHNICAL SPECIFICATION FOR PROCESS PLC SYSTEM ANNEXURE 2_TECHNICAL SPECIFICATION FOR F&G PLC SYSTEM ANNEXURE 3_ICSS SECURITY SPECIFICATION FOR SUPPLIERS ANNEXURE 4_SCOPE OF WORK FOR FDIS ANNEXURE 5_ALARM RATIONALISATION GUIDELINES	Noted & incorporated, refer Appendix-1 Noted & incorporated, refer Appendix-2 Noted & incorporated, refer Appendix-3 Please note that FDIS requirement is not in PROJECT scope as per TB 10. Noted & incorporated, refer Appendix-4	Noted
7	Section 12.1	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.	Noted & incorporated, refer section 12.1	Noted. Add requirements and details related to asset management System in ICSS
8	Section 12.4	System power supply located inside ESD cabinets shall be dual redundant and each shall be capable of supplying 100% system power if other fails	Noted & incorporated, refer section 12.4	Noted
9	Section 12.4	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.	Noted & incorporated, refer section 12.4	Noted
10	Section 12.4	Power supplies shall be replaceable on-line without disrupting the process and without affecting functioning of ESD System	Noted & incorporated, refer section 12.4	Noted
11	Section 12.9.2	CPU battery backup durations to be specified. CPU battery fault alarms to be specified	Noted & incorporated, refer section 12.22	Noted
12	Section 12.9.3	Back up storage capacities and durations for the Back up server has to be specified	Noted & incorporated, refer section 12.33	Noted
13	Section 12.9.3	Historian capacities and durations has to be specified	Noted & incorporated, refer section 12.33	Noted
14	Section 12.10	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.	Noted & incorporated, refer section 12.10	Noted
15	Section 12.10	Communication interfaces and Network Loading shall not be loaded more than 50% at maximum loading after all tyhe systems and the plant start-up.	Noted & incorporated, refer section 12.10	Noted
16	Section 12.10	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	Noted & incorporated, refer section 12.10	Noted

SN	Reference Page/Section	COMPANY Comments Received	EPC CONTRACTOR Response	COMPANY Response / Remarks
17	Section 12.12	Add Section :- 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.	Noted & incorporated, refer section 12.12	Noted
18	Section 12.12.3	For Solenoid or similar higher loads cabling shall utilize terminal boards suitable for 2.5 mm2 or higher size conductor cables.	Noted & incorporated, refer section 12.13.3	Noted
19	Section 12.13.1	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. Preferably 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.	Please note that in our Project all shutdown valves are of hydraulically operated not pneumatic. And hence type H or type 15 will be followed. Accordingly section 12.17 is included to refelect this requirement.	Noted
20	Section 12.13.3	Requirements for Operator CONSOLE Desk for the all the HMI's and desktop Stations/ Monitors Printers etc to be captured. These items should be in scope of Control System Vendors	Please note that this requirement is already specified in section 12.13.4. However we have updated the section as 12.14.4.1.	Noted
21	Section 12.13.3	Cover the requirements for ESD hardwired Mimic or Matrix panel. Hardwired Consoles, F&G Matrix panels etc. Requirements of ESD Push buttons and MOS enable etc.	Noted & incorporated, refer section 12.34	Noted
22	Section 12.13.3	All cabinets should have lamps on the door to indidate the required 230 VAC power On, 24 VDC power On and FAULT Status	Noted & incorporated section 12.13.1	Noted
23	Section 12.14	CAUSE & EFFECT SCREENS NEEDS TO BE CREATED	This requirement is already specified in 12.15 2nd last paragraph	Noted
24	Section 12.14	System Diagonistic screens need to be created as mentioned in the section for diagonistics	Noted & incorporated section 12.15	Noted
25	Section 12.19.1	maximum	Noted & incorporated section 12.21.1	Noted
26	Section 12.19.1	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.	Noted & incorporated section 12.21.1	Noted

SN	Reference Page/Section	COMPANY Comments Received	EPC CONTRACTOR Response	COMPANY Response / Remarks
27	Section 12.19.2	4-20mA, HART compatible, 24VDC powered by the System and load resistance 600Ω nominal.	Noted & incorporated section 12.21.2	Noted
28	Section 12.19.5	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.	Noted & incorporated section 12.21.5	Noted
29	Section 12.19.5	Digital outputs shall be current rated for minimum 0.5 amp for an inductive load per point at 60°C.	Noted & incorporated section 12.21.5	Noted
30	Section 12.25	Add following in section 12.25 All diagonistics alarm requirements to be specified. Power failure diagonistic alrarms to be hardwired. Each and every MCB trip in the cabinets to be loading or fuse failure has to be alarmed in system and shown on System diagonistic screens in SCADA All the requirements such as creation of dedicated diagonistic screens in SCADA has to be specified here. Failure of any component, IO channel, IO card, Relays,Redundancy Network failure, each and every network switch failure in ICSS has to be alarmed and shown on diagonistic pages in SCADA. 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.	Noted & incorporated section 12.27	Noted
31	Section 12.30	We request to add as an appendix and attach :- DOC. No. 30-99-39-0020 ICSS Cyber security Specifications. Because this standard has to be used by ICSS Vendor completely line wise and word wise just as ICSS specifications. Because while taking a quotation/technical offer for ICSS from Control System Vendor we need to take signed and stamped this document too along with ICSS Specifications to avoid conflicts at later stage	Noted & incorporated, Refer Appendix -3	Noted
32	Section 15	We request to add as an appendix and attached Engineering Standard :- Design Guidelines for Alarm Management DOC. No. 30-99-39-0002. Because this standard has to be used by ICSS Vendor completely line wise and word wise just as ICSS specifications. Because while taking a quotation/technical offer for ICSS from Control System Vendor we need to take signed and stamped this document too along with ICSS Specifications to avoid conflicts at later stage. Aslso add this standard in section 3.3 COMPANY STANDARDS	Noted & incorporated, Refer Appendix - 4	Noted
33	Section 20	2015	Noted & incorporated, refer section 20	Noted

SN	Reference Page/Section	COMPANY Comments Received	EPC CONTRACTOR Response	COMPANY Response / Remarks
34	Section 20	Delete "ADNOC ONSHORE Projects Quality System Requirements Doc. No. EP 30.99.97.0006.1 "	Noted & removed, refer section 20	Noted
35	Section 22	Training will be arranged at System vendors Training Center for total of 6 Maintenance Personnel in 2 batches and total of 2 Operations persons in 2 batches because all Company persons cannot be released to attend training at same time System Maintenance Training shall be separate and proper hands on training. Maintenance training will be on dedicated simulators stations for each representative. The purpose of the course is to train Engineers/Supervisor/Technicians for first line fault diagnosis, and repair by replacement. And Operations Training shall be separate. All the training curriculum shall the Salt Dome project specific.	Noted & incorporated, refer section 22	Noted
36	Page no 63	Section 24 . 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	Noted & incorporated, refer section 24	Noted
37			Added additional EWS requirement in operation facility based on COMPANY comment on ICSS system architecture, refer section 12.14.4	Noted
38			Server cabinet requirement is added, refer section 12.35	Noted
Al ASAB Comments Received				
39	Page no 3	Update TOC to include all sections of the doc.	Please note that this is the COMPANY approved template. Hence this comment is not incorporated.	Noted
40	Section 3.3	Confirm if new ADNOC specs are to be used	Please note that these specs are added as per TB-08.	Noted
41	Section 4	Check and confirm refer detailed process design basis	Please note that the environmental conditions were updated based on TQ response (Refer P03430-03-99-83-1033)	Noted
42	Section 9.2	Quantify	Noted and added as Qty. 2 as per Comment received in ICSS architecture	Noted
43	Section 10	include	Noted & incorporated, refer section 10	Noted
44			Document number is updated, hence hold point is removed, refer section 3.5.	Noted
45			All comments incorporated & document is issued as Rev B Issued for approval.	Noted

EPC FOR SALT DOMES EXPLORATION (LEACHING FACILITY) AT JEBEL DHANNA AREA

ADNOC Onshore Contract No.: 4700017112
ADNOC Onshore Project No.: P03430

SPECIFICATION FOR INTEGRATED CONTROL AND SAFETY SYSTEM (ICSS)

					
1	29-May-2023	ARJ	CAV	CAV	Issued for Construction
B	15-May-2023	ARJ	NBH	SKU	Issued for Approval
A	31-Mar-2023	ARJ	CAV	CAV	Issued for Review
REV	**DATE**	**ORIGINATOR**	**REVIEWED**	**APPROVED**	**DESCRIPTION**

THIS DOCUMENT IS INTENDED FOR USE BY COMPANY AND ITS NOMINATED CONSULTANTS, CONTRACTORS, MANUFACTURERS AND SUPPLIERS.

EPC CONTRACTOR: **AL ASAB Gen. Transport & Contracting L.L.C**	AL ASAB GENERAL TRANSPORT & CONTRACTING L.L.C.
ORIGINATOR: **AMEC INTERNATIONAL LIMITED**	wood.

ADNOC Onshore Document No.	: 03-99-39-1603	Revision	: 1
ORGINATOR No:	: N/A	Date	: 29-May-2023
ADNOC Onshore Project No	: P03430	Page	: 1 of 73

SHEETS INDEX AND REVISONS

Rev No.	Section	Revision Description
B	Refer CRS	Issued for Approval
1	Refer CRS	Issued for Construction

Note: Revision Table to be used on Post-IFR Issues

HOLDS

Hold No.	Section	Hold Description

Table of Contents

1 PROJECT DESCRIPTION

1.1 Project Objective

The objective is to design, procure and construct the required facilities to allow the creation of one (1) salt cavern for Murban crude and one (1) salt cavern dedicated for Naphtha with all associated facilities. The capacity of crude cavern is mandated as 1 MMbbl, similarly for Naphtha cavern, the capacity is 1 MMbbl.

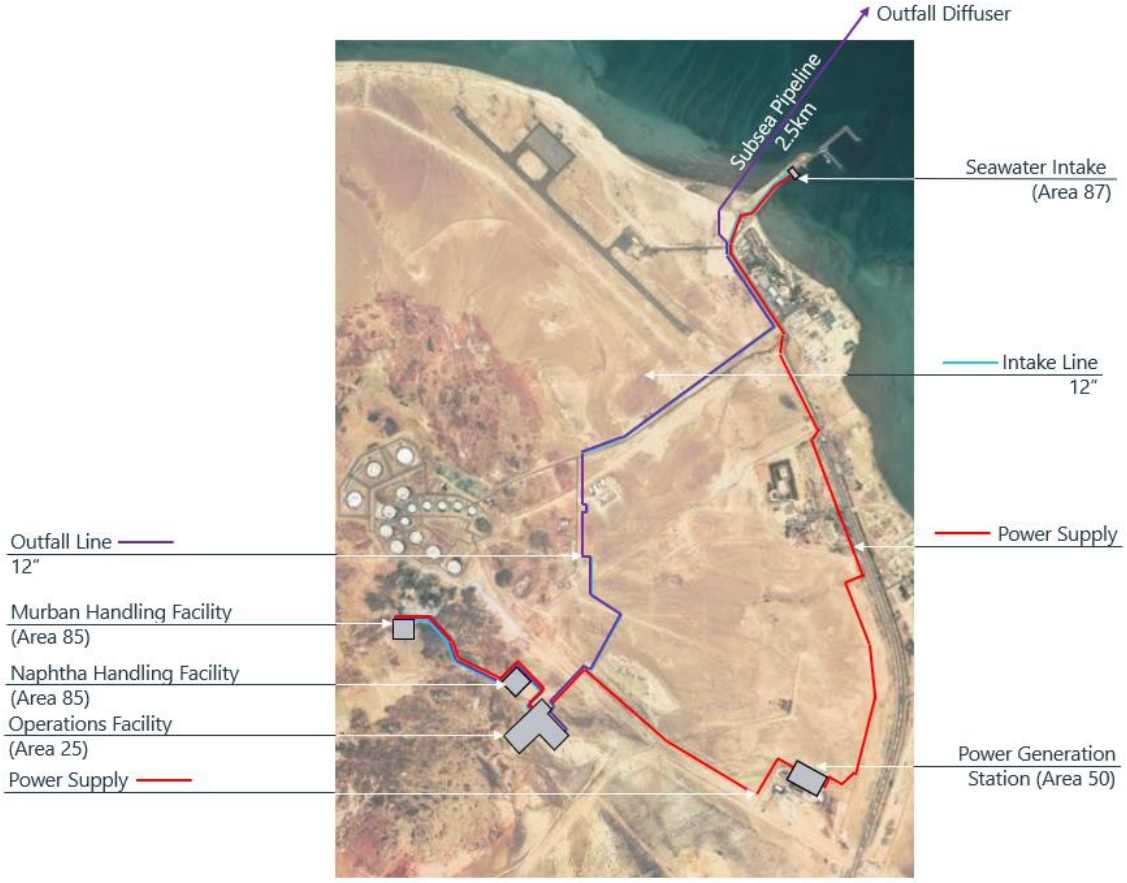


Figure 1.1 – JEBEL DHANNA Aerial picture with the lateral salt dome boundaries

1.2 Project Scope

General scope to meet the project objective are as follows:

- Design and construct leaching facilities to allow the creation of two (2) Caverns or underground storage units in rock salt (by leaching) of Jebel Dhanna with all associated facilities. The storage capacity of Murban crude Cavern crude will be 1 MMbbl, similarly one (1) Naphtha Cavern will have capacity of 1 MMbbl. Total storage capacity is 2 MMbbl.
- Design and construct Leaching facilities so as to form 2 caverns from approx. 1.5 to 2 years, full of brine.
- Create a risk-based design that recognizes and reduces to ALARP the quantified risks of all facilities, layouts, etc.

- HSE:
  - Comply with COMPANY policies on Health, Safety and Environment.
  - Adopt inherently safe design arrangements.
  - To minimize life-cycle operating costs (OPEX).
- Design and construct the surface facilities for a project design life of 30 years for the above ground facilities.
- Design and construct state-of-the-art Installations that meet the requirements of the Project specifications and all applicable codes and standards.
- All design, fabrication, construction and changeover work associated with the project shall be performed in a manner that:
  - Is safe for people, assets and reputation.
  - Minimize the potential damages to environment.
  - To adopt inherently safe designs for all facilities.
  - To adopt simple, robust and flexible processing and utility facilities.

1.3 Purpose of Document

This purpose of this document, in conjunction with the referenced COMPANY specification and standards, SHELL DEPs and other PROJECT documents, is to define the minimum technical requirements for the design, engineering, manufacture, installation, assembly, procurement, material, services, inspection, testing, coating, painting, marking, packing, documentation, pre-commissioning, commissioning and supply of New Integrated Control and Safety System (ICSS) portion of ICSS and its interface with other sub systems and the existing ICSS at BCDS for the project.

Compliance with the specification, codes and standards does not relieve the Supplier of the responsibility for supplying equipment of proper design and construction, fully suitable for all specified operating conditions.

VENDOR shall conform fully to the requirements of this specification and shall provide adequate performance.

2 DEFINITIONS & ABBREVIATIONS

2.1 Definitions

For consistency within this document as well as with other documents, the following definitions shall be followed for the facilities within this project.

PROJECT	EPC for Salt Domes Exploration (Leaching Facility) At Jebel Dhanna Area
COMPANY	Abu Dhabi Company for Onshore Petroleum Operations Ltd. (ADNOC Onshore)
EPC CONTRACTOR	AL ASAB General Transport & Contracting LLC

ENGINEERING SUBCONTRACTOR	AMEC INTERNATIONAL LIMITED
SUBCONTRACTOR	The party(s) to whom any part of PROJECT has been subcontracted by EPC CONTRACTOR
VENDOR / MANUFACTURER	The party which manufactures or supplies the material / equipment, and / or provides technical documents / drawings and services to perform the duties specified by EPC CONTRACTOR
SHALL	Indicates a mandatory requirement
SHOULD	Indicates a strong recommendation to comply with the requirements of this document

2.2 Abbreviations

A	Ampere
AC	Alternating Current
ADNOC	Abu Dhabi National Oil Company
AGES	ADNOC Group Engineering Standards
AI	Analog Input
ANSI	American National Standards Institute
AO	Analog Output
API	American Petroleum Institute
BOPD	Stock Tank Barrels of Oil Per Day
BWPD	Barrels Water Per Day
CD	Compact Disk
CD-ROM	Compact Disc Read Only Memory
dB	Decibels
DC	Direct Current
DEP	Shell Design Engineering and Practice
DG	Diesel Generator

DI	Digital Input
DO	Digital Output
DVD	Digital Video Disc
EDG	Emergency Diesel Generator
EPC	Engineering Procurement Construction
EPROM	Erasable Programmable Read-Only Memory
ES	Engineering Standard (Specification)
ESD	Emergency Shutdown System
EWS	Engineering workstation
F&G	Fire and Gas
FACP	Fire Alarm Control Panel
FAT	Factory Acceptance Test
FO	Fiber Optic
GA	General Arrangement
GB	Gigabyte
GPS	Global positioning system
HART	Highway Addressable Remote Transmitter
HAZOP	Hazard and Operability Analysis
HMI	Human Machine Interface
HPU	Hydraulic Power Unit
HSSD	High Sensitivity Smoke Detection
HTML	Hypertext Markup Language
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
ICSS	Integrated Control and Safety System

IEC	International Electrotechnical Commission
IFAT	Integrated Factory Acceptance Test
IRP	Interposing Relay Panel
IPL	Independent Protection Layers
IS	Intrinsically Safe
ISO	International Organization for Standardization
LCD	Liquid Crystal Display
LCP	Local Control Panel
LED	Light Emission Diode
MCB	Miniature Circuit Breaker
MMBOPD	Million Barrels Oil Per Day
MMS	Machine Monitoring System
MOV	Motor Operated Valve
MTBF	Mean time between failures
MTTR	Mean Time to Repair
NIS	Non-Intrinsically Safe
OWS	Operator Workstation
PA/GA	Public Address General Alarm
P&ID	Piping And Instrumentation Diagram
PC	Personal Computer
PCS	Process Control System
PLC	Programmable Logic Controller
PVC	Polyvinyl Chloride
QA	Quality Assurance
QC	Quality Control

RAM	Random access memory
RTD	Resistance Temperature Detector
SAL	Security Assurance Levels
SAT	Site Acceptance Test
SCFD	Standard Cubic Feet Per Day
SCMS	Substation control and monitoring system
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIT	Site Integration Test
SNTP	Simple network time protocol
SOE	Sequence of Events
SOV	Solenoid Valve
SPIR	Spare Parts Interchangeability Record
SRAM	Static Random Access Memory
TB	Terabyte / Terminal block
TCP/IP	Transmission Control Protocol/Internet Protocol
UAE	United Arab Emirates
UCP	Unit Control Panel
UPS	Uninterruptible Power Supply
V	Voltage

3 REFERENCE DOCUMENTS

EPC CONTRACTOR / SUPPLIER / VENDOR / MANUFACTURER shall seek clarification in writing from COMPANY in the event of any apparent conflict arising between the Project documents. COMPANY shall determine which document to prevail. Unless otherwise specified in Data Sheets / Specifications. Latest editions including any addendum or supplements or revisions thereto in being at the time of order/award (unless otherwise specified) of the following codes/standard/specifications are applicable.

3.1 Order of Precedence

The design and installation shall be in accordance with the applicable UAE regulations and Company / International standards in the following order of precedence:

- Laws Standards and Regulations of the UAE and the Emirate of Abu Dhabi
- ADNOC Standards and Safety Manuals
- PROJECT Datasheets
- PROJECT Specifications
- PROJECT Deliverables
- ADNOC Onshore Engineering Specifications, Procedures, Amendments / supplements to Shell (DEP) and Standards.
- ADNOC HSE Manual and HSE Risk Management
- SHELL DEP & MESC Specifications (Version 47)
- International Codes and Standards
- Internationally recognized oil and gas industry best practices.

The latest issues of standards shall apply. In the absence of specifications, the best engineering practice shall be provided. In case different standards are applicable, the most stringent one shall be followed.

The following sub-sections include the minimum documents and standards applicable for the Project or for references. However, any conflict within or between the standards and project documents shall be notified to the COMPANY in writing and resolved prior to the starting of the related works.

In case of conflict between documents in the same level of the hierarchy, the most stringent requirement shall apply. In such cases of conflict CONTRACTOR shall provide its interpretation in writing of the most stringent requirement for COMPANY's approval.

3.2 Codes and Standards (Latest Revision)

As a minimum, the materials shall be designed, manufactured, tested and delivered in accordance with the applicable SHELL DEPs, International Codes and Standards that form part of this document as listed below. Note: Unless otherwise specified, latest revision of the codes and standards shall be used together with any amendments / supplements thereto.

Codes, standards and other related documents shall be as per the list tendered below. The listing covers the majority of applicable codes, standards and specification. However, it is not exhaustive. Latest editions of each publication shall be used, together with any amendment / supplement / revision thereto.

The following codes and standards (to be added/deleted as required)

Document Number	Document Title
American Petroleum Institute (API) (Latest Revision)	
API STD 670	Machinery Protection Systems

Document Number	Document Title
API RP 552	Transmission Systems
API RP 554	Process Control Systems
British Standards (BS) (Latest Revision)	
BS 6739	Code of practice for instrumentation in process control systems: installation design and practice
EN 10204	Metallic products Types of inspection documents
International Electrotechnical Commission (IEC) (Latest Revision)	
IEC 60079	Electrical apparatus for explosive atmospheres - All parts
IEC 60189	Low-frequency cables and wires with PVC Insulation and PVC sheath
IEC 60331-1	Tests for electric cables under fire conditions
IEC-60332-1-1	Tests on electric and optical fibre cables under fire conditions
IEC 60381	Analogue signals for process control systems - All parts.
IEC 60529	Degrees of protection provided by enclosures (IP Code)
IEC 60654	Industrial-process measurement and control equipment - Operating conditions – All Parts
IEC 60751	Industrial platinum resistance thermometers and platinum temperature sensors
IEC 60812	Failure modes and effects analysis (FMEA and FMECA)
IEC 61000	Electromagnetic Compatibility (EMC) - All parts.
IEC 61131	Programmable Controllers – All Parts
IEC 61158	Industrial communication networks – Fieldbus specifications
IEC 61326	Electrical Equipment for measurement, control and laboratory use – EMC Requirements
IEC 61508	Functional safety of electrical/electronic/ programmable electronic safety related systems

Document Number	Document Title
IEC 61511	Functional safety. Safety instrumented systems for the process industry sector.
IEC 62381	Automation systems in the process industry- Factory acceptance test (FAT), site acceptance test (SAT), and site integration test (SIT)
IEC 62382	Control systems in the process industry - Electrical and instrumentation loop check
IEC 62443	Security for industrial automation and control systems
IEC 62682	Management of Alarms Systems for the Process Industries
IECEx	IEC System for Certification to Standards relating to Equipment for use in Explosive Atmospheres (IECEx System)
International Society of Automation (ISA) (Latest Revision)	
ISA 5.1	Instrument Symbols and Identification
ISA 5.2	Binary Logic Diagrams for Process Operations
ISA 5.3	Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic, and Computer Systems
ISA 5.4	Instrument Loop Diagrams
ISA 5.5	Graphic Symbols for Process Displays
ANSI/ISA 18.2	Management of Alarm Systems for the Process Industries
ISA 84.00.01	Functional Safety: Safety Instrumented Systems for the Process Industry Sector
ISA 84.91.01	Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry
ISA RP60.1	Control Center Facilities
ISA RP60.3	Human Engineering for Control Centers
ANSI/ISA-5.06.01	Functional Requirements Documentation for Control Software Applications

Document Number	Document Title
ANSI/ISA-50.00.01	Compatibility of Analog Signals for Electronic Industrial Process Instruments
ISA-51.1	Process Instrumentation Terminology
ISA 71.04	Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants
International Standard Organization (ISO) (Latest Revision)	
ISO 3746	Acoustics — Determination of sound power levels and sound energy levels of noise sources using sound pressure — Survey method using an enveloping measurement surface over a reflecting plane
ISO 9000	Quality Management Systems -- Fundamentals and Vocabulary
ISO 9001	Quality Management Systems -- Requirements
ISO 27001	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie (NAMUR) (Latest Revision)	
NAMUR NA 102	Alarm Management
DIN 19234	Measurement and control; electrical position sensors and signal converters used for intrinsically safe two-wire DC systems

3.3 COMPANY Standards Specifications and Code of Practices

Document Number	Rev	Document Title
EM 30-99-95-0004	6	ADNOC Onshore CAD Manual
ES 30.99.39.0020	2	ICSS Security Specification for Suppliers
EM 30-99-95-0006	3	ADNOC ONSHORE Guidelines for Submission of Electronics Documentation
EP 30.99.90.0001	10	Engineering Procedure for Drawing Design and Numbering Systems

Document Number	Rev	Document Title
EP 30.99.90.0024	3	Procedure for Preparation of Vendor's / Vendor's Engineering Drawings and Documents
ES 30.99.00.0001	5	Engineering Specification-Tag Plates for Field & Indoor Equipment
ES 30.99.91.0013	1	Earthing Philosophy
30.99.90.0028	Latest Revision	ADNOC ONSHORE Approved Vendor List
EP 55000/31	Latest Revision	Operations Safety – General
30.99.00.0037	3	Instrument for Measurement & Control
30.99.24.0714	Latest Revision	SPIR Procedure
30.99.37.0013	3	Painting and coating of new equipment
30-99-00-8517-1	0	Equipment / Materials Criticality Rating
AGES-GL-13-001	1	CONTRACTORS QAQC Requirement Specification
AGES-SP-13-002	1	Procurement Inspection and Certification Requirement in Projects

3.4 Shell DEP (Version 47)

Document Number	Document Title
DEP 30.00.60.18-Gen	Human Factors Engineering – Design and Procurement of skid-packaged units
DEP 30.00.60.20-Gen	Human Factors Engineering – Workspace Design
DEP 30.00.60.21-Gen	Human Factors Engineering - Labelling of Facilities, Equipment and Piping
DEP 32.01.20.12-Gen	Operational Technology Security
DEP 32.31.00.32-Gen	Instruments for Measurement and Control
DEP 32.31.09.31-Gen	Instrumentation for packaged equipment

Document Number	Document Title
DEP 32.37.20.10-Gen	Instrument Signal Lines
DEP 32.80.10.10-Gen	Safety Instrumented Systems (Amendments/ Supplements to IEC 61511-1 Including IOGP Report 636)
DEP 33.64.10.33-Gen	Electromagnetic compatibility (EMC)
DEP 32.30.20.11	Fire, Gas and Smoke Detection Systems
DEP 32.30.20.15	Basic Process Control System (BPCS) Application Standards
DEP 33.64.10.10	Electrical Engineering Design
DEP 32.80.10.14	Alarm Management
DEP 62.10.08.11	Inspection and Functional Testing of Instruments
DEP 70.10.90.11-Gen	Spare parts
DEP 30.48.00.31-Gen	Protective Coating for onshore and offshore facilities

3.5 Project Documents (Latest Revision)

Document Number	Document Title
03-99-52-1601	Instrumentation & Control Design Basis
03-99-39-1602	Specification for Package Instrumentation & Control
03-99-91-1610	Control and Safety System Philosophy
03-99-39-1612	Specification for HSSD
03-99-39-1613	Specification for Fire Alarm System
03-99-39-1617	Specifications for MMS System and System One Server
03-99-52-1603	ICSS System Architecture Drawing
03-99-91-1607	Emergency Shutdown Philosophy
03-99-91-1608	Operating & Control Philosophy
03-99-91-1611	Startup and Shutdown Philosophy

Document Number	Document Title
03-99-91-1010	HSE Philosophy
03-99-67-1601	Electrical Design Basis
03-99-67-1616	Architectural Diagram-SCMS (Overall)
03-99-70-1605	FO Network Block Diagram
03-99-70-1602	Overall Telecom System Block Diagram
03-87-52-1628	Instrument Equipment Room Layout - Sea water intake
03-25-52-1632	Instrument Equipment Room Layout - Operation facility
03-85-52-1636	Instrument Equipment Room Layout – Well Pad area
03-50-52-1640	Instrument Equipment Room Layout - Power generation facility
03-50-42-1607	Cause & Effect (ESD) - Power Generation Area
03-25-42-1603	Cause & Effect (ESD) - Operations Facility
03-87-42-1601	Cause & Effect (ESD) - Seawater Intake Area
03-85-42-1605	Cause & Effect (ESD) - Well Pad Area
03-50-42-1608	Cause & Effect Charts (F&G) - Power Generation Area
03-25-42-1604	Cause & Effect Charts (F&G) - Operations Facility
03-87-42-1602	Cause & Effect Charts (F&G) - Seawater Intake Area
03-85-42-1606	Cause & Effect Charts (F&G) - Well Pad Area
03-50-48-1602	Instrument IO Schedule (PCS) - Power Generation Area
03-50-48-1603	Instrument IO Schedule (ESD) - Power Generation Area
03-50-48-1604	Instrument IO Schedule (F&G) - Power Generation Area

Document Number	Document Title
03-25-48-1612	Instrument IO Schedule (PCS) - Operations Facility
03-25-48-1613	Instrument IO Schedule (ESD) - Operations Facility
03-25-48-1614	Instrument IO Schedule (F&G) - Operations Facility
03-87-48-1602	Instrument IO Schedule (Pcs) - Seawater Intake Area
03-87-48-1603	Instrument IO Schedule (ESD) - Seawater Intake Area
03-87-48-1604	Instrument IO Schedule (F&G) - Seawater Intake Area
03-85-48-1622	Instrument IO Schedule (PCS) - Well Pad Area
03-85-48-1623	Instrument IO Schedule (ESD) - Well Pad Area
03-85-48-1624	Instrument IO Schedule (F&G) - Well Pad Area

4 ENVIRONMENTAL CONDITIONS

The following is general guidelines intended to be used in technical specifications of equipment and material design for outdoor installation. For more details refer to project document Process Design Basis Doc. No. 03-99-11-1606.

Temperature and Pressure	
Maximum recorded shade temperature	58 ^{0}C
Average maximum shade temperature	36 ^{0}C
Average minimum shade temperature	22 ^{0}C
Normal minimum winter temperature	12 ^{0}C
Minimum Design temperature	4 ^{0}C
Maximum sun radiation temperature	85 ^{0}C
Average barometric pressure	0.98 bara
Humidity	

Relative maximum humidity @ 43 ^{0}C	95 %
Relative maximum humidity @ 54 ^{0}C	60 %
Rainfall	
Frequency	Infrequent. Once in a year
Average rain fall	25 mm/day
Maximum rain fall	48 mm/day
Highest rate January to April	25 mm in 24 hour
Wind	
Prevailing wind direction	NNW
Hourly Mean Wind Speed (as per BS 6399-Part 2)	26 m/s
Maximum wind gust Speed (3 s Gust) (as per ASCE 7-0.5)	44.7 m/s
Mean Speed	8 m/s
Sandstorm	Airborne particles. Saliferous dust and sand. Frequent sandstorms.
Thunderstorms and Lightning	Occur infrequently
Sandstorms	Occurs frequently in desert areas
Surface-soil Temperature	84 ^{0}C (Summer – Directly Exposed) 58 ^{0}C (Summer – Sun Shaded) 4 ^{0}C (Winter)
Sub-soil Temperature at 1 m Below Ground	40 ^{0}C (Summer) 10 ^{0}C (Winter)

Table 4.1 – Environmental conditions

5 UNITS OF MEASUREMENT

The metric system of units shall be used on documents. The following table gives the units that shall preferably be used:

Parameter	Units	Symbols
Length	Meter	m
Actual flow	Cubic meter per hour	m^3/h
	Liter per hour	l/h
Volume	Cubic meter /(gallon)	m^3 /(gal)
Liquid flow (standard)	Barrel per day	BPD
Gas flow (standard)	Million standard cubic feet per day	MMSCFD
Mass flow	Tonne per hour	t/h
	kilogram per hour	kg/h
Pressure	bar (gauge)	barg
	bar (absolute)	bara
Temperature	Degree Celsius	^0C
Density	Kilogram per cubic meter	kg/m^3
Concentration	parts per million by weight	ppm (wt)
	(Pounds per thousand barrels of oil (salt)	(PTB)
	milligram per liter	mg/l
	grams per cubic meter	g/m^3
	Kilogram per cubic meter	kg/m^3
Viscosity (kinematic liquid)	Square millimeter per second	mm^2/s(cst)
Viscosity (dynamic gas)	Milli Pascal -second	mPas (cP)
Corrosion rate	Millimeter per year	mm/yr
Force	Kilo Newton	kN
Power	Kilo Watt	kW

Parameter	Units	Symbols
	Mega Watt	MW
Temperature	Degree Celsius	C
Heavy duty	Million kilocalorie per hour	MM kcal/h
Molecular weight	Kilogram per kilomol	kg/kmol
Velocity	meters per second	m/s
Bit rate	Bite per second	bit/s
Area	Meter square	mm^2 or m^2
Elevation	Meter	m
Time	Hour or Second	hr or sec
Dimension	millimeter	(mm)
Level	meter	(m)
Force and Weight	Kilo Newton or Newton	(kN) or (N)
Mass	$kN.sec^2$ / m or kilogram or Ton	(kg) or (t)
Stress	kN/m^2 or N/mm^2	(kPa) or (MPa)
Moment	Kilo Newton-meter	(kNm)
Frequency	Hertz	(Hz)

Table 5.1 – Unit of measurement

Notes:

- Imperial units shall not be used with the following exceptions:
  - For nominal bore and sizes of piping, flanges and valves.
  - Where required, for code calculations.
  - SCFD and BPD will be given on PFD.
- SCFD, BPD, psi and °F may be added in brackets in general descriptive text.
- Reference conditions are 1.013 bara, 15° C (stock tank condition).
- Gauge pressure shall be referenced from 1.013 bar absolute. Always indicate gauge pressure (barg, psig) or absolute pressure (bara, psia) except for pressure difference (bar, psi) e.g., pump differential pressure.

- Gallon to be read as US gallon (0.0037854 m^3) unless otherwise stated.

6 COMPLIANCE TO SPECIFICATION

Compliance with this Specification, and Standards and documents referenced therein does not relieve VENDOR of his responsibility to furnish units of proper design, workmanship and materials to meet the specified conditions and duties required in datasheets.

Where other Specifications & Standards are referred in this Specification, it is the VENDOR's responsibility to obtain the latest revision of such documents and be familiar with the requirements thereof.

VENDOR's offer is deemed to be in full compliance with all applicable specifications in this project. Any exception or deviation that it is not possible to meet due to technical constraints shall be submitted with appropriate reasons and justification as an itemized list for COMPANY or CONTRACTOR acceptance. VENDOR to note that any deviation NOT listed shall not be considered and VENDOR is deemed to be in full compliance with all such specifications.

7 POWER SUPPLY

The following shall be available:

Power Supply	Remarks
240V, 50 Hz from UPS	Two Feeders (primary & Backup both online configuration) at each location. Further distribution shall be by VENDOR.
240V ± 10%, 50 Hz ± 5% (For Utility)	Two Feeders (primary & Backup both online configuration) at each location. Further distribution shall be by VENDOR.
24 V DC	Shall be derived from 240 V, 50 Hz UPS power Supply within system Cabinets by VENDOR.

Field instruments 24 V DC power and field-mounted solenoids shall be powered by 24 V DC supply from Control System.

The electrical power supply shall be made available at the new power supply skids located in sea water intake area, Murban caverns area, power generation facilities and operations facility.

VENDOR shall state all utility requirements in their tender.

8 ICSS IMPLEMENTATION PHILOSOPHY

8.1 General

All new field instrumentation and F&G devices provided in the following areas as part of the project shall be integrated to the new PLC based Integrated Control and Safety System (ICSS). The PLC shall be SIL-3 certified to handle the control and safeguarding functions as part of project scope.

- Sea water Intake Area
- Operation Facilities Area
- Murban Caverns PAD Area

- Naphtha Caverns PAD Area
- Brine Disposal Facilities Area
- Power Generation Facility

The ICSS shall be PLC based system comprising of common network in star topology for safety and process control based on hierarchies of functionalities and purpose.

All the control and monitoring function of the facilities provided for leaching shall be carried out from new power supply skid provided in Operation facility as part of current project scope.

Interfacing the ICSS at sea water intake area, Murban caverns area & power generation facilities area to the main ICSS at Operation facilities area shall be carried out by ICSS Vendor via redundant FO cables made available by CONTRACTOR. ICSS Vendor shall design, supply and configure the hardware and software such that single point failure of components shall not lead to failure of communication with console and engineering station. All the required hardware/software necessary for the new ICSS shall be supplied by the ICSS Vendor.

The process and safeguarding control unit along with their communication network shall be redundant.

Operator workstation (OWS) & Engineering workstation (EWS) shall be provided at new power supply skid of operation facility for remote monitoring and control of new leaching facilities.

Operator workstation (OWS) shall be provided at Sea water intake power supply skid and local panel mounted HMI in the Murban cavern and power generating facility power supply skids for performing LOCAL operation in case the communication to Operation facility is lost or to perform pre-commissioning / commissioning activities during construction phase.

Vendor packages identified as type P2 shall be controlled & monitored by ICSS, type P3 shall have dedicated PLC based unit control panels for the control, monitoring & shutdown functions. For further details refer project document Specification for package instrumentation & control Doc. No. 30-99-391602.

New ICSS components shall be installed in power supply skids, within safe area and temperature-controlled environment in the following locations:

- Sea water Intake Area
- Operation Facilities Area
- Murban Caverns Pad Area
- Power Generation Facility

8.2 ICSS Control Objective

The Control Objectives shall include the following:

1. Safe operation.
2. Cost effective.
3. Comply with latest, mature, and proven technology.
4. Simple to operate and maintain.
5. High Mean Time Between Failures (MTBF)
6. Meeting the required throughput, within the design envelope of the plant.

7. Flexible and capable of accommodating future modifications, expansions, or upgrades

The following requirements shall be adhered for control systems:

- The availability of the ICSS shall be 99.99%, excluding the downtimes of the FO telecommunication system. All single points of failures shall be removed, where reasonably possible, for critical subsystem components.
- New ICSS/ PLC cabinets shall be provided with independent cable ducts for IS, NIS and power cables. Each panel shall be provided with IS and power earth strips. Each panel shall be provided with cooling fan, heater, illumination and filters.
- The ICSS hardware equipment will be installed in power supply skids, classified as safe, non-hazardous area. The HMI system for local operation will be located in the power supply skid, which are also designated as safe area.
- Redundant Fiber-Optic cables shall be utilized to connect ICSS equipment at different locations. ICSS network shall be redundant and certified for safety and control.
- New control logic shall be developed for this project.

9 SCOPE OF SUPPLY

Following sections defines the minimum scope of supply for new ICSS system. VENDOR shall consider all necessary ICSS system components which are not listed herewith but are deemed necessary for implementation of ICSS as per project requirements.

9.1 Sea Water Intake Area

The ICSS VENDOR scope shall include the following system components as part of project scope but not limited to:

- SIL 3 capable redundant PLC system (segregated I/Os for PCS, ESD and F&G) along with necessary system and marshalling cabinets.
- Network components such network switch, firewall, patch chords etc.
- Common OWS/EWS (1 No.)

9.2 Operation Facilities Area

The ICSS VENDOR scope shall include the following system components as part of project scope but not limited to:

- SIL 3 capable redundant PLC system for ESD and F&G along with necessary system and marshalling cabinets.
- SIL 3 capable redundant PLC system for PCS along with necessary system and marshalling cabinets.
- Network components such network switch, firewall, patch chords etc.
- Redundant HMI Server
- Redundant GPS Time Synchronization Server with GPS equipment's.
- Dedicated OWS (2 Nos.)
- Dedicated combined OWS/EWS (1 No.)

- Backup EWS laptop (1 No.)
- Printers (2 Nos.)
- Servers including SOE, Historian (VENDOR shall review & suggest separate historian server including SOE or combined with HMI server)

9.3 Murban Caverns Area

The ICSS VENDOR scope shall include the following system components as part of project scope but not limited to:

- SIL 3 capable redundant PLC system (segregated I/Os for PCS, ESD and F&G) along with necessary system and marshalling cabinets.
- Network components such network switch, firewall, patch chords etc.
- Panel Mounted HMI (1 No.)

9.4 Power Generation Facility

The ICSS VENDOR scope shall include the following system components as part of project scope but not limited to:

- SIL 3 capable redundant PLC system (segregated I/Os for PCS, ESD and F&G) along with necessary system and marshalling cabinets.
- Network components such network switch, firewall, patch chords etc.
- Panel Mounted HMI (1 No.)

10 INPUTS FOR SYSTEM SIZING

VENDOR shall refer to the following documentation for system sizing including graphics generation and software licenses.

- Instrument Input / Output Schedule
- ESD Cause & Effect Diagram
- F&G Cause & Effect Diagram
- Project P&IDs (Refer Project EDDR for P&ID numbers)

For the document numbers and details refer Section 3.4

VENDOR shall note the following:

- The project Instrument I/O schedule does not include the panels monitoring I/Os (fan fault / high temperature, various diagnostic I/Os etc.) and it is VENDOR's responsibility to capture and include those I/Os in their scope of supply.

11 SCOPE OF WORK

ICSS system shall be designed, engineered, assembled, tested, pre-commissioned, and commissioned to ensure a trouble-free start-up, operation and maintenance of the project facilities. Any hardware / software not listed in this document, but required for the proper functioning and maintenance of the system shall be provided by the Vendor in due co-ordination with COMPANY.

The scope includes but not limited to:

- Project management & reporting
- Site survey & report
- Interface with Third party systems
- Interface and testing with the Telecom equipment.
- Fiber optic interface
- Preparation of a System Engineering document
- Supply of hardware and software, with licenses
- Hardware Design, Configuration, input to loop drawings, manufacturing, and testing of the ICSS and Peripheral Equipment
- Software detailed design, engineering and development including:
    - System sizing, selection of nodes, node configurations, system setup and ICSS network map and definition, Historization capacity, I/O assignment, control schemes and logic schemes, narratives input to CONTRACTOR
    - Functional Design Specification (FDS), Software Design Specification (SDS) and all relevant GA drawings, Wiring Drawings, Loop Details in SPI module for CONTRACTOR to generate Loop Drawings etc.
    - System and Loop configuration
    - System Database generation based on I/O schedule and Functional Specification/ narratives.
    - Graphics generation based upon P&IDs and COMPANY approved HMI Functional Design Specification.
- Factory Acceptance Test (FAT) for ICSS in accordance with an approved procedure including total system integration test (IFAT) with staging facilities for third party system.
- Site Acceptance Test (SAT) after installation of equipment on site in accordance with the approved procedure
- Site Integration Test (SIT)
- System cabling
- Provide consumables and spare parts for construction and pre-commissioning activities.
- Providing supervision and ICSS technical services for the site installation, pre-commissioning and commissioning activities
- Documentation and Training Manuals
- Storage, preservation, packing, transportation and delivery
- Installation and Pre-Commissioning assistance
- Provide start-up and commissioning spares.
- Provide list of spare parts for 2-year operation (filled in SPIR form)
- Provide special tools required for installation, start-up and maintenance.

- Training
- Drawings and documentation including as built.

The Application engineering & project execution shall be carried out from vendor's center of excellence and have adequate, qualified and well-trained resources for local support to the system, that can be deputed to the project and work together with the specialists / experts during application development & FAT, available to assist during commissioning, SAT, up to Project close out.

12 DESIGN REQUIREMENTS

12.1 General

The system design shall ensure that highest reliability and integrity is achieved. The design shall consist of proven hardware and software modules. No project special hardware or software (prototype design) shall be utilized.

Due regard shall be given to the aspects of operability, maintenance and incorporation of future developments in the system design. The design shall take into account the operational needs in both steady and upset plant conditions, including start-up and shutdown.

The effects of all reasonably foreseeable failures shall be considered in the configuration of hardware to minimize the loss of control, monitoring or protection.

Input/ Output modules and controllers shall be grouped such that common failures do not cause dangerous conditions to arise.

A database shall typically comprise tag numbers description, I/O locations, instrument ranges, integrator limits and factors, alarm settings, screen information and trending information for each loop.

Facilities should be provided for initiating manual changeover and monitoring automatic changeover of duplicated equipment.

All controllers shall be redundant. Redundant I/Os shall not reside in the same rack. Power supply to redundant controller racks shall be powered separately via separate breakers and shall be able to be isolated and serviced separately without affecting the I/Os and loops.

System design shall ensure maintenance (e.g., board replacement) and testing to proceed with the minimum disruption to online facilities.

The system design shall provide information processing, display, recording and reporting facilities for the presentation of processed measured data in the formats suitable for management, operations, technical, commercial and maintenance personnel.

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

Refer to “ICSS System Architecture Drawing Doc. No. 03-99-52-1603.

12.2 Hazardous Area Classification

All control hardware equipment’s & HMI system will be installed in the power supply skids, classified as safe, non-hazardo)us area.

12.3 Surge Protection and Electromagnetic Compatibility

The ICSS System offered shall be supplied with provisions for protecting against system errors and hardware damage resulting from electrical transients on power or signal wiring. These transients include those generated by switching large electrical loads, by power line faults and due to lightning strikes, which induce surges on power or signal cables. The IEEE Standard 472-074 shall apply to all system power inputs and signal inputs and outputs from field devices.

The most common sources of electromagnetic radiation are portable handheld radio transceivers. Other sources are fixed radio stations, commutator type electrical devices and spurious sources such as from welders, variable speed drives and contactors. The ICSS System shall be immune from these EMI/RFI interferences. Particular attention shall be given to the immunity of the system to RFI from hand-held radios potentially transmitting a distance of one meter from the cabinets whilst the cabinet doors are open.

The application of EMI/RFI protection components or configurations such as filtering, shielding, minimal physical discontinuities and bonding shall be employed. This includes unit construction and packaging design to ensure easy serviceability and also that the integrity of EMI/RFI features, such as screening will not be degraded during normal maintenance conditions.

The power supply provided to the ICSS System is expected to comply with IEC 61000.

All ICSS System equipment shall comply with IEC 60079.

Vendor shall provide evidence that standard ICSS system components, modules and typical complete systems have been tested in accordance with the relevant sections of IEC 61000, for immunity from supply voltage and frequency fluctuations, and radio frequency interference.

12.4 Power Supply

The power to ICSS system will be supplied from a 240 V AC UPS backed up system. It is the system’s VENDOR responsibility to make necessary provisions within the system cabinets to convert 240 V AC into any other required voltage levels e.g., 24 V DC.

VENDOR shall state all utility requirements in their tender.

In-line AC transient protectors shall be provided to protect all power supply units within the system cabinets.

24 V DC power systems shall operate between 19–30 V DC.

The systems shall be grounded in accordance with manufacturer recommendations. Particular attention is required to ensure that proper grounding of all transient suppressors is achieved using the shortest possible straight path to facility ground.

Circuit protection shall be properly sized to protect system equipment and prevent shutdown.

System power supply located inside ESD cabinets shall be dual redundant and each shall be capable of supplying 100% system power if other fails.

The power supplies shall be designed for 150% of required capacity considering future requirements and derating. Derating due to extreme ambient temperatures or radiation heating shall be considered in the selection of power supplies.

The incoming cables shall be terminated to a suitable sized primary and secondary busbar arrangement and onward to MCBs double pole to feed the 240V AC power to individual controller and or I/O Module, AC/DC power supply units as well as peripheral equipment's ensuring dual redundancy of the 240V AC power source distribution.

The ICSS system shall be supplied with redundant internal power units to feed the redundant electronic components. Each power unit shall be sized for the total load of the input/output field devices. The power used by the system components shall be galvanically isolated from the power used for the field equipment. Furthermore, equipment such as modules that are physically separated from them and connected via the telecommunication system or via the serial data link shall also be galvanically isolated. The minimum isolation must be 1500V peak.

Cabling, fastenings, fittings, screw-heads, nuts and bolts shall be compliant with international standard.

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.

Power supplies shall be replaceable on-line without disrupting the process and without affecting functioning of ESD System.

12.5 Equipment Location

Equipment will be located indoors, within safe area and temperature-controlled environment. Refer section 4 for environmental condition.

Any equipment installed outdoors shall meet the requirements of the Hazardous Area Classification under which the equipment is installed.

12.6 Noise Limitation

The measurement of noise levels shall be carried in accordance with ISO 3746 or an alternative equivalent recognized international standard. The sound pressure level measured at 1 m distance from the control system panel with doors open at any position, shall not exceed 40 dB(A). The control system panel shall be located away from the HMI unit in order to minimize the disturbance.

12.7 Design Life

The ICSS system equipment and components will be suitable for continuous design duty operation for a period not less than 10 years, without the need for a complete system revamp due to technological obsolescence. All the components proposed as part of ICSS System shall be in their preferred zone of the product life cycle management and VENDOR shall ensure technical support and the hardware support for minimum 10 years.

12.8 System Availability

The availability of the ICSS shall be 99.99%, excluding the downtimes of the FO telecommunication system. All single points of failures shall be removed, where reasonably possible, for critical subsystem components.

12.9 System Redundancy

To provide a high level of availability and safety integrity, ICSS shall be implemented on redundant basis.

Following Redundancy shall be considered as minimum:

12.9.1 Common for all Systems:

- Power supply modules.
- Communication interface to ICSS network node.
- 240V AC/ 24V DC power supply distribution to I/O modules, (redundant 24V DC power supply shall be provided with Zener diode circuits to prevent back currents). Panel temperature and power supply status signals shall be configured in ICSS.

12.9.2 PCS:

- PCS internal bus and Control processors.
- PCS communication interface to package control system.
- I/O modules for closed loops and independent protection layer trip and alarms.

12.9.3 ESD / F&G:

- ESD / F&G internal bus and Control processors.
- ESD / F&G communication interface to other systems (e.g FACP).
- I/O modules

12.10 System Spare Capacity and Spares

The system will be supplied with the following amounts of spare capacity as a minimum:

For Hardware (interface/IO cards/slots, wiring, termination and cabinet space):

- 20% spare capacity on interface/IO cards, wired and terminated, ready to configure and use.
- 15% spares supplied for cards, terminations and physical slots available for use, but not installed.
- 25% expansion space capacity provided in cabinets/racks for cards, terminations and termination space in the cabinets, but no hardware supplied.
- 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.

For Systems, Servers/workstations- Hardware, software, licenses etc.

- A Maximum of 30% system memory (RAM) utilization, under maximum load, for all servers/workstations after commissioning. Hardware upgrade space (slots) to install a further 50% memory which the system can use.

- 50% spare storage capacity memory (hard disks), under operation, for all servers/workstations, after installations of all application/system software. 50% additional storage memory up gradable space available for future hot-plug upgrades.
- 100% spare software license capacity available for all application/system software installed, additions of workstations/consoles, ready to configure and use, without the need for additional licenses.
- 50% spare Historization storage space, for all servers having Historization feature built into application/system software, ready to be configured and used.
- Communication interfaces and Network Loading shall not be loaded more than 50% at maximum loading after all the systems and the plant start-up.
- 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

Both hardware and software spares and sparing philosophy above is exclusive of commissioning and 2 years spares supplied by the VENDOR.

Other spares, wherever required, shall be recommended by VENDOR.

12.11 Time Synchronization

The ICSS networks and interfacing workstations/servers, in addition to the Electrical Systems and sub-systems, ESD/F&G systems, UCP/LCPs, and all third-party devices which form a part of the ICSS system across JD SALT DOME project need to follow a standard time reference.

Dual Global Positioning System (GPS) shall be installed at new power supply skid of operating facility to synchronize the ICSS for PROJECT. All components of GPS systems i.e. GPS Antennae, Time strobe generator card, Master time keeper modem, etc. shall be redundant (Main and backup).

Master and backup server/workstation shall be provided at operating facility power supply skid.

12.12 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 utilize 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 SCN communication network via a time signal broadcast on the SCN 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.

12.13 Marshalling and System Cabinets

12.13.1 Construction of Cabinets

Cabinets shall be of the free standing, Rittal or equivalent type.

Cabinets shall house all the equipment such as input/output module cards, controllers, communication interface cards etc. complete with all the relevant power supplies for internal distribution and powering of field equipment.

Cabinet construction shall be based upon proprietary multiple bays housing 19-inch standard rack mounting equipment with a minimum degree of protection to IP42 in accordance with IEC 60529, whilst maintaining adequate ventilation.

Marshalling and system cabinet dimension shall be approximately 800mm (w) x 800mm (d) x 2100mm (h). Both system and marshalling cabinets shall be bolted together and mounted on a common 100mm (h) plinth forming a bay. The length of this bay shall not exceed 1800 mm.

Eye bolts shall be fitted on top of the cabinets for lifting purposes.

Marshalling cabinet shall be utilized for the termination of field cabling and shall have segregated areas for galvanic isolators associated with IS circuits.

Each cabinet shall be provided with adequate lighting, socket outlet, and anti-condensation heater with temperature switch to generate an alarm in the event of high temperature inside cabinet and alarm shall be passed on to ICSS. Fan failure alarm shall also be sent to ICSS for operator attention.

Each cabinet shall be provided with heat extraction fan, louvers and dust filters.

Panel lights shall be LED type with motion sensing operation.

Marshalling and system cabinets shall be constructed steel sheet insect-, weather- and vermin-proof.

The color of the panel shall be RAL 7035. The cabinet shall have front and rear access.

The cabinet shall be provided with door handle and door lockable by means of a common key. Inside door, there should be a provision (i.e., drawing holder) for keeping termination drawing and system document.

The cabinets located within power supply skids shall employ bottom cable entry via cable gland plate with dust sealing. Cable gland shall be predrilled to accommodate all cabling and non-unoccupied shall be sealed. Sufficient free space shall be made available for proper accommodation and termination of the cables.

The cabinet layouts are to allow full and easy access for installation and maintenance requirements.

Suitable cable clamps and supports shall be provided inside the marshalling panel for all incoming cables. Adequate cable connection stress relief shall be provided.

Cable access shall be bottom entry via suitable cable clamping mechanisms.

Separate and isolated cabinets earthing connections shall be provided as follows:

- Safety earth (cabinets and steelwork)
- Signal earth (cable screens and signal common)
- Intrinsically safe earth

Utility power supplies shall be provided from non-UPS supply such as conventional type receptacles, panel LED Lighting etc.

All cabinets should have lamps on the door to indidate the required 230 VAC power On, 24 VDC power On and FAULT Status

12.13.2 Terminal Blocks

A terminal block shall be provided for every core entering or exiting the cabinet and for each wiring splice.

Internal wiring and terminal blocks shall be segregated by voltage level and type as follows:

- AC power
- DC power
- Analog input
- Analog output
- Digital Input
- Digital Output
- Intrinsically safe (IS) signals
- Non intrinsically safe (NIS) signals

All of the connections including the PC boards and the power plugs must be equipped with Locking/latching mechanism.

A barrier shall separate terminal blocks for each type of I/O signal. Terminal blocks for AC power, DC power, and I/O signals shall be separated by a minimum 25 mm space, and preferably should be on separate mounting rails.

Terminal block groups shall be labelled. Each terminal in a group shall be numbered.

Terminal blocks shall be arranged within the cabinet in vertical columns on a steel plate / panel from the cabinet sub-VENDOR.

Every I/O point shall be wired to terminals, including spare I/O points. Wiring from the I/O card to the terminal block shall utilize VENDOR supplied pre-connected multi-core cable.

Every terminal of each I/O point shall be wired to terminal blocks.

The VENDOR'S internal wiring shall be restricted to the system side of the terminal blocks. The VENDOR shall connect no more than two wires to any terminal block. The field side of the terminal blocks shall be kept completely free of any wires and jumpers.

Fused terminal blocks with blown fuse indicators shall be provided for all devices requiring 24V DC power. Each device shall have an individual fused terminal block. Daisy chaining of 24V DC power from device to device shall not be accepted. Fuse terminal shall be KLIPPON SAK SI AFT (or) similar with fuse failure indication.

Other field terminal blocks shall be knife edge disconnect type (KLIPPON or similar) terminal block for field cables.

12.13.3 Wiring and Terminations

Covered PVC ducts/wire-ways shall be provided between terminal blocks for wiring. Ducts/Wire-way loading shall not exceed 30% fill at any point.

AC power wiring shall utilize separate wire-way from DC and I/O wiring.

I/O signal termination shall be able to accept a minimum of 2.5 mm^2 stranded copper with PVC insulation.

Power wiring shall accept a minimum of 4.0 mm^2 stranded copper, 600 V insulation. All power wiring shall be via suitable MCBs and fused terminal blocks with proper labelling of the consumers.

Wire termination shall be crimped solder-less compression spread or pin type insulated terminal lug. Any other type shall be subjected to CONTRACTOR approval. Non-terminated or soldered connections shall not be accepted.

All I/Os including spares shall be fully terminated at TB's.

There shall be and adequate segregation between terminals and cables in the following categories:

- Analog
- Digital
- Intrinsically Safe
- Serial Communication

ICSS VENDOR shall supply all system cabling, including redundant Ethernet switches, up to the fiber optic break-out terminals (i.e., patch panel). Fiber optic cables between geographically separated network nodes will be supplied by others.

System equipment cabinets shall be designed to provide a `cross wiring area' to give maximum flexibility for the assigning signals in the cables to the physical channels on the I/O cards.

ELCO or equivalent connectors and sockets shall be considered for connecting system cables.

All wiring shall be neatly run in vented flame-retardant trunking (i.e., PVC close-slotted ducting with a cover) with segregating between IS and NIS signals and different power voltage levels. Trunking shall not be more than 50% full. No more than one wire shall be connected to one terminal. The trunking shall be as follow:

- Blue for IS signals
- Grey for NIS signals

All the spare wire/ core of the field cable shall be connected to the terminal block. Terminal arrangements shall be such that all single cores, including spares, of multi-core cables can be connected in the same sequential order as the pattern and layout of the cores in the field cable.

No splices or connections shall be made in wire ways or trunking, or in any place other than at terminal strips.

Heat shrink sleeves with permanently printed wire numbers shall be placed at each end of every wire.

Screens shall be connected to instrument earth bar within the Marshalling cabinet.

Wire sizes for internal cabinet wiring shall be according to VENDOR's standard.

Wire colors shall be as follow:

- Analog
  - Black: +ve
  - Blue: -ve
- Digital (potential free contacts)
  - Black: NC / NO
  - Blue: C
- DO (i.e SOV)
  - Red: Line(+)
  - Black: Neutral (-)
- Multicore
  - White: All cores

The interconnecting cabling between marshalling cabinets and system cabinets shall be arranged by VENDOR.

All control wiring shall be carried out using not less than 1mm² flexible multi-stranded, annealed copper conductors and shall be flame retardant to IEC 60332, halogen free, low smoke emission and PVC or PE insulated. Insulation resistance shall be 300V.

Complete segregation between IS and NIS is required and shall be carried out in accordance with EN 50020 /IEC 60079.

For Solenoid or similar higher loads cabling shall utilize terminal boards suitable for 2.5 mm2 or higher size conductor cables.

12.14 Operator/Engineer Workstation Requirements

12.14.1 Operator Workstation (OWS)

The ICSS system shall be provided with Operator workstation consoles to enable view, monitoring and control of the new facilities.

Each manned control center shall be provided with optimal number of local operator workstations to enable proper view, control and operational requirement.

Each operator workstation shall support video adaptors with dual display ports but using only a single keyboard and pointing device.

All Operator station monitors shall use dual 27” LED (TFT) flat panel technology to provide durable, low radiation, low power consumption and low heat dissipation operation.

Groups of operator workstations shall be logically grouped into Operator Consoles for segregation of operations and ease of alarm management and control functions. Each workstation shall be supplied with an integrated Operator’s keyboard. The operator’s keyboard shall have a minimum of 40 user-configurable buttons for configuring trends/graphics/process operation groups/logs and reports.

Each operator station shall have the feature of storing graphic pages in its local memory to enable fast access, reduce graphic call-up time and reduced network loading.

The Operator workstation shall function as the primary HMI interface for carrying out all Operator functions including:

- Call up of Graphical displays of various sections as well as overviews showing the process conditions.
- Call up Trends/groups of selected process variables/control loops etc.
- Call up Process/System Alarm Events displays for alarm management functions.
- Commands and controls access
- Call up system/alarm summaries, logs and reports.
- Call up System maintenance message displays, network status displays, device status displays and other system information, as required.
- Call up Intelligent Cause and Effect displays for the ‘what-if’ analysis.
- Call up ESD Displays (including critical alarms)
- Call up F&G Displays (including critical alarms)
- Call up system diagnostics of the system up to card level & Instrumentation including system malfunction indications.
- Call up Tuning displays.
- Call up sequencing guides.
- Provide status of maintenance overrides, inhibit, and set/reset functionalities for ESD.
- Provide component level system status and I/O fault indication for PCS, ESD and F&G.

The operator interface shall insure that the plant integrity or operability is not affected by the unintentional actions of the operator, for example any soft buttons used for stop / start functions should require two actions (select and confirm).

System faults, including those caused by earth faults shall be annunciated, at the PCS as they occur.

Systems shall not produce executive outputs, capable of disrupting plant operation, in response to 'bad' input signal(s). All bad input signal values shall be alarmed with high priority.

Loss of data communication between OWS and ESD system shall not result in trips or status changes of Safety communication points, recovery of communication shall be automatic.

Various levels of password security systems shall be provided to prevent unauthorized access to system modification facilities.

The ICSS Operator stations shall be provided with the following access levels:

- **Operator access:** This "operation" level shall include the normal operator functions (Auto/Manual command, set point change, alarm acknowledgment, etc.)
- **Maintenance access:** This level aims at testing equipment, and/or modifying software parameters which are not accessible to operator (some PID's action, timer setting, maintenance inhibit, etc.). It shall also provide access to all operator displays and to study all real time system loads/ errors, network loads/ errors, communication path/ packet loss/ status, real time point database counts on each node etc.
- **Engineer access:** This level aims at providing system network maintenance functions and developing & testing software configuration. This "supervisor and configuration" level shall also include all operator and maintenance functions and provide access to study all real time system loads/ errors, network loads/ errors, communication path/ packet loss/ status, real time point database counts on each node etc.

12.14.2 Engineering Workstation

ICSS shall be equipped with engineering station that can be used for performing system configuration/analysis/programming changes directly on the devices and testing these changes prior to actually implementing them live on the systems.

EWS should be furnished with all licensed software applications and maintenance tools necessary to maintain, diagnose, modify, document and configure the system. A full list of all software, engineering tools, together with details of all licensing agreements and restrictions shall be submitted by Vendor. Vendor shall also supply the original software media and licenses.

All software licenses shall be under the name of end user. It shall be possible for the licenses to be transferred to affiliated/operating COMPANY without additional cost.

System shall be capable of self-documenting configuration data in English format directly to printer for hard copy.

Latest version of engineering station available at the time of delivery shall be supplied.

It shall be possible to remotely access all PCS, ESD and F&G system panels from Operation facility power supply skid.

Engineering workstations shall be protected by strict security access levels as well as log on permissions to lock out any unauthorized interventions.

The engineering workstation shall be identical to the operator workstation hardware and shall consist of a single non-redundant machine that is equipped with sufficient memory and disk for performing engineering functions.

Each workstation shall be supplied with an integrated keyboard consisting of engineer's standard 101 programming keyboard as well as operator's keyboard.

This system shall function as the main engineering platform as well as a back-up operator workstation.

The engineering workstation shall have multiple backup capabilities in form of tape drives as well as DVD RW drive installed to allow weekly backups or as required of the complete system.

12.14.3 Minimum hardware Specification for OWS & EWS

Operating System	:	Windows (latest)
Processor	:	Latest (Intel Core i9 or better)
Minimum RAM	:	16 GB or better
Minimum Expandable RAM	:	64 GB or better
Hard Drive	:	1 TB (RAID 1), integral
External Storage Media Drives	:	2 ext. USB + 1 DVD RW Drive
Display Screen	:	27" LED
Display Resolution	:	1280 x 1024 pixels as minimum
Network Interface Cards	:	Two, 10/100/1000 Mbps Ethernet Cards
Integrated Keyboard	:	Standards operators functions with 101 engineering keys
Pointing Device	:	Integral Trackball on Keyboard

12.14.4 Quantity and Location of OWS & EWS

The following are OWS & EWS requirement:

LOCATION	OWS QUANTITY	EWS QUANTITY	REMARKS
Sea Water Intake	1 No. (Refer Remarks)	Refer Remarks	Common OWS/EWS for PLC system
Operation Facility	3 Nos. (Refer Remarks)	1 No. Refer Remarks	Two OWS, One EWS & One EWS/OWS for PLC system and a backup laptop configured as EWS for PLC system

Murban Cavern	Refer Remarks	1 No. Refer Remarks	Panel mounted HMI and a laptop configured as EWS for PLC system
Power Generation Facility	Refer Remarks	1 No. Refer Remarks	Panel mounted HMI and a laptop configured as EWS for PLC system

12.14.4.1 Operator Console and Furniture

VENDOR shall supply the furniture for all the equipment supplied. The furniture supplied by ICSS VENDOR shall be fire retardant.

12.15 Display/Graphics Building Tools

ICSS shall be equipped with an advance graphics display configuration tools and display builder to enable the system support staff and users to build and modify graphics displays and reports. All graphics-loop, trends, overlay, reports shall follow ADNOC ONSHORE philosophy.

Standard graphic displays provide the operator with a standard format for displaying information and are configurable and normally accessible from dedicated function keys. Customized graphic display details a schematic presentation of the plant at different levels, from overview level right through to equipment detail level.

The graphic displays, together with the keyboards shall provide a complete window to the plant for all control and monitoring requirements as per Process P&ID and Packages P&ID.

The real time data within these displays shall be automatically updated without the need for operator action with a configurable refresh rate of four seconds or less.

The following standard type of graphic displays shall be provided and accessible from dedicated function keys:

- Loop (Faceplate) Displays: The loop display shall contain, in engineering units and bar graph format, the process variable, set point and loop output values. In addition, all control and configuration parameters including tuning constants shall be displayed. All adjustable parameters shall be changeable from within the display.
- Group Displays: Predefined and operator configurable group displays shall consist of approximately eight loops displayed in similar format as in Loop Displays. Configuration parameters shall not normally be changeable from within this display.
- Trend Displays: Both historical and real time trend displays shall be available for any variable point. Trend displays shall be able to accommodate at least three different points simultaneously in different colours.
- Alarm Displays: Alarm displays shall contain the alarm summary in chronological order and alarm groups for the configurable plant area/group.
- System Diagnostic Displays: Diagnostic displays shall be specially designed to facilitate system maintenance and shall, as a minimum, list all the system devices, including communication systems and their associated status. System maintenance functions such as module restarts/switchovers, accepting errors, etc. shall be action from this display.

The system shall support a powerful and flexible custom graphic display capability which shall include, as a minimum, the following:

- Hierarchical display relationship for ease of movement

- Display capacity of at least 200 dynamic elements per graphic including calculated values
- Symbolic presentation of data by means of change in colour/shape and/or flashing.
- Configurable data/numeric format including colour
- Unique colour combination display capability for multi-state devices
- Suppression of inactive status messages and/or alarms
- At least two different text/data sizes
- Movement of displays from one screen to another.

Graphics shall follow the recommendations from ASM (Abnormal Situation Management) consortium and EEMUA guidelines.

The system shall support Microsoft Windows technology which shall, as a minimum, provide the following added features:

- Displaying data from other devices connected to ICSS.
- Displaying multiple sets of data on a single screen
- Display resizing, repositioning including reduction to icon size.
- Running other standard software packages such as Microsoft Office etc
- Graphic Displays shall use Web based (HTML) graphic building tool, enabling easy building of graphics and ease of access by local as well as remote operator stations. The Graphic tool shall use system standard as well as customizable building blocks libraries for the graphics displays.

ICSS OWS shall contain custom graphic pages to display the status of all inputs and outputs to / from the ESD/F&G systems in a cause and effect chart format. These graphics shall include a first out alarm display such that the first in a series of trip initiators can be easily identified.

System Diagnostic screens need to be created as mentioned in the section for diagnostics (Section 12.25).

Loss of data communication between ICSS HMI and ESD/F&G systems shall not result in trips or status changes of the safety communication points. Recovery of communication shall be automatic.

12.16 Printer

One number printer (A3 size) shall be the latest, top of the line models proposed by ICSS Vendor and capable of directly being installed on ICSS LANs with its own dedicated IP address.

Printers shall be provided in minimum in the power supply skid of operating facilities.

12.17 Partial Stroke Test

ICSS shall capable of performing PST scheme as indicated as type-H or type-15 in P&ID P03430-03-99-08-1603.

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 ICSS and PST diagnosis software shall be installed on ICSS OWS. Refer to project function specification for Shutdown Valves Doc. No. 03-99-39-1606 for further PST implementation requirements.

12.18 Maintenance Override

Maintenance overrides for F&G and ESD shall be applied by first selecting the maintenance override permissive for the location/group on the respective matrix panel followed by targeting the individual device to be bypassed through OWS. F&G or ESD system will then confirm in the PCS whether the selected transmitter has been bypassed.

ICSS OWS shall provide status of maintenance overrides, inhibits, and set/reset functionalities. Also component level system status and I/O fault indications shall be available on the ICSS OWS.

Maintenance override philosophy shall be as per Shell DEP 32.80.10.10.

Maintenance Override Switches (MOS) may only be provided for IPF sensors if secondary or back-up indication plus an associated means to stop the process are available to the operator.

Therefore, MOS shall not be provided on, for example:

- Single flame sensors
- Manual ESD inputs such as Break Glass Units (BGUs) or Operator ESD Push buttons.

For Fire and Gas Detectors, a voting strategy of 1ooN Alarm and 2ooN trip will be adopted.

A time limit shall be placed on the duration an MOS is active. A timeout alarm should also be considered for the MOS enable switch. The MOS time out alarm shall never cause the MOS to be automatically removed (causing a trip).

MOS activation shall generate a (low priority) alarm in the PCS after 4 hours. If the MOS is not removed the alarm shall be repeated every 4 hours.

A MOS shall not inhibit the alarm function. A MOS can only be activated from Operation facility power supply skid.

A MOS shall be provided for each sensor in 2oo2 IPF configurations. The setting of one MOS shall degrade the logic. During the time the override is activated, the configuration automatically functions as a 1oo2 system (a ‘negative’ MOS).

A MOS shall not be used as an Operational Override Switch (OOS). If an OOS is required and a MOS is permitted, both an OOS and a MOS shall be provided.

12.19 Reset Functionality

Reset facility shall be provided in ICSS HMI. This function shall be enables only after the clearance of the cause.

In ESD, it can be activated when source of ESD has been cleared and ESD system has been reset locally.

The requirement for local resets shall be minimized to facilitate remote operation of the new facility. There will be one hardwired reset button in the operation facility power supply skid for each ESD button. There will be one PCS “soft” reset button for each PCS level 3 ESD.

ESD-1, ESD-2 shall have push buttons in Operation facility Power supply skid. Hence no local push button is required. The Reset Philosophy shall be as follows:

- The initiators shall be normalized (healthy), the operation facility power supply skid hardwired reset button for the applicable ESD buttons shall be activated. And then ESD valves shall be reset from the field.
- Major equipment package ESDs shall be reset via the PCS. Following one unsuccessful start attempt, the safeguarding logic shall lock up until reset locally. Re-starting of a single piece of equipment shall (wherever safe) be through an operator initiated automatic sequence following a single reset, as opposed to a series of start (or reset) commands.
- Rotating Equipment shall be reset via the PCS if the trip is due to process malfunction. However, local resets shall be utilized for rotating equipment trips on the Machinery Protection System. A separate ESD for the Associated Package, if applicable, will also need a local reset.
- Instrumented Protected Functions (IPF) shall not be designed with auto reset i.e. the outputs remain in the tripped state until a reset command is given. If an auto reset must be used (i.e., for process needs such as reset for low level trip), the rationale should be documented formally.

12.20 Operational Overrides

IPF inputs that are in the tripped state prior to start-up of equipment should be temporarily overridden to allow reset and start-up. Operational overrides may be required in this instance.

Automatic start-up overrides are preferred to manual start-up overrides. Automatic start-up overrides shall:

- Have override functionality for a duration of few seconds above the minimum time required for start-up; or
- Have override functionality based on process or equipment conditions (i.e. auto reset to the protected condition by means of a timer or when the set point has been exceeded by process value).

Such automatic overrides will have a positive effect on the overall IPF PFD by removing the risk associated with human error (i.e., leaving on, or switching on again, a manual start-up override).

Operational overrides shall not be provided on manual ESD inputs.

Operational override switches (OOS) shall be provided in the Operator Workstation.

An Operational override signal shall not inhibit the alarm functionality.

12.21 Input/Output Modules

12.21.1 General

Intrinsically safe Inputs and outputs cards shall have galvanic isolation between field equipment and the system. Galvanic isolator can be integrated in I/O modules or independent component.

Each I/O channel shall be fully isolated and I/O modules shall be installed in the system cabinets.

I/O cards shall be designed so that a short-circuit or a high voltage on one I/O will not induce a fault on any other I/O of the card. All modules shall be protected against short circuit, lightning and earth faults.

System components shall be modular in design with rack mounting and plug-in type assemblies. Each system module shall be equipped with light indicators for fault and status display.

The system shall have self-diagnostic programs that run independently from the application programs on a continuous basis with fault detection capability down to the I/O module individual channel.

It shall be possible to replace cards without switching off the power.

Modules shall be replaceable without requiring special tools. All modules shall be replaceable on-line without degrading the system performance. Re-initialization of newly installed module shall be automatic. Where anti-static precautions are necessary when handling cards, they shall be clearly identified. If such precautions are required, grounding wrist straps shall be supplied as permanently fixed items.

Adequate filtering shall be available in order to improve noise immunity and avoid errors. If digital filtering technique is used, the facility to change filter constant on-line in engineering mode is to be made available. There shall be a unique filter constant per point.

I/O modules and chassis shall be organized in logical sections such that each section corresponds to a group of facilities.

The segregation of I/O shall be done according to their I/O type like NIS, IS, volt free signals etc.

For redundant I/O module, failure of one module shall not affect functioning of other modules and shall be possible to replace online without affecting them.

Redundant I/Os and redundant process units/systems I/Os shall not share common hardware. Signals related to status indication shall not be arranged in the I/O card allocated for safety functions.

Redundant IO to be connected in separate IO cards and in separate racks/chassis.

Any pumps or process equipment's having configured as A & B process equipment's i.e., one in standby mode and other in running mode, then it will be considered as redundant process equipment's and hence its IO's to be in separate cards, etc. same as redundant IO's.

As a minimum following philosophy shall be maintained while allocating the I/O's:

1. Inputs and outputs from redundant Equipment shall be wired to separate Input and outputs cards.
2. Inputs and outputs from duty/standby Equipment shall be wired to separate Input and outputs cards.
3. F&G and ESD I/O's of voting group (1oo2, 2oo3, 2oo2) shall be connected to separate Input cards.

Input modules shall be arranged such that inputs forming the voting groups shall be connected to different input modules. Also shall be applied for output modules. Additionally, any loop/function used as Independent Protection Layer (IPL) for any Safety Instrumented Function (SIF), shall not share modules and controllers with that SIF (complete independency shall be achieved).

Maximum number of channels in I/Os card proposed as below:

TYPE	PCS	ESD / F&G
Analog Input (AI)	8	8

TYPE	PCS	ESD / F&G
Analog Output (AO)	4	4
Digital Input (DI)	16	16
Digital Output (DO)	16	8

All unused spare slots shall be provided with suitable blind cover/plate.

I/O modules utilized for safety application shall be SIL compliant. They shall support line-monitoring facilities, allowing open and short circuit detection and alarming.

I/O cards used for analogue control loops shall scan the input signals at 10 msec rate or better, without effecting the signal quality or resolution.

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.

12.21.2 Analog Input (AI)

The device shall not be grounded.

Cards shall support Addressable detectors.

Analog input card shall accept 4-20mA DC signal from 2-wire, 3-wire and 4-wire instruments. 24V DC power shall be provided from the system. Short circuit protection by current limiting or replaceable fuse shall be provided for each channel. However, it shall be able to accept passive inputs, i.e., powered by the field devices. The signal range shall be software configurable per input channel.

Analog input modules shall support HART protocol.

RTD input card shall accept input from Platinum RTDs 100 ohm as per IEC 60751. Range shall be user selectable at site by software tools without need for any recalibration or mechanical adjustment.

Burnout detection shall be available for all channels.

Analogue input card (voltage/current) accuracy shall be better than ± 0.1% of full scale.

T/C and mV input card accuracy shall be better than ± 40micro-V.

The following facilities shall be available for each type of detection loop:

- Detection loop fault (auto-test, beam block, over range, etc.).
- Open and short circuit line monitoring with generation of fault.
- Inhibit facilities for maintenance operation.
- Detection loop alarm reset
- 4-20mA, HART compatible, 24VDC powered by the System and load resistance 600Ω nominal.

12.21.3 Analog Output:

Each analogue output shall be standard 4-20 mA DC signal. Output channels shall be isolated, independent and individually protected by fuse. 24 VDC power shall be provided from the system.

The negative and positive sides of the circuit output shall be wired to independent terminals .Each output channel shall be able to drive an external load up to 750ohms.

Analogue output card (voltage/current) accuracy shall be better than ± 0.3% of full scale.

12.21.4 Digital Inputs (24V DC)

Digital inputs shall be of dry contact type connected directly to the digital input card.

24VDC as input “1” (logical “true”) and open circuit as input “0” (logical “false”). The sense voltage to field contacts shall be supplied from the F&G System via individually fused circuits.

All digital Input cards shall provide loop status LED indication. Fuses shall be able to be replaced without removing the I/O card.

Digital input signal circuits shall interface to intrinsically safe certified field instrumentation (Ex’i’ certified).

Contact inputs shall detect dry contact field switch status changes with sensing voltage supplied from the system side.

Digital input cards shall have software configurable filter to eliminate contact chattering.

Digital input card shall have LED indication for each channel to show the status of the signal.

Sensors shall either be volt-free contacts, or NAMUR proximity type. WPLCS shall provide the power for each type of switch. For volt-free contacts, power will be 24V DC.

NAMUR type modules shall be compliant with current limitations and thresholds as defined in DIN 19234.

Input modules shall include circuitry (filtering, etc.) to ensure that any "chatter" or "bounce" encountered during contact closure does not initiate erroneous information. Filter time may be software configurable. Dielectric strength for digital input shall be tested between I/O terminals and ground for 2 seconds. VENDOR shall state the required voltage test.

12.21.5 Digital Outputs (24VDC)

Digital outputs shall use either solid state or relay technology and be voltage free. Output circuits shall be short circuit proof. Short-circuiting of one output shall not affect any other channel. Electronic “fuse” shall be part of output module.

Each output contact shall be individually configurable to allow the following actions:

- Latched
- Pulse
- Normally open
- Normally close

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.

The output contacts shall be powered by the internal 24V DC power supply. Interposing output relays will be used when output load requires any other voltage. These relays shall be hermetically sealed and fitted with LEDs.

Digital outputs shall be current rated for minimum 0.5 amp for an inductive load per point at 60°C.

Relay shall be DIN rail mounted plug-in type with socket, dust cover and LED indication.

The interposing relays shall be replaceable type on individual channel bases. Changing of a relay will not require replacing more than the faulty relay, other relays or signals shall not be affected.

Relay contact rating shall be 1.5A at 240V AC, or 0.5A at 24V DC resistive load.

Card shall support capability of programmable selection of fail state action on communications failure.

VENDOR shall provide load current per channel for the output card which can drive without use of relays.

12.22 Controller Modules

CPU redundancy will be based on a one-to-one redundancy system. CPU redundancy system (including power supply) shall ensure continuous automatic control in the event of CPU failure. This means that the backup CPU shall automatically take over all card functions and control strategies of the primary controller in less than one second without loss of automatic control, process disturbance, or control upset (bump less transfer).

Failure of any CPU shall cause an alarm to be displayed and logged. Loss of both the active and redundant CPUs shall cause system outputs to freeze at their last position, or to drive to pre-define fail safe conditions. Watch dog function shall be supplied.

The processor's memory shall be backed up by battery power to retain the application program in its memory for a period of 30 days in the event of continuous power loss for 30 days.

System alarm shall be generated in case of low voltage of the battery backup. It should be possible to change the battery online without having to remove the processor from its location.

All redundant parts of the system shall be designed to allow hot on-line replacement of any failed component without any loss of system performance and plant integrity level. Re-initiation of newly installed module shall be automatic.

The ICCS system modules shall be provided with LEDs for normal and fault indication.

System components design shall be modular with rack mounting and plug-in type assemblies.

Each processor shall be provided with the battery back-up (or equivalent means) to retain its memory. VENDOR shall advise for back-up time. Low battery level alarm shall be included as part of the diagnostic alarm.

The ICCS controllers shall be time synchronized with the GPS clocks. The synchronization signal will be received through the ICSS network.

Shell standards DCS Basic Application Standard DEP 32.30.20.15 & Shell Base Layer Control Applications DEP 32.30.20.16 shall be used for the application of ICSS VENDOR software function blocks used for control and monitoring loops:

- DCS Basic Application Standard DEP 32.30.20.15. This DEP specifies requirements, gives recommendations and describes the conventions to be applied to all DCS base layer function block configurations.

- Shell Base Layer Control Applications DEP 32.30.20.16. This DEP specifies rules, policies and guidelines for configuration of process control loops.

The ICCS Controller Unit shall be supplied with a set of functionality to allow the operation of the plant.

The VENDOR shall state the list of available standard functions or algorithms.

The ICCS controllers shall be programmed and configured to meet the functional requirements. At start-up, the system shall be immediately and automatically available without human action.

Logic, control functions, timing data and operating subroutines shall be loaded and tested into the controllers at the manufacturer premises and shall be stored in memory secured by batteries.

The system shall be protected from unauthorized modification of programs and configuration by key lock and/or password.

All the facilities that are necessary for making modification to the system configuration shall be provided on the ICCS engineering workstation.

Each ICCS Controller Unit shall be capable of performing standard algorithms and regulatory control functions by predefined algorithms with configurable parameters.

The following requirements are to be considered as a strict minimum:

- Control algorithms and standard associated functions.
- All inputs shall be fitted with filtering, compensation, bad measure detection, alarms, etc.;
- During operation, switching from auto to manual output mode or switching from local to remote set point shall be bump less.
- Digital Algorithms and standard associated functions.
- The controller shall be capable of registering and stamping events. The VENDOR shall state how/where the events are stamped, the maximum discrepancies between the clocks of the different controllers, and how these clocks are synchronized with GPS clock system.
- Sequence Control.
- If required by the ICCS functions, VENDOR shall provide the programming language that will be loaded in the ICCS controller through the ICCS engineering workstation.
- Loop tuning
- On-line loop tuning facility shall be provided and it shall be bump less to the process and shall be no separate loop setting time required for tuning. It shall be.
    - Applicable to processes with slow and fast dynamics.
    - Used with self-regulating and integrating processes.
    - Immune to noise and process load disturbance.

This auto tuning facility shall allow tuning of PID control blocks whether they reside in the controller or the field device. An easy-to-use graphical interface shall be provided for auto tuning.

PCS Controller are combined with safety controllers the functionality PCS controller shall be identical to that of Safety controller except that the I/O cards will be non-redundant.

12.23 Communication Modules

Communication modules shall be "hot swappable" (It shall be possible to replace without switching off the power).

Communication modules shall be fitted with termination resistance or switches set appropriately if required.

Re-initialization of newly installed modules shall be automatic. Each communication module shall be equipped with light indicators for fault and status display and shall provide error and alarm status at the operator station.

Communication interfaces shall have internal self-diagnostics to ensure data integrity and operational security. Identification and location of faults and status shall be automatic.

Faults and failures of the communication link or module shall not degrade the system reliability. Communication modules shall be immune to interferences present in the environment in which they are installed.

Loss and restart of communication shall not result in trips or status changes of the communication points. Recovery of communication shall be automatic.

12.24 Communication Network

ICSS network shall be extended to the different location as per section 8.1 via dedicated Fiber optical cores/cable (provided by others). Network shall be high speed Ethernet based, redundant and fault tolerant. Safety certified by TUV or equivalent network shall be used for ICSS. If separate networks for PCS and ESD/F&G are provided, ESD/F&G network shall be safety certified and VENDOR shall provide required interfaces.

ICSS networks shall be designed so that no single fault can cause total loss of communication between the operator with any part of the process (e.g., dual highways, screen interfaces, screens and power supplies).

Design of network shall be in full compliance with network security requirements as per “ADNOC ONSHORE ICSS Security Specification for Suppliers”, document no. 30-99-39-0020, IEC 62443 and ISO 27001.

VENDOR shall advise the main characteristics of used protocol, data exchange speed, maximum number of nodes, other limitations, and capacity for expansion.

VENDOR shall state clearly the tools and methods utilized to manage transmission error detection and elimination. These shall include but not be limited to:

- Error checking on all transmissions.
- Automatic re-transmission on error detection.
- Automatic switching to standby data path in the event of primary link critical fault or failure.
- ICSS shall display the number of re-tried transmissions resulting in non-fatal communications errors to enable advance warning of network issues.

12.25 Expansion Capability

ICSS shall be capable of being expanded and scalable in an incremental mode and without any impact on the plant operation. To accomplish this objective, the ICSS shall be specified in a modular architecture having major system components organized and linked hierarchically through the system propriety network. The ICSS shall be designed for future expansion capability

in terms of processing capacity, network loading, point licensing, database, historian sizing and spare requirements outlined in the project specifications. ICSS system shall be scalable to at least 100% of the sized capacity, without complete revision or upgrade of the entire ICSS system.

12.26 System Performance

ICSS shall provide the capability to apply Analog input point, process variable filtering to prevent signal noise degrading the system and communications performance. Filter time constants shall be configurable from engineering workstations on an individual input point basis.

VENDOR shall furnish scan time and frequency, and display response time in his bid. As a minimum, the performance parameters shall be as below:

Scan Time:

Controller for PCS	:	500 milliseconds or better
Controller for ESD/F&G	:	100 milliseconds or better

Display Response Time:

Graphics display	:	1 second or better
Operation Group	:	1 second or better
Trend Group	:	4 seconds or better
Response to Keyboard/Trackball	:	Immediately
Sequence of Event resolution	:	1 millisecond or better
Graphics display Dynamic Data Update (Time for change in Controller to be reflected on graphic)	:	1second Alarm response time

The system shall be able to record all alarms and events occurring under critical process conditions for a period of less than 1 second. The resolution of such alarms shall be as per applications requirement.

The peak load generated by the alarm burst shall not cause any disruption of loss of data on any of the network communications.

All the alarm and event resolution shall be 1 second. All alarms shall be correctly detected, annunciated, time stamped and stored chronologically in the alarm event journal.

ICSS devices or components containing volatile memory shall employ a means of battery back-up in order to preserve memory contents for not less than 3 months subsequent to interruption of power to the system, and so avoiding the need to re-load software. Alarms shall be provided for the back-up battery alarm with at least 1 month before failure occurrence.

VENDOR shall fully describe where all software resides in the system and identify where volatile memory cannot be preserved for the specified time.

12.27 System Diagnostics

VENDOR shall state clearly the tools and methods available for system health monitoring, system performance statistics and proactive failure analysis for all ICSS components.

Test programs should preferably be in firmware and the use of application software-based test programs should be avoided.

All software shall also be subjected to automatic testing, including the application program, to ensure the system's ability to meet a demand.

All system hardware shall be regularly exercised by automatic complete self-testing diagnostics. All software shall also be subjected to automatic testing, including the application program, to ensure the system's ability to meet a demand.

As a minimum, this shall include testing of all input and output circuits, I/O modules, logic processing modules, memory tests, logic solve tests, mis compare tests, console support electronics and communications facilities. Testing shall be comprehensive testing all paths in the system.

For ESD, on receipt of any trip demand, the auto-test routine shall not inhibit the processing and implementation of the logic function required.

Should a fault be detected, and where there is redundancy of design, the system shall automatically adapt to maintain its ability to meet a demand. No fault condition shall remain undetected.

VENDOR'S Detail Functional Design Specification (DFDS) shall describe in detail the software and hardware self-testing routines.

ICSS shall have extensive self-diagnostic capabilities running on-line as a background function. ICSS shall generate graphic displays dedicated to providing diagnostic and system performance overviews to enable clear identification of system component failures including both primary and backup.

ICSS shall generate alarms and log internal errors/faults to the system log files for archiving.

Automatic self-test routine is necessary to maintain the requirements of system availability and reliability.

All diagnostics alarm requirements to be specified. Power failure diagnostic alarms to be hardwired. Each and every MCB trip in the cabinets to be loading or fuse failure has to be alarmed in system and shown on System diagnostic screens in SCADA.

All the requirements such as creation of dedicated diagnostic screens in SCADA has to be specified here.

Failure of any component, IO channel, IO card, Relays, Redundancy Network failure, each and every network switch failure in ICSS has to be alarmed and shown on diagnostic pages in SCADA.

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:

- ‘stuck-on’ - short circuited failure of a discrete input or output.
- ‘stuck-off’ - open circuit failure of a discrete output.

12.28 Changer, Repair & test On-line

ICSS supplied must provide comprehensive automatic diagnostics and on-line testing of the hardware, including back-up or hot spare modules, monitored through the supplied engineering workstation package, without disruption to any other system component.

As a complete re-load of software would necessitate shutdown of one or more operating stations, with substantial consequent Operating losses, Vendor must state any limitations that would force COMPANY to schedule such shutdown once commissioned.

12.29 Software Requirements

ICSS shall provide as part of the system all system and application Licensed software (fully configured & documented) necessary to implement the functionality described in the philosophies, specification, narratives and Cause and Effect Diagrams.

The application program shall be held in flash EPROM and the data shall be stored in SRAM which permits the direct downloading of revised application programs through the communications network from the Engineering Workstations.

Maximum use shall be made of standard application logic function blocks for all commonly used functional requirements at each location.

VENDOR, in his Bid proposal, shall state the memory size required for the application program for the given I/O's and logic. The memory size shall be expandable.

12.29.1 Operating System

VENDOR shall submit the details of the standard system software release version that is proposed in the bid, and his expected software updates for the coming 3 years. The migration path for future software upgrades shall be clearly specified by the VENDOR.

The Operating system software and User Programming language and all associated software must be included in the certification for the system.

VENDOR shall be responsible for the preparation of all application software and configuration for the system.

The system software shall be programmed to facilitate maintenance, modification and future expansion of facilities and be of modular structure. For standard Safety functions, monitoring and interlocking, the software coding shall be provided through the VENDORS standard function block-oriented application programming techniques. Such programming languages must be IEC 61131-3 compliant. Continuous Function Chart (CFC), Sequential Function Chart (SFC) / Functional Block Diagram (FBD), Structured Text (ST), Ladder can be used Function Block Diagram (FBD) programming is preferred.

VENDOR application language shall be a user-friendly window based, intuitive tool that facilitates ease of use for maintenance and engineering. The system shall be based on architecture utilizing modular function block architecture in accordance with IEC 61131 from the VENDORS standard system library incorporating extensive parameter selection, help menus, Functional Blocks and online documentation and configuration manuals.

ICSS, as offered, shall accept and manipulate as a minimum sixteen-character tags.

The Application software development package shall be structured such that data entry is required only for detailed engineering fields. These shall be accessed from pull down options menus and configured with smart default settings to minimize data entry.

The Application software development package shall support cut, copy, and paste control strategy development built to the IEC 61131-3 standard for control strategy development.

The use of multiple instances of Program modules (supported by IEC 61131) shall be avoided. Where Safety Function Program segments appear to be functionally identical to other Safety Programs, separate programs, each instanced once only, shall be generated using conventional Copy and Paste techniques.

The resulting application software shall provide all functions, with logical and interactive operator control via the ICSS operator consoles. The software shall be backed up and stored on non-

volatile media such as CD-ROM/DVD, such that it can be loaded into the system simply and quickly.

12.29.2 Database Management & Software Revision Control

ICSS shall provide an integrated database, system, and application software revision control management tool that automatically audits the system and saves all preceding revisions of System software and database to a secure environment whenever a change is made. The system shall save the data to an external media source i.e., optical disk, CD, or similar. The software revision control tool shall incorporate software security control to ensure software integrity.

VENDOR shall assume total responsibility for the database assembly and records management up to the point of agreed handover to CONTRACTOR. Facilities shall be provided to enable examination, logging, archiving and printing of the system database to storage media. Import – Export function shall be provided for system database management.

The database shall be developed using OLE compatible package for ease of use and interoperability.

12.29.3 Source Program Security

VENDOR shall retain copies of all system source program and configuration files supplied for a period of 10+ years after the delivery of the software and system.

Upgrading of these copies under revision control shall be the responsibility of the VENDOR after each maintenance intervention or software modification performed by the VENDOR until the end of the guarantee period.

12.30 Interface With Third-Party

ICSS VENDOR shall include all the required hardware and software for communication with third party systems (bi-directional communications).

The following table illustrates method of communication between ICSS and third-party systems.

All serial link MODBUS definition maps for all parameters from third party devices and connectivity shall be coordinated between ICSS VENDOR and third party system VENDORS.

At each Power supply skid:

Third Party System Package	ICSS
Hydraulic Pressure unit (HPU)	Hardwired
MOV Control Station	Redundant Serial (MODBUS TCP/IP)
FACP	Redundant Serial (MODBUS TCP/IP) for feedback signals and hardwired for critical signals
PA/GA, ACS	Hardwired
CCTV	Redundant Serial (MODBUS TCP/IP)

Third Party System Package	ICSS
Various Packages	Redundant Serial (MODBUS TCP/IP) for feedback signals and hardwired for critical signals
Electrical System	Hardwired via IRP
HVAC Panel	Hardwired
HSSD/VESDA/Incipient Smoke Detection	Hardwired
UPS	Redundant Serial (MODBUS TCP/IP) for feedback signals and hardwired for critical signals
DG Panel	Redundant Serial (MODBUS TCP/IP) for feedback signals and hardwired for critical signals
EDG Panel	Hardwired for critical signals
SCMS	Redundant Serial (MODBUS TCP/IP)
Machine Monitoring System & System-1 server	Redundant Serial (MODBUS TCP/IP) for feedback signals and hardwired for critical signals

Furthermore details, refer ICSS system architecture drawing Doc. No. 03-99-52-1603.

ICSS VENDOR shall include all applicable firewalls in accordance with ADNOC ONSHORE "ICSS Security Specification for Suppliers" document No 30.99.39.0020.

12.31 Alarm Philosophy

ICSS shall provide alarm display, where alarms are generated if an abnormal condition arises in the process and persists for a specified period of time. The alarms shall be logged in a permanent storage and can be retrieved as and when required by the operator.

Alarms are assigned a time stamp based on the execution cycle in the controller with a time stamp.

The alarm system generates alerts for any change of state that the system detects including:

- Any violation of limits
- Any change of state of a device connected to the system including all of its peripherals.
- The failure of any communications channel used by the system.
- The failure of system's hardware, which results in an automatic fail-over of the system's functions from the active to standby device. i.e., scan failure of processors, memory faults, fan failure, watchdog failure etc.

The alarm messages facilitate easy interpretation of the current alarm status by

- Different text color and background color for those points that are in alarm, those that have been acknowledged, and those that are no longer in alarm.
- Flashing of the current alarm message(s) in the alarm list
- Alarms that have been automatically hidden by the system or manually by the operator
- The system shall provide the option of displaying alarms in ascending or descending temporal.

ICSS HMI interface shall be provided with the ability to disable or suppress alarms at the following levels:

- For each individual alarm condition
- For all alarm conditions associated with a device or point using message suppression buttons provided for equipment's like motor and valve.

Alarm annunciation for process and system alarms shall be in one or more of the following ways:

- Activation of an external audible alarm or light
- Activation of the internal PC sound card (playing of .wav files)
- Updating an alarm display with the current alarm
- Updating an alarm overview screen to indicate the occurrence of an alarm in a specific process area / display.
- Printing the alarm message on a printer
- Any graphic object associated with the alarm point will change colour, shape, appear, disappear, etc. as configured.

All alarm that initiates a trip action shall be configured as critical alarms. Non trip alarms shall be configured as advisory alarms. I/O faults and diagnostic alarm are to be configured as hardware/diagnostic alarm. All status inputs are to be logged as events.

In general, exiting alarm philosophy in ADNOC ONSHORE shall be followed.

12.32 Cyber Security

ICSS security shall be as per ADNOC ONSHORE Specification "ICSS Security Specification for Suppliers" Doc. No. 30.99.39.0020.

Vendor shall design the ICSS security system on robust defense in depth concept according to NESA/ANSI/ISA-62443/ISA 99 cyber security standard for Industrial Automation and Control Systems (IACS). The system shall meet ADNOC ONSHORE "ICSS Security Specification for Suppliers" document No 30.99.39.0020 requirements and NESA framework.

The ICSS system shall be provided with a security / access management system to restrict access to authorized users only to all ICSS operator workstations and servers. Multiple access levels shall be provided to allow differentiation of privileges for the following as a minimum:

Various levels of password security systems shall be provided to prevent unauthorized access to system modification facilities.

The ICSS Operator stations shall be provided with the following access levels:

- **Operator access:** This "operation" level shall include the normal operator functions (Auto/Manual command, set point change, alarm acknowledgment, etc.)
- **Maintenance access:** This level aims at testing equipment, and/or modifying software parameters which are not accessible to operator (some PID's action, timer setting, maintenance inhibit, etc.). It shall also provide access to all operator displays and to study all real time system loads/ errors, network loads/ errors, communication path/ packet loss/ status, real time point database counts on each node etc.
- **Engineer access:** This level aims at providing system network maintenance functions and developing & testing software configuration. This "supervisor and configuration" level shall also include all operator and maintenance functions and provide access to study all real time system loads/ errors, network loads/ errors, communication path/ packet loss/ status, real time point database counts on each node etc.

ICSS security system requirements shall include but not limited to the following:

- Segregation of control network levels into zones as per ISA 62443 standard Control system specific fire wall per each control zone extended for all Independent Protection Layers (IPL).
- Security system backup, restoration and disaster recovery.
- Vendor shall assign Security Assurance Levels (SAL) targets of each security zone based on risk analysis approved by ADNOC ONSHORE and provide evidence of SAL achieved.
- Vendor shall provide ADNOC ONSHORE, a list of ICSS security system certificates.

All ports within the systems and switches shall be managed and unused ports hardened.

Vendor shall use only ADNOC ONSHORE approved fire walls, antivirus and antispyware products and shall get ADNOC ONSHORE approval of products data sheets.

12.32.1 Cyber security SAL Assessment Report & SAL Verification Report

ICSS VENDOR shall conduct/perform cyber security SAL assessment targets for each security zone based on risk analysis approved by ADNOC ONSHORE and provide report for COMPANY review and approval.

ICSS VENDOR shall provide Cyber security SAL Verification Report indicating with proof of SAL achieved for COMPANY review and approval.

12.33 Backup and Historian Server

An automatic archiving facility shall be available to archive historical data and events over a rolling period of 60 days duration. Typically required data to be historized shall include but not limited to operating programs, Application programs, System files, Setpoints, Process Alarms, Operator changes and System errors. Two hard disks shall be utilized to write data simultaneously as aback up to each other, Failure of one will create an operator alarm.

12.34 Matrix Panel

12.34.1 ESD Matrix Panel

ICSS VENDOR shall provide hardwired ESD matrix panel in Operation facility power supply skid with the following signals as a minimum.

- ESD-1 Push button – Overall

- ESD-2 & ESD-3 Push button – Sea water intake area
- ESD-2 & ESD-3 Push button – Operation facility
- ESD-2 & ESD-3 Push button – Murban well pad area
- ESD-2 & ESD-3 Push button – Naphtha well pad area
- ESD-2 & ESD-3 Push button – Power generation area
- Maintenance Override Switch – Sea water intake area
- Maintenance Override Switch – Operation facility
- Maintenance Override Switch – Murban well pad area
- Maintenance Override Switch – Naphtha well pad area
- Maintenance Override Switch – Power generation area
- Reset Push button – Sea water intake area
- Reset Push button – Operation facility
- Reset Push button – Murban well pad area
- Reset Push button – Naphtha well pad area
- Reset Push button – Power generation area

ESD matrix panel will have lamps (RED and Green) just below each individual push button to show the status.

ESD matrix panel shall be a dedicated console with suitable safety shrouds for all push buttons and switches to avoid inadvertent operation.

The matrix panel shall be provided with maintenance enable switches, manual trip switches and tripped status indication of ESD hierarchy trips as per ESD hierarchy and system healthy indication.

The matrix panel shall also be provided with audible alarms, acknowledge and lamp test facility.

The alarm sequence of the matrix panel shall be in accordance with ISA S18.1 M (alarm only with lock-in facilities) and ISA S18.1 F (first failure or first-up alarm groups).

The new ESD matrix panel shall cater for all the requirements on the project C&E diagrams, layouts and philosophies with consideration of 20% spare. All switches and push buttons shall be prewired to dedicated terminal blocks.

12.34.2 F&G Matrix Panel

F&G matrix panel shall be mounted on F&G panel in Operation facility power supply skid by ICSS VENDOR with suitable safety shrouds for all push buttons and switches to avoid inadvertent operation.

Matrix panel shall be provided with switches and indicating lights for each zone. Also, shall be provided with lamp test facility.

The alarm sequence of the matrix panel shall be in accordance with ISA S18.1 M (alarm only with lock-in facilities) and ISA S18.1 F (first failure or first-up alarm groups).

The new F&G matrix panel shall cater for all the requirements on the project C&E diagrams, layouts and philosophies with consideration of 20% spare. All switches and push buttons shall be prewired to dedicated terminal blocks.

12.35 Server cabinet

ICSS VENDOR shall provide dedicated server cabinets with all accessories in operation facilities for mounting all servers such as HMI server, GPS server, SOE sever, historian & backup server. Redundant server to be placed in separate cabinets.

13 ADDITIONAL REQUIREMENT FOR ESD SYSTEM

13.1.1 General Requirements

As a minimum, all component/parts of the ESD system including I/O modules shall be duplicated.

Allocation of safety functions within the system hardware shall consider the following:

- Plant integrity
- Common mode failure
- Cable marshalling
- Efficient use of equipment
- Segregation for maintenance
- Calculation of heat load and distribution

All ESD initiators shall be hardwired to respective input cards in redundant configuration, no software signals from Process Control shall be used as ESD action initiator.

13.1.2 Functional Safety

CONTRACTOR will perform a detailed Safety Integrity level (SIL) analysis of all safety Functions in accordance with IEC 61511 as part of the detailed design and advice the VENDOR of any detailed engineering consequences of that analysis.

Additional measures, including verification and testing by an independent organization nominated by the CONTRACTOR, shall be applied to those safety programs identified as SIL level.

Safety Logic shall be partitioned into functionally related Program Modules. All SIL rated Safety loops must be coded in separate Program Modules such that modifications to other Modules shall have no impact on the SIL rating of program modules. This program module independence shall include but not limited to: -

- A separate, automatically assigned Software Revision Number for each Program Module, such that any changes to a SIL rated Program Module since initial approval and validation, however minor, can be identified.
- SIL rated Program Modules shall use TUV or equivalent approved system standard Functions, or Custom Function Blocks that are not available to be used within other Program Modules, to ensure that any modification of a Custom Function Block subsequent to commissioning cannot inadvertently affect the behavior of a SIL rated Program Module.

13.1.3 Sequence of Event Recording

When required by project specifications, First-Out alarm annunciation and sequence of events (SOE) capabilities shall be provided. The SOE events shall be captured and stored in a dedicated SOE Server, from which these events can be displayed and printed on demand from any workstation.

ESD System shall provide a Sequence of Events Recording (SER) feature including a virtual printer and the ability to print out results to a hard copy printer via PC based data logger.

Events shall be logged in and stored in non-volatile memory as they occur for printing or downloading later.

The SER shall primarily function as back-up for the ICS logging equipment and provide a high-resolution audit trail.

For postmortem analysis, the SER shall be capable of storing 100,000 time-stamped events in a circular file. The time stamp shall equal the system clock time at the time the trip alarm is generated, with a resolution equal to or better than the smallest scan time of any of the ESD system. The SOE shall have a resolution equal or half of the scan time of the ESD controller.

To allow for SER or communications failure, at least the last 100 events shall be stored in a buffer in the ESD system.

For each SER input a unique tag number and service description shall be assigned. A tag number shall consist of at least 16 alphanumeric characters, starting with either an alpha or a numeric character. The minimum number of characters for the service description shall be 30. The VENDOR shall clearly confirm the maximum system capacity for accepting tag numbers and shall identify any constraints.

It shall be possible to copy the SER file onto a back-up medium.

The VENDOR shall provide all software for the SER and its configuration.

It shall be possible, with the correct authorization by means of a password or key, to disable and enable inputs from being recorded on an individual, selected logic group and/or process unit basis.

Event "play-back" and print-out for selected time frames, process units and tag numbers shall be possible. The Supplier shall state the details in the quotation.

Common database facilities such as sorting, querying etc. shall be available, as well as the possibility to export the SER file to Microsoft Windows based applications. The VENDOR shall state the possibilities in his Bid proposal.

Historical data shall be retained on loss of power supply to the system.

14 ADDITIONAL REQUIREMENT FOR FIRE & GAS SYSTEM

14.1 PA/GA System Interface

F&G system shall request alarm tone via PA/GA system. This request shall be available at the ICSS for operations to take appropriate action.

The Fire and Gas system initiates alarms via hard wired monitored outputs from the Fire and Gas system through interposing relays to the PA/GA systems, output required for Confirmed Fire, and confirmed toxic gas detection zone wise with a redundant pair of outputs for each power supply skid.

The fire & gas system upon receipt of detection shall initiate to activate pre-recorded voice messaging and audio announcements via PA/GA system with appropriate Operator intervention. The zone wise announcement shall be done at operator's discretion.

15 ALARM MANAGEMENT

The alarm management system shall be a fully configurable system capable of processing all alarms in an appropriate manner to maximize the information provided, but to minimize the number of alarms displayed. It shall be design in accordance with COMPANY Design Guidelines for Alarm Management DOC. No. 30-99-39-0002, Shell DEP 32.80.10.14 and international standards mentioned in section 3.2.

In order to minimize the number of alarms, grouping, suppression and/or filtering techniques shall be available. Suppressing and/or filtering of alarms shall include:

- Automatic suppression of individual and/or groups of alarms based on the occurrence of a pre-selected alarm or event.
- Automatic disabling of alarms based on the associated equipment running status.

Each alarm point shall be capable of being configured to at least three different alarm priority levels in order to discriminate between critical and non-critical alarms.

Each alarm shall activate an audible and visual alarm at the configured operator console. The alarm shall be displayed on the alarm summary and on the respective graphic displays. In addition, each workstation screen shall display a warning that a point is in an alarm state including the number of unacknowledged alarms.

Once the alarm has been acknowledged:

- The alarm shall change from flashing to steady state.
- The audible alarm signal shall be silenced at all the assigned consoles.
- Once the alarm returns to the normal state:
  - The alarm shall be removed from the alarm summary (if acknowledged).
  - The displays shall return to normal.

All alarms and first out alarms from other machinery packages shall be time stamped with a resolution of at least one second. Both the alarm occurrence and acceptance times shall be recorded.

All alarms and associated information shall be stored on the mass data storage medium for historical purposes.

All alarms configured to be logged shall automatically be printed at the assigned alarm printer and in the event of a printer malfunction; the alarm system buffer shall be able to store up to 200 alarms while the printer is restored to normal.

Alarm's philosophy shall follow the ADNOC ONSHORE philosophy of alarms and alarms handling.

An alarm priority assessment study will be done during detailed engineering. Upon the alarm priority assessment alarm rationalization will be done and the results will be implemented in the ICS. Alarm Management and rationalization workshop shall be carried out, in accordance with COMPANY Design Guidelines for Alarm Management DOC. No. 30-99-39-0002 & Shell DEP

32.80.10.14-Gen, after HAZOP/SIL meeting. The ICSS shall be supplied with the application software package for alarm management which includes dynamic alarm suppression.

The system shall support a sequence of event capability either as part of the alarm management system or in a similar format and/or presentation. The time stamping of the sequence of event signals shall be carried out in the ICSS. The time stamping resolution shall be 10 milliseconds or less.

The sequence of event facility shall allow reports to be displayed or printed automatically and/or on demand.

All sequence of events shall be stored for historical purposes.

16 INSPECTION AND TESTING

16.1 Vendor's Responsibility

The inspection and testing of the ICSS and its accessories shall be as per this specification and Inspection and Test Plan for the ICSS. Procurement Inspection & Certification requirement shall be as per Projects Specification AGES-SP-13-002, Rev-1.

The Factory Acceptance Test (FAT) shall be performed at the ICSS VENDOR's factory.

VENDOR shall internally carry out all agreed system tests before the FAT and present all pre-FAT records to the FAT team for review prior to commencement of the FAT. If any failures are discovered and replacements made during pre-FAT, these shall be logged. This signed and certified records log shall be available for COMPANY/ CONTRACTOR inspection 4 weeks prior to call of FAT witness by COMPANY/ CONTRACTOR and form part of the FAT documentation.

VENDOR shall present to COMPANY/ CONTRACTOR weekly progress reports with all HOLDs, pending issues, concerning areas, ongoing progress and plans for weekly forecast activities/ deliverables.

Testing shall involve all components and subcomponents of the ICSS. The VENDOR shall be responsible to perform a complete functionality test of the ICSS and all the communication interfaces. 100% testing of all I/O points and functions are required or as agreed to by COMPANY and also give the details of staging area in square meter, how the system IFAT with telecom systems etc are proposed to be carried out. VENDOR shall also present to COMPANY their project loading, staging capacity with regard to project schedule etc. This information shall be presented with the bids.

ICSS VENDOR shall provide office accommodation in their ICSS staging facility for up to 6 for COMPANY and CONTRACTOR representatives during the FAT.

The accommodation shall consist of 4 offices, desks, chairs, telephones with international access, and access to e-mail service, broadband WIFI internet, fax machines, scanners and copiers.

In addition to the above ICSS VENDOR shall be responsible for:

- Provision of adequate test area for ICSS equipment, Telecom equipment as well as third party panels, as required.
- Provision of all necessary test equipment (switch/lamp/PB racks, potentiometers, 4-20mA sources, Ammeters, MODBUS simulators etc, as necessary)
- Connection of equipment prior to the tests, and its operation during the tests

- Provide adequate sets of test procedures, test report forms and engineering drawings/ documents.
- Provision of all consumable items
- Correction of errors and deficiencies

For ICSS, Inspection class shall be 1, criticality rating shall be considered 1 and material certification shall be 3.2 as per COMPANY standard 30-99-00-8517.

16.2 Factory Acceptance Test (FAT)

ICSS VENDOR shall provide FAT Procedure and a detailed schedule of tests to CONTRACTOR/ COMPANY, at least three months before commencement of the testing. This shall provide the following details:

- Description of each test, its purpose and expected result.
- Scheduled start date of each test and its approximate duration.
- Detailed FAT procedure for every system

COMPANY/ CONTRACTOR engineers will review the FAT procedure & schedule and shall have the right to make such additions or amendments that are necessary in their opinion to adequately test the system.

VENDOR shall give 6 weeks notification before FAT commencement and make all necessary arrangements.

FAT/IFAT shall be performed only on approved procedure.

The test shall include a loop-by-loop functional test of each input and output signal according to the FAT Procedure to be developed by ICSS VENDOR and to be approved by the COMPANY and CONTRACTOR.

The tests shall demonstrate that the equipment complies fully with the Project specifications, is fully suitable for its intended purpose and that it shall have the required reliability.

The following are the minimum list of tests to be performed during FAT:

- Bill of Materials check for all hardware and software.
- Visual inspection to ensure neat workmanship in cabinet construction, internal layout, cable ducting, wiring, earthing, gland plates, personnel protection for high voltages, dimensional check, door and keylock operation, tag plates/ name plates, warning labels for LASER, cable ferruling, etc.
- I/O testing (5-point calibration check for Analog I/Os, Simulation check for Digital I/Os, Short Circuit/ Open Circuit check etc).
- Testing of system, I/O configuration loading for completeness of all tags, ranges, limits, alarm points, engineering units.
- Testing of sequence and control logic configuration.
- Testing of the facilities provided to load, dump, initialize and recover all the programmable elements of the system.
- Testing of correct changeover of the redundant hot back up units in case of main units failure for Controllers, I/Os, Historian, Power Supplies, and Communications.

- Testing of system performance requirements including Display update rates, Scan times for controllers, communication network loading.
- Testing of controller functions including loop tuning, changing algorithms, changing controller mode, changing controller action etc.
- Checking of various graphic displays including process and system displays on Operator and Engineering Workstations.
- Checking correct functioning of key board operations.
- Functional testing of Large Screen LED displays. (If applicable)
- Testing of hardwired Aux panels, pushbuttons, lamps, switches etc.
- Testing of all circuit breakers, fans, thermostats, power sockets.
- Checking of module serial numbers against system documentation.
- Checking of software inventory including module name and revision number, against system documentation.
- Checking of System diagnostic displays such as failure of a sub system, module, power supply, interface unit, failure of transfer to redundant module on main module failure etc., and other detailed diagnostic displays. Diagnostic alarms for ventilation fan failure, FO switch failure shall also be checked.
- Testing of proper functioning of PCs, all Printers and any other bought out item.
- Testing of system features like inter-changeability between Operator Workstations.
- Testing of synchronization of system clocks through GPS server.
- Checking of Password and key lock functions for various workstations.
- Checking of log formats, shut down reports, MIS reports.
- Checking of I/O mapping of third-party system interfaces.
- Testing of PST functions (if applicable)
- Software integration test
- Testing of proper system operation for specified variations in power supply.
- Testing of system performance under varying load conditions and extreme conditions such as alarm bursts.
- Testing for system restart upon power failure (black start).
- Testing of Alarm Management system software and functionality
- VENDOR shall note that there is absolutely no “SIMULATION” tests acceptable during FAT and IFAT.

16.3 Integrated Factory Acceptance Test (IFAT)

All subsystems (third party system i.e Condition monitoring MMS, System 1 server, FACP, EDG, SCMS, HVAC, etc) interfacing with the ICSS shall be tested during IFAT (integrated test). Prior to this the subsystem shall be factory tested at the respective subsystem VENDOR’s factory for its proper operation.

During IFAT, the integrated system shall be tested for the communication interface functioning, communication (network and serial link) load, the ICSS data base configuration, displays associated with the subsystem and time synchronization with all ICSS as well as third party devices shall be tested (100%).

Subsystem I/O and configuration shall be tested at the respective VENDOR's factory and software simulated for the integrated test. ESD and F&G Cause & Effect matrix configuration, partial stroke test, first-out alarm with ESD time tag shall be fully tested along with corresponding display animation.

Maintenance console functions including sub-system diagnostic alarms shall be tested. Witnessing of these tests by package unit supplier is required. The package unit supplier shall confirm the adequacy of ICSS design in terms of safe start-up, operation, maintenance, shutdown and diagnostics for package unit and its instruments.

16.4 Site Acceptance Test (SAT)

A SAT shall be carried out by VENDOR on completion of the installation and testing of the equipment at site which shall be witnessed by the CONTRACTOR/COMPANY's representative.

The SAT shall be conducted as an integrated test with all the required sub-systems connected together as per the project requirements together with the communication interfaces.

SAT procedure shall be submitted for COMPANY for approval.

For a period of thirty days, the systems behavior and performances during routine working shall be monitored. Check of network load shall be done in the course of the Site Acceptance Test. After thirty days if the system operates as per specification, Site Acceptance of the system shall be signed.

In addition to the tests defined in FAT, the following minimum tests shall be conducted:

- Loop function test
- System integration test for new ICSS
- Verification of HMI Graphics at each OWS
- Verification of hardwired ESD actuation panel

16.5 Integrated Site Acceptance Test (ISAT)

ICSS functionality will have to be tested with complete operational interfaces with all other systems and 3rd party systems. The test shall be witnessed / approved by CONTRACTOR / COMPANY.

17 PREPARATION FOR SHIPMENT AND PRESERVATION

Panels, cabinets, instruments or devices shall be packed and marked as per the project general guidelines and specifications.

All openings must be positively sealed by proper backing plates or other methods to ensure against ingress of dirt and transportation hazard. The use of adhesive tape alone is prohibited.

Easily damageable parts such as machined faces, electrical/electronic components, solenoid valves, limit switches shall be suitably protected with protective caps, plates etc. Protection shall be a minimum 3mm thick. Machined or threaded surfaces exposed to the atmosphere in shipment or storage shall be coated with rust preventative.

All items with components/accessories made of austenitic stainless steel must be stored under cover and out of contact with the ground.

Electrical/electronic components such as positioner, solenoid valves, limit switches shall be suitably packed for installation at site.

VENDOR shall advise any special requirements for storage, inspection, re-application of preservation etc.

18 SITE SERVICES

Vendor shall provide site assistance for the following.

- Installation
- Pre-commissioning and commissioning
- SAT
- Start-up
- Post start-up support for any failures

The expected time for each of these periods will be estimated by the VENDOR and indicated in the proposal for information with the required qualification of personnel and related day costs.

19 SPARE PARTS, CONSUMABLES AND SPECIAL TOOLS

19.1 Philosophy

Any spare parts or services for the ICSS used during the Warranty Period shall be replenished at the VENDOR's expense.

VENDOR shall submit the recommended spare parts list in accordance with the SPIR Procedure.

The time scale and procedure for repair and/or replacement of parts shall be given by VENDOR. VENDOR shall provide information to assist in the ordering of consumables and spare parts as required.

Information required (SPIR Form) is:

- Description of item.
- VENDOR's reference and part number.
- Standard quantities recommended for start-up and commissioning.
- Standard quantities recommended for 2-year operation.

19.2 Commissioning Spares and Special Tools

VENDOR shall supply start up and commissioning spares and tools, as required in order to avoid using any of the recommended operational spares.

VENDOR shall also supply a one-year supply of spares. The one-year spares list shall be approved by COMPANY. VENDOR shall supply all software programs (including licenses) as well as any special tools, programmers, calibration equipment and trouble shouting equipment deemed necessary for the correct installation, testing, commissioning and subsequent maintenance of the ICSS equipment.

19.3 Operational Spares

The VENDOR shall review the equipment (including tools, testing and calibration equipment) offered in his proposal and shall include a comprehensive recommended spare parts list sufficient for two (2) year's continuous operation of the equipment.

The costs of the recommended spares shall be quoted separately, by part. Two-year spares, one year consumable, commissioning and start-up spares and consumable for basic and optional works.

CONTRACTOR shall provide order preparation services for spare parts and consumable during the warranty period and for 2 years operation. This cost assumes that the procurement service will be executed within a period such that the orders to the suppliers are placed before the corresponding SAT. COMPANY will place the order directly to the VENDOR. All cost of material, packing, shipping, clearing, custom duties. If applicable, delivery to site will be paid directly by COMPANY.

20 QUALITY ASSURANCE/ QUALITY CONTROL

VENDOR proposed quality system shall fully satisfy all the requirement of ISO 9001 2015- Quality Management Systems – Requirements and CONTRACTORS QAQC Requirement Specification (AGES-GL-13-001. Rev 1) The VENDOR and Sub-vendors shall be ISO certified. The effectiveness of the quality system and the VENDOR's compliance with it shall be subject to monitoring by COMPANY and in addition, may be audited by an agreed period of notice.

VENDOR shall provide a specific Quality Control Plan (QCP) within 2 weeks of order award for COMPANY review and approval.

VENDOR shall provide the following to COMPANY for approval:

- Coordination procedure to coordinate the manufacturing of all materials, parts and components in different places;
- The source of material supply for all parts and components including the country of origin and place of manufacturing, assembly and testing
- Material certificates for all parts and components before assembly
- Sub-vendors and contractors list and these shall be from COMPANY approved list

The VENDOR shall provide facilities for and cooperate with COMPANY and its designated authorized inspectors during manufacturing, assembly and testing.

21 DOCUMENTATION

All documentation, drawings, correspondence, operating, maintenance and installation manuals shall be in English.

The following are the minimum required documentation:

- ICSS architecture drawings.
- Bill of Materials.
- Operation manual and maintenance manual for all equipment for the use of process operators, control engineers, maintenance engineers and programmers.
- Installation and start-up procedure.

- Power consumption and heat dissipation.
- GA drawings for all cabinets and consoles.
- Weight data for all cabinets and consoles.
- Wiring & termination diagram (including FO cables) and loop diagrams.
- Functional Design Specification (Hardware and Software)
- Detailed Design Specifications
- Tagging Conventions
- HMI Rules for Graphics Generation
- Area and Unit Assignments
- Controllers and Computation Configuration
- Data maps for communication link i.e MODBUS
- As built of system drawings and documents
- I/O assignment / Nest loading schedules
- Graphic Displays for ICSS and all sub-systems.
- Reports and Logs
- Power supply skid console layouts.
- FAT Procedure & Report
- IFAT Procedure & Report
- SAT Procedure & Report
- Logistics Support (spare parts supply and after sales service) letter
- List of Start-up, Commissioning, Operations spares and consumables
- Cyber security SAL Assessment Report
- Cyber security SAL Verification Report
- Packing, Shipment & Preservation Procedure
- Manufacturing Record Book
- Single line diagrams for power distribution.
- Equipment earthing diagrams.
- GPS wiring schematic and configuration details.
- System interconnection cable schedule.
- VENDOR Data Book.

22 TRAINING

Training needs for site personnel for configuration, operation, installation, commissioning and troubleshooting and maintenance of equipment and systems need to be identified.

As a minimum Training for following category of Operations and plant personnel shall be considered.

- System Implementation and maintenance training for Engineers
- System Operators/Supervisors Training
- System Overview and Business Applications training for Managers.

Training shall include the following:

- Overall description and illustration of PCS capacities and functionalities (control, communication, I/O types, programming)
- PCS's major components - racks, CPUs, power supply, communication modules, I/O modules of each type, marshalling and system cabinets.
- Programming functionalities - I/O and database configuration, control program, communication, SOE
- Maintenance functionalities - On-line running monitoring, component replacement, diagnostic alarm analysis
- All software and standard program blocks used definition.
- Spare parts ordering, coding, care of spares.

Training shall be conducted hands-on either on the training system at end user site or at VENDOR's training center as per end-user preferences.

Training will be arranged at System VENDORS Training Center for total of 6 Maintenance Personnel in 2 batches and total of 2 Operations persons in 2 batches because all COMPANY persons cannot be released to attend training at same time.

System Maintenance Training shall be separate and proper hands-on training. Maintenance training will be on dedicated simulators stations for each representative. The purpose of the course is to train Engineers/Supervisor/Technicians for first line fault diagnosis, and repair by replacement.

And Operations Training shall be separate.

All the training curriculum shall the Salt Dome PROJECT specific.

The VENDOR shall provide the separate cost for training along with all training materials and must be itemized to include all costs such as mobilization and demobilization, applicable day rates for VENDOR personnel and all other associated costs.

23 GUARANTEE AND WARRANTY

The guarantee and warranty shall be as per the purchase order requirements.

24 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.

APPENDIX 1: SPECIFICATION FOR PROCESS PLC SYSTEM

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae
أدنوك البرية
ADNOC Onshore

شـركة أبـوظبي للعمليـات البتـرولية البـرية المحـدودة (أدكـــو)

Abu Dhabi Company for Onshore Petroleum Operations Ltd. (ADCO)

Project No. P03404

Replacement of DCS, PLC, F&G and Automatic Sampling System at Jebel Dhanna

ES 03-99-39-1603

(SILVERTECH DOCUMENT NO.: PRJ198-STME.P-JD-IC-SPC-0008)

SPECIFICATION FOR PROCESS PLC SYSTEM

1	15-June-2016	BN	FA	JS	FJ	Issued For Purchase
D	31-May-2016	BN	FA	JS	FJ	Issued For Approval
C	23-May-2016	BN	FA	JS	FJ	Issued For Approval
B	11-May-2016	BN	FA	JS	FJ	Issued For Approval
A	03-Apr-2016	BN	FA	JS	FJ	Issued For Review
REV.	DATE	ORIGINATOR	REVIEWED	APPROVED	APPROVED	DESCRIPTION

CHANGE HISTORY

Rev.	Date of Issue	CR/DR Numbers	No. of Pages	Pages Changed and Reasons for Change
A	03-Apr-2016	-	41	Issued for Review
B	11-May-2016	DR-0021	39	Issued for Approval
C	23-May-2016	DR-0031	41	ADCO comments incorporated
D	31-May-2016	DR-0035	42	ADCO comments incorporated
1	15-June-2016	DR-0045	42	Issued for Purchase

Distribution List

Copy	Registered Holder
Master	SILVERTECH MIDDLE EAST FZCO
Copy 1	TELECTRON AGENCIES & TRADING
Copy 2	ADCO

Questions or comment regarding this document or the product to which it relates should be directed to:

Silvertech Middle East FZCO
P.O. Box: 17910
Jebel Ali, Dubai,
United Arab Emirates
Ph: +971-4-8995000
Fax: +971-4-8995001
Email: stme@silvertech-dubai.com
www.silvertech-me.com

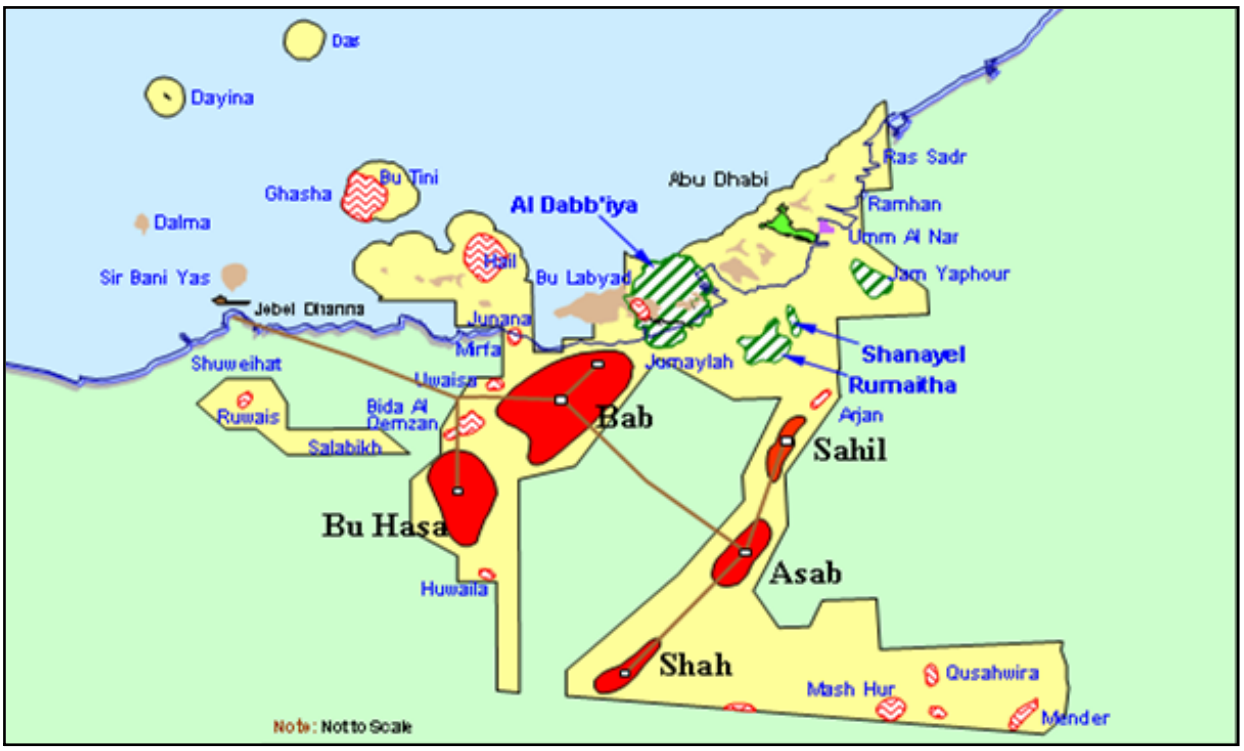
TABLE OF CONTENTS

1. INTRODUCTION

Jebel Dhanna is the storage and export terminal for crude oil produced by Abu Dhabi Company for Onshore Petroleum Operations (ADCO). Its location was chosen because of its proximity to relatively deep seawater and the Jebel being the most appropriate high rock formation on the coast to provide the necessary height for oil gravity feed from the tanks to the shore and outward to the three offshore berths (SPMs), where very large crude carriers can be loaded.

The crude oil is received in the Jebel Dhanna Tank Farms from the crude oil stations: Asab, Sahil, Shah, Bab, NEB and Bu Hasa. This crude oil enters the JD tank farms along three Main Oil Lines, MOL-1, MOL-3, and MOL-4.

The above three incoming MOLs deliver the stabilized crude into JD for storage in sixteen tanks. The crude oil is loaded into oil tankers via three 48" gravity lines supported by diesel turbine driven loading pumps (4 Working +1 Standby), for pressure loading when required. The gravity lines are further branched into four meter banks, four sea lines which finally feed three berths (SPM) serving the oil tankers.



ADCO has awarded this CONTRACT to Telectron Agencies and Trading as an EPC contract. Telectron has selected Silvertech Middle East FZCO as primary EPC SUBCONTRACTOR, responsible for the bulk of the project scope.

The replacement of DCS hardware and software, including workstations, servers, furniture, networking, Field Data Integration System, cyber security, and communication with Process and F&G PLC's will be provided by Invensys (now part of Schneider Electric).

This specification covers the minimum requirements for design, engineering, manufacturing, testing, supply, software development, inspection, testing, FAT, IFAT, preparation for shipment, Documentation, training, Supervision of installation, commissioning and SAT of Process PLC Systems (Metering PLC, MCC

PLC, Pump House PLC, Tank Farm PLC) to be used in terminal systems, handling sour crude oil, for Replacement of Control & Safeguarding System at Jebel Dhanna Terminal.

2. DEFINITIONS

To match the definitions, as used in the Specification, the following terminology shall be used

PROJECT	Replacement of DCS, PLC, F&G and Automatic Sampling System at Jebel Dhanna
CLIENT / COMPANY / PURCHASER	Abu Dhabi Company for Onshore Petroleum Operations (ADCO)
EPC CONTRACTOR	Telectron Agencies & Trading
EPC SUBCONTRACTOR	Silvertech Middle East FZCO This Entire Document is developed by SUBCONTRACTOR
Vendor	Company which builds the panels and develops the software for the PLC System.
Supplier	Company which supplies the hardware and software to build the PLC System.
Must	Signifies a legal or statutory requirement
Shall	Signifies a requirement made mandatory by this Specification
May	Signifies a feature which is discretionary in the context in which it is applied
Will	Signifies a feature which the Supplier may assume to be already present
Should	Used where a provision is preferred; strong recommendation

3. ABBREVIATIONS

ADCO	Abu Dhabi Company for Onshore Petroleum Operations
BS	British Standard
C&ED	Cause and Effect Diagrams
CMMS	Computerized Maintenance management System
CFM	Configurable Flow Meter
DEP	Design and Engineering Practice
DSA	Distributed Server Architecture
ESD	Emergency Shutdown System
EMI	Electromagnetic Interference
FAT	Factory Acceptance Tests
FEED	Front End Engineering and Design
F&G	Fire and Gas System
FGDS	Fire and Gas Detection System
FO	Fibre Optic Cable
GPS	Global Positioning System
HMI	Human Machine Interface
HSC	High Speed Counter
ICSS	Integrated Control and Safety System

ICS	Integrated Control System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISS	Integrated Safety System
IFAT	Integrated Factory Acceptance Tests
IED	Intelligent Electronic Device
I/O	Input/Output
LAN	Local Area Network
LCP	Local Control Panel
MCC	Motor Control Centre
MCN	Master Control Network
MCR	Master Control Room
MOL	Main Oil Line
MOV	Motor Operated Valve
ODBC	Open Database Connectivity
OEM	Original Equipment MANUFACTURER
OPC	OLE for Process Control
OSI	Open Systems Interconnect
PAT	Performance Acceptance Tests
PLC	Programmable Logic Controller
PCN	Process Control Network
RBE	Report By Exception
RFI	Radio Frequency Interference
RTU	Remote Terminal Unit
SAT	Site Acceptance Tests
SDRL	Supplier Data Requirements List
SIL	Safety Integrity Level
SBO	Select Before Operate
SCN	Supervisory Control Network
SCR	Station Control Room
SMS	Safety Management Station
SOE	Sequence of Events
UCP	Unit Control Panel
U/G	Under Ground
UPS	Uninterruptible Power Supply
VSD	Variable Speed Drives
VTA	Vendor to advice

4. CODES AND STANDARDS

4.1. ORDER OF PRECEDENCE

The Standards and Codes shall be applicable in accordance with COMPANY requirements. Should conflict arise between the statements of different specifications, codes or standards, the following precedence shall be applied:

- The laws, standards and regulations of the United Arab Emirates
- Contract Terms and Conditions
- Project Documents
- ADCO Procedures, Codes and Standards
- ADCO specifications and Engineering Practices.
- ADCO amendments and supplements to Shell DEPs
- Latest Shell Design Engineering Practice (DEP)
- International oil and gas industry Codes and Standards and recommended practices

Should different, non-conflicting requirements be made by different specifications, codes or standards, the most stringent one shall apply, and clarification should be sought from COMPANY.

VENDOR shall inform the COMPANY in writing about any deviation from Shell DEPs or COMPANY engineering standards and amendments which it shall be subject to COMPANY's approval.

4.2. SHELL DEP'S

Design shall be in accordance with latest Shell DEP's version. ADCO has documented specific amendments to Shell DEP's, and where identified, shall be applied. Some of the applicable Shell DEP's and ADCO amendments are listed below:

31.10.00.31	Noise Control (amendments/supplements to ISO 15664)
30.00.60.15	Human-Factors Engineering - Control Room Design
32.30.20.11	Fire, Gas and Smoke Detection Systems
32.31.00.10	Instrument Engineering Procedures
30-99-00-0037-1	Instruments for Measurement and Control
32.31.00.34	Instrumentation Documentation and Drawings
32.31.09.31	Instrumentation for equipment packages
70.10.90.11	Spare Parts

4.3. ADCO SPECIFICATIONS AND PROCEDURES

ES 30.99.00.001	Engineering Specification – Tag Plates for Field & Indoor Equipment
EP 30.99.90.001	Engineering Procedure – ADCO Drawing Office Practice
EP 30.99.90.002	Engineering Procedure for the Preparation of Project As Built Drawings/Documents for Vol. 1 and 2.
EP 30.99.90.0024 Rev 2	Procedure for Preparation of Supplier's Vendor's Engineering Drawings and Documents.
EP 30.99.90.027	Submission of Drawings and Engineering Schedule in Electronic Format
EP 30.99.95.004	Engineering Manual-ADCO CAD Manual for Consultants
EP 30.99.90.0006	Submission Of electronic document
EP 30.99.00.004	Procedure for Preparation of Supplier's/CONTRACTOR'S Engineering Drawings and Documents.

4.4. INTERNATIONAL DESIGN CODES AND ENGINEERING STANDARDS

The latest editions of the International Design Codes and Engineering Standards as referenced shall be used:

4.4.1. API - American Petroleum Institute

API RP 551	Process Measurement Instrumentation
API RP 552	Transmission Systems
API RP 554	Process Instrumentation & Control.

4.4.2. CENELEC -Centre for European Normalisation

EN 50014	Electrical Apparatus for Potentially Explosive Atmospheres General Requirements
EN 60079-0	Electrical Apparatus for Potentially Explosive Atmospheres General Requirements
EN 60079-1	Electrical Apparatus for Potentially Explosive Atmospheres – Flameproof Enclosures 'd'
EN 60079-7	Electrical Apparatus for Potentially Explosive Atmospheres – Increased Safety 'e'
EN 60079-11	Electrical Apparatus for Potentially Explosive Atmospheres – Intrinsic Safety 'i'
EN 60079-15	Electrical Apparatus for Potentially Explosive Atmospheres, Type of Protection 'n'
EN 55022	Limits & Methods of measurement of radio interference characteristics of information technology equipment.
EN 50.039 (BS 5501: Part 9: 1982)	Intrinsic Safety Systems
EN 10204	Metallic Products-Type of Inspection Documents

4.4.3. ISA - Instrument Society of America

ISA S5.1	Instrument Symbols and Identification
ISA-S84.01-1996	Application Of Safety Instrumented Systems for the Process Industries
ISA S51.1	Process Instrumentation Terminology
ISA-S5.4	Instrument Loop Diagrams

4.4.4. IEC-International Electrotechnical Commission

IEC 60529	Classification of Degrees of Protection Provided by Enclosures (IP code
IEC 61000 6-2	Electromagnetic Compatibility (EMC) – General Standard – Immunity for Industrial Environments
CISPR 61000 6-3	Electromagnetic Compatibility (EMC) – Part 6 Generic Standards – Section 3 : Emission Standard for residential, commercial and light industrial environments
IEC 61131: Part 1 Part 2 Part 3 Part 4 Part 5 Part 8	Programmable Controllers: General Equipment Information Programming User Guidelines Communications Guidelines for the application and implementation of Programming languages
IEC 61508 Parts 1to 7	Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-Related Systems
IEC 61511	Functional Safety Instrumented Systems for the Process Industry Sector
IEC 60255-22-3	Electrical Disturbance Tests for Measuring Relays and Protection Equipment
IEC 60255-5	Electrical Insulation Coordination for Measuring Relays and Protection Equipment
IEC 60255-4	Electrical Isolation
IEC 60529-1	Degrees of Protection provided by Enclosures
IEC 60079	Electrical Apparatus for Explosive Gas Atmospheres – Intrinsic Safety ‘i’

4.4.5. ANSI / NFPA – American National STDS Institute/National Fire Protection Agency

ANSI/NFPA 70	National Electrical Code (NEC)
ANSI/NFPA 75	Standard for the Protection of Electronic Computer / Data Processing Equipment
ANSI/ISA S18.1	Annunciator Sequences and Specifications
ANSI/ISA S5.5	Graphic Symbols for Process Display

4.4.6. NEMA – National Electrical Manufacturer's Association

NEMA ICS 1	General Standards for Industrial Control and Systems
NEMA ICS 2-230	Components for Solid-State Logic Systems
NEMA ICS 3-304	Programmable Controllers
NEMA ICS-6	Enclosures for Industrial Controls and Systems

4.4.7. IEEE – Institute of Electrical and Electronic Engineers

IEEE C37.1	Automatic and Supervisory Station Control and Data Acquisition
IEEE 730	Software Quality Assurance Plan
IEEE 830	Software Requirement Specification
IEEE 802.3	Standard CSMA/CD Media Access Control (Ethernet)
IEEE 829	Software Test Documentation

4.5. CONFLICTS, DEVIATIONS, AMENDMENTS, AND VENDOR EXCEPTIONS

VENDOR's offer/tender shall clearly state and list exceptions to this specification and all referenced documents. In the event of any conflict arising between this specification and other documents listed herein, refer comments to PURCHASER for clarification before design or fabrication commences.

5. ENVIRONMENTAL CONDITIONS

The site is in desert locations with frequent sandstorms. Rainfall is infrequent but at times can be very heavy.

Wind: Prevailing direction is from NW
Mean Speed: 8 m/s
Max Speed I Design Speed: 44.7 mls

Particulates borne: Saliferous dust and sand

Temperature	Max Solar	85°C
	Max Shade	58°C
	Min Shade	40°C
Temperature	Average Shade	
	Summer	36°C
	Winter	22°C
	Yearly	28°C

Air Temperatures for design of various equipment under shade or indoor:

Air Coolers in main process	46°C
Air Coolers - others	58°C
Air Coolers, Process design approach to ambient	10°C
Gas Turbines	55°C
Electrical generators /motors	55°C
Electrical equipment	52°C
Instrumentation Equipment	55°C
Air compressor	46°C
Diesel / gas engines	58°C
Relative humidity maximum at 43°C:	95%
Average at 53°C:	60%
Solar Radiation	946 W/m2 (300 BTU/hlfe)

Rainfall Infrequent

Maximum	51 mm per year
Minimum	trace

Highest rate in January –April
Heavy dew daily
Early morning mists cause an evaporative cooling loss.

Design ambient temperatures for electrical cables:

Underground cable (buried)	40°C
In concrete trench	54°C
Soil thermal resistivity	2SC mlw

6. DESIGN REQUIREMENTS

This section describes the general specifications, capabilities, programming and control capability, communication capability as well as physical layout characteristics like enclosures, wiring and termination etc of the PLC hardware components forming a part of the Control System. This section describes the minimum requirements of PLC's.

6.1. PLC CONFIGURATION

All the PLC's shall have redundant (hot standby) processors, redundant power supplies and dual redundant communication cards (each CPU shall be provided with a set of redundant communication cards). In case of failure of any of these main component, the changeover to the standby shall be bumpless, ie. Without any process disturbance.

The PLC's provided shall be self-contained units capable of collecting and processing data from intelligent devices through Ethernet, serial interfaces from third party systems like metering systems etc from dry contacts, current or voltage signals, and contact-making pulsing devices.

All PLC's shall include the following features:

No false outputs shall occur during power up or power down

Capable of handling up to 256 Nodes

No single component logic failure shall result in a false output operation. The failure of the first component, which in conjunction with a second component failure could cause a false command, shall be detectable in the course of normal PLC operation.

6.2. PLC PROGRAMMING

System configuration, Logic Programming and database editing shall be performed using a Windows-based user interface. Programming, monitoring, search, and editing shall be accomplished with a dedicated workstation permanently connected to the PLC. These functions shall be capable of being carried out while the controller is off-line or on-line.

It shall be possible to remotely access all PLC's from Engineering workstations at Main Control Room.

The engineering workstation shall be identical to the operator workstation hardware and shall consist of a single non-redundant machine that is equipped with sufficient memory and disk for performing engineering functions. Refer section 6.25 for workstation specifications.

The "look and feel" shall follow the same general style as typical Windows based application programs and shall make extensive use of functions such as drop down lists, drag-and-drop features for standard function blocks and windows system features for data selection, editing etc. All configuration, logic programming and data entry functions shall be password protected with appropriate access control methods.

Data import/export functions shall be provided. The system shall be capable of exporting the database or a selective subset of the database to a file in plain ASCII format, Microsoft Excel and Microsoft Access formats. Similarly, the system shall support importing of data from ASCII text files and Excel and Access worksheets to facilitate large-scale data changes.

The screen format shall display program functions using functions based on IEC 61131-3. The logic editor must allow the use/creation/editing of function blocks and support use of a central code library (whereby applications that are using function blocks from the code library can be updated on a global basis if the function block in the code library is modified).

The Engineer shall be able to monitor and set the status of all inputs, outputs, timers, counters, and coils; the contents of all registers in decimals, and hexadecimal; disable and force all inputs, outputs, and coils to simulate system operation through the engineering workstation.

The programming device shall be capable of indicating “power flow” through all elements and include a search and trace function to locate any element and its program locations.

Machine status information such as error indication and amount of memory used shall be available on the screen.

The system shall be able to compare versions of the programmed ladder logic with the program executing in memory and provide a summary printout of differences.

The following shall be the preferred methods of programming tools:

Software packages for programming of the PLC shall be able to run on a compatible personal computer or Laptop running Microsoft Windows based OS (latest version).

It shall be possible to:

Program in ladder logic, text as well as “drag and drop” function block format and other formats supported by IEC 61131.

Enter program titles, comments, and I/O lists

Modify the program off-line, whilst the system is on-line. The changes made to be stored permanently and not lost when the PLC does a reboot.

Modify the program on-line, whilst the system is on-line. The changes made to be stored permanently and not lost when the PLC does a reboot.

6.3. PLC DATA LOGGING

The PLC shall have data logging capability of any I/O or register data value. The event log entry shall be time tagged with a 1 ms resolution time stamp and each entry shall include the following parameters:

Year, month, day, hour, minute, second, millisecond,

PLC ID, data ID, data priority (0-7), data user type (0-31)

Data value, (2 bytes)

The event log capacity shall be configurable in the PLC memory setup, with a minimum capability of 50,000 event logs before any data is overwritten.

The PLC logic shall allow the storage of logs using the data priority field to mark the priority of the data to the Master so logs can be retrieved based on their priority when required.

The PLC event logs shall be retrievable using any/all arguments of;

Date/time,

Priority,

User type,

PLC/data ID

The PLC's shall time stamp status changes to the nearest millisecond and pass the time stamp to the DCS system for display in the alarm displays and event summaries.

Analogue and pulse input accumulators shall be time stamped to the nearest millisecond when scanned by the PLC.

6.4. PLC COMMUNICATIONS INTERFACE

The PLC's shall be capable of communicating peer-to-peer with other PLC's over the PCN, over 10/100 Ethernet.

The PLC Communications shall support MODBUS TCP/IP for DCS interface.

The DCS VENDOR shall be responsible for providing and enabling the communication interfaces with the F&G, MCC and all other existing interfaces.

In case of failure or malfunction, overloading or breakdown of any communication links, the DCS system shall generate appropriate priority of system alarms.

6.5. PLC I/O & HARDWARE SPECIFICATION

I/O points shall be logically grouped and appropriately segregated between I/O modules to build the system flexibility. Mixing of different types of I/O cards shall be avoided.

I/O designs shall be modular with quick–connect wiring terminations that allow replacement of modules without disturbing field wiring. I/O modules shall be provided with status LED's for each discrete I/O and module "health" status LED for analogue and specialized I/O.

All discrete I/O shall be optically isolated and provide a minimum of 1500V channel to chassis isolation. I/O circuit designs shall be based on 24V DC. All output circuits shall be individually fused with fuse status indication. All input circuits shall be fuse protected to minimize impact to the control system where there is an input short circuit. Individual fusing of each input is required if analysis of logical grouping of inputs is unclear.

Outputs that shut in equipment or fail-safe valves shall be designed fail-safe. Interposing relays are required for AC switching or when the on-board relay capacity is insufficient for the task.

Unless specified, all analogue and digital input / outputs shall be powered by the PLC system. The system shall be able to interface the following types of I/O:

4-20 mA, 24V DC analogue inputs / outputs powered by the system

Digital inputs, 24V DC volt free contacts powered by the system

Digital outputs, 24V DC (1 amp resistive) volt free contacts or 24V DC externally powered (for Solenoid Valve)

RS-232/RS-485 Modbus PLC communication Interface.

Zener barriers requirement as per the existing system shall be considered.

Line Monitoring feature/diagnostic shall be provided for all analog input/output and digital input/output signals. Related Line monitoring Alarms along with other system alarms (eg: Module failure, Processor related alarms, system communication, power supply failures etc.) shall provide via dedicated diagnostic graphics.

It is VENDOR'S responsibility to make sure that the quantity of I/Os matches the project requirements.

6.5.1. Analog Input Requirements

The hardwired analogue inputs shall be wired to the PLC through individually isolated inputs and not input multiplexers.

The A/D converter(s) shall have the following characteristics as a minimum:

Resolution: 16 bits (15 plus one sign bit)

RTD inputs

4 to 20 mA differential isolated input (high level)

0 to 10 VDC differential isolated input (high level)

0 to 50 mV thermocouple inputs with cold junction reference (low level)

Input impedance greater than 250 Ohms

Common mode noise rejection radio: 80 dB or more

Differential mode noise rejection 85 dB at 50 Hz

Accuracy: ± 0.1% or better from 0 to 50oC and over the full range of the power supply

A/D drift detection/correction.

The PLC shall provide linearization of standard thermocouple signals.

The 4-20 mA signals shall be converted to 1-5 VDC at the input terminals by means of a conditioning resistor which maintains an accuracy of at least + 0.1%.

If the A/D operates in under or over-range conditions, for samples less than the minimum values specified above, the PLC shall report 0%, and, for samples greater than the maximum values specified, the PLC shall report 100%.

The update rate of all hardwired analogue input module must not be worse than 2 ms for all channels.

All Analog inputs shall follow the Report-By-Exception (RBE) protocol, to minimize network polling, thereby reducing network bandwidth. The analog input percentage of change in value to which reporting occurs shall be user configurable.

6.5.2. Analog Output Requirements

The analog output modules must allow connection of at least 4 outputs from a multi-channel Digital to Analog Converter (DAC) with a minimum of 12 bits resolution, overall accuracy of at least 0.1% of full scale and output 0/4 to 20mA in to a load of up to 850 ohms. The update rate of the analog module must be no worse than 250mSec for all channels.

The analog output modules shall provide isolated 24VDC loop power for each output channel.

6.5.3. Configurable Flow Meter Module OR High Speed Counter Module

The CFM Module (Configurable Flow Meter) or HSC Module (High Speed Counter) to be capable of connecting directly to a flow meter from field without any other additional interface/converters in between.

The CFM or HSC module to be performs high-speed totalizing and/or rate calculation operations for the flow. This module shall mount in a slot in a Remote I/O chassis along with the other I/O module. The module shall interface with the processor and transfers the data over the Backplane communication.

The CFM or HSC Module interfaces with magnetic pickups, single-channel shaft encoders, turbine flowmeters, or any source of TTL pulses. The module shall support rates as high as 100 kHz and counts to a maximum of 9,999,999.

The CFM or HSC Module shall be capable of accepting the Input Signal Range of:

50 mV⋯200V AC peak — magnetic pickup

4⋯40V DC (TTL compatible)

Visual indication by means of LEDs shall be provided in the module's front panel for each input channel to indicate the condition of hardwired inputs. The module shall have a common multi status indicator on the module's front panel, to show the module's configuration status.

The CFM or HSC modules shall have isolation from high electrical noise and a high immunity towards surge transient RF, Conducted RF etc.

6.5.4. Encoder Counter Module

The encoder/counter module is to be capable of connecting to an input pulses source that typically quadrature type encoders or certain types of switches.

This counter module has to be capable of connecting to an encoder device or any switch, where the voltage signal range is between 12-24VDC.

The input channels to be capable of high speed counting to a minimum of 50kHz

All input channels capable of low speed counting (up to 1 kHz),

All input channels capable of frequency measurement (to 1 Hz resolution),

Any pair of inputs shall be capable of quadrature counting

Visual indication by means of LEDs shall be provided in the module's front panel for each input channel to indicate the condition of hardwired inputs. The module shall have a common multi status indicator on the module's front panel, to show the module's configuration status.

The encoder counter modules shall have isolation from high electrical noise and a high immunity towards surge transient RF, Conducted RF etc.

6.5.5. Digital Input Requirements

The digital input modules must allow connection of at least 16 inputs, with configurable frequency / pulse / quadrature counting, and sequence of events (SOE) recording. Features shall include,

Wide ranging AC or DC inputs (18-250V AC or 12-180VDC),

Sequence of events (SOE) recording on any input channel (to 1ms resolution) with sufficient memory capacity on the input module to store at least 1000 SOE records,

Configurable de-bounce filtering (filter time constant of 1ms – 250ms) for all/any input channels,

Configurable logical channel inversion for all/any input channels

Visual indication by means of LEDs shall be provided for each input to indicate the condition of all hardwired digital inputs. A lit LED shall indicate that the external contact is closed. Serially linked digital input signals shall be monitored directly from the operator workstations.

Each digital input shall be isolated from high electrical noise and properly filtered for contact bounce such that contact transitions must last for a minimum of time before a change is reported. The time of the change is at the initial contact.

The PLC shall provide a 24 V DC interrogation voltage as a standard for the status of all hardwired input contacts.

All digital inputs shall follow the Report-By-Exception (RBE) protocol, to minimize network polling, thereby reducing network traffic.

6.5.6. Digital Output Requirements

The digital output modules must allow connection of at least 8 or 16 outputs. Where 8 channel modules are used, each output channel shall provide both NO and NC contact pairs, with no more than 2 channels sharing a common. Where 16 channel modules are used, each output shall provide NO contacts, with no more than 8 channels sharing a common. Each output shall have a contact rating of at least 2A.

The PLC shall have the ability to connect to an external DIN rail mounted relay board with screwed terminals for field wiring and connection for 16 on board relays. These relay boards could be used when higher rated relay contacts are required for switching up to 16A @ 250VAC, 16A @ 30VDC or 1A @ 125VDC.

6.5.7. Removal of I/O Modules

The equipment shall make extensive use of plug in modules. Input and output modules shall be capable of being removed from or inserted into a fully powered and operational rack without risk of damage. Failure and subsequent replacement of an input or output module shall not affect other modules or cause a system failure.

Modules shall be arranged so that they may be removed without unsoldering or unscrewing wires or breaking any other kind of permanent fastening.

For output modules associated with analogue control, the system shall include an optional standby manual station. This station shall be capable of installation in any input/output rack where it shall receive DC power and provide an adjustable 4-20 mA output in place of a

defective analogue output module. The main function of the manual station shall be to ensure bump-less changeover of an output module i.e. there must be a method of sending a subtitle signal to all output devices driven from the module and there must be an automatic means of balancing them to match the output of output module before it is removed.

The hardware shall be modular in construction and replacements and adjustments can be made as far as possible with the system on-line.

6.5.8. Remote I/O Stations (RIO)

Remote I/O (RIO) station shall be provided in collection tank area for interfacing the I/O signals from the collection tank with the tank farm PLC located at Tank farm control room. This Remote I/O (RIO) shall be connected to the tank farm PLC through Fiber Optic Cable. The new RIO shall be provided without any processor module. RIO panel shall be suitable for outdoor harsh environment conditions like dust, wind, humidity, etc. RIO panel shall be constructed from SS316L material, minimum protection shall be IP65 and certified for respective hazardous area installation. RIO stations shall be provided with sun shade.

6.6. PLC DIAGNOSTICS

The PLC shall have in-built diagnostics that allow local and remote interrogation of diagnostic information. Basic diagnostic information shall be presented to the user via the module LEDs or display the error message/code on a single line display and advanced diagnostic information via the PLC programming and configuration interface program.

The advanced diagnostic information for I/O modules should include the health/presence of each PLC module and the current state/value of each I/O channel (including power supply I/O data).

Diagnostic information specific to the processor module and PLC in general should include the scan rate of I/O and logic, the current time and date, the PLC firmware version, firmware options (i.e. protocols, application extensions etc), list error status flags. Communications statistics should be accessible for each PLC in the network that includes the number of message successes; message fails and fails since last success.

The PLC shall have port monitoring capability that allows local and remote capture of data packet messages to/from any PLC port for display in the programming and configuration interface. These captured messages should be able to be saved to a text file for viewing at a later date.

All the PLC diagnostics shall be logged to Engineering station and the same shall be retrievable when required for Alarm/Event analyzing.

6.7. PLC SECURITY

The PLC shall have two types of security, one for the programming and configuration interface and the other for the PLC ports.

Programming and Configuration Interface - User Security.

The programming and configuration interface shall support at least six levels of user access that can be configured by a system administrator. These should include as a minimum;

Unlimited Access: Allows unlimited access, can read and write all PLC parameters including configuration parameters. PLC parameters include :- Local Registers, Network Registers, System Registers, Hardware (I/O) Registers, Event Logs, and Logic Program/s.

Read All, Write All (except configuration): Allows reading and writing of all PLC parameters, except for System Registers and Ladder Logic. Thus reconfiguring a PLC is not possible from this access level.

Read All, Limited Write Access: Allows reading all PLC parameters. Writing is limited to some Local Registers. No other parameters can be written at this access level.

Read-Only Access: Allows reading all PLC parameters. No parameters can be written at this access level.

Limited Read Access only: This access level allows reading some Local Registers. No parameters can be written.

No Access: No PLC parameters can be read or written. This access level is useful only for PLC port configuration.

The user interface program shall be protected by access control logon permissions. This is checked against the User Database, to verify the password, and to provide the authorized access level. Alternatively, the user can select 'View-Only' mode.

Each PLC Communication Port shall have a configurable access level. The default access level can be any of the levels specified above to control read and write access to that port.

Thus, if a PLC port has default access level “Read-Only”, then only some of the local data registers can be read via that port (e.g. in energy delivery applications this functionality allows the energy. VENDOR shall allow the customer to access ‘some’ of the PLC data).

6.8. PLC POWER SUPPLIES

The PLC power supply shall accept AC or DC input and provide all necessary power to support the PLC operation. The PLC power supply shall be redundant and to be installed on the PLC/IO Chassis or in a separate power supply rack.

The power supply outputs shall be fully isolated from the input power source and include both monitoring and control of the various outputs to allow advanced power management functionality.

Power supply inputs shall include,

AC Input – a wide ranging input of 90-260VAC 50/60Hz from a UPS based power source.

DC Input – a wide ranging input of 20-60VDC, nominally 24VDC.

The Chassis Power supply outputs shall cater to the PLC system requirements and feed the complete PLC or I/O Racks/Chassis.

Monitoring and control of the existing Mains/UPS power supply source operations via the PLC logic shall include the following, but not limited to;

Monitoring: The power supply shall allow monitoring of status and analogue values,

Input supply failure

Low battery voltage

Aux. 24VDC present

Alarm/Fault

Total PLC current consumption – Amps

Battery charge/discharge current – Amps

PLC/battery supply voltage - Volts

Temperature – degrees C/F

Control: The power supply (UPS or any power source) shall allow control via the PLC logic of,

Aux. 12VDC on/off

Aux. 24VDC on/off

I/O module loop power on/off

Required I/O channels shall be considered in the PLC system for Monitoring and Controlling.

6.9. INSULATION AND ISOLATION REQUIREMENTS

The PLC, including all Status inputs, control outputs analog inputs, power supply inputs and communications inputs/outputs shall meet the following insulation and isolation levels specified in IEC 255-5.

Insulation: The PLC shall be designed to withstand a Power Frequency withstand test voltage of 1.5 kV rms and shall conform to IEC 255-5 test standards.

Isolation: The PLC shall have an insulation resistance of more than 5 Mega ohms. It shall also pass an impulse withstand test of 5 kV and shall conform to IEC 255-4 test standards.

High Frequency Disturbance: The PLC shall be designed to pass a high frequency disturbance test to a 5 kV impulse test voltage and shall conform to IEC 255 test standards.

6.10. GALVANIC ISOLATOR PROTECTION

Galvanic Isolators shall be provided in PLC I/O circuits to protect the system from lightning or switching transient exposure; all analogue I/O, installed as per manufacturer specifications.

6.11. SURGE PROTECTION DEVICE

Surge protection devices (arrestors) shall be provided (on the system side) for all I/O's installed in outdoor areas.

6.12. OUTPUT ISOLATION

Isolated relay outputs shall be provided for all other discrete output requirements. Outputs that drive inductive loads shall be equipped with external "fly-back diodes circuits" designed into the output module. Interposing relays shall be provided for MCC related digital outputs.

6.13. FUSE PROTECTION

All output circuits shall be individually fused with fuse-status indication.

All input circuits shall be fuse-protected to minimize impact to the control system when there is an input short circuit. Individual fusing of each input is required if analysis of logical grouping of inputs is unclear.

6.14. INTERPOSING RELAYS

Interposing relays are required for all digital outputs

Interposing relays shall be grouped into AC and DC in different racks. AC switching 110 V and above shall be identified indicating the AC voltage hazard. Solenoid valves power shall be fed from the PLC cabinet.

6.15. OUTPUT FORCING

Output forcing functions shall be provided. Security measures to prevent unauthorized access by password controls shall be part of the feature.

6.16. DIAGNOSTICS

The PLC's must be capable of providing detailed system diagnostics including "smart" field device integrity from the operator and engineering workstation.

6.17. PLC OPERATING ENVIRONMENT

The PLC shall operate over the temperature range of –20deg C through to +70deg C. The PLC shall be suitable for storage over a temperature range of –20 deg C through to +80 deg C.

The PLC shall meet all relevant local requirements for noise immunity and noise emissions.

6.18. SYSTEM AVAILABILITY

The availability of the PLC systems shall be 99.99%. All single points of failures shall be eliminated.

6.19. DESIGN LIFE

PLC equipment and components shall be suitable for continuous design duty operation for a period not less than 30 years, without the need for a complete system revamp due to technological obsolescence.

6.20. SYSTEM SPARE CAPACITY AND SPARES

The system will be supplied with the following amounts of spare capacity as a minimum:

For PLC Hardware (interface, I/O cards, slots, wiring, termination and cabinet space):

- 20% spare capacity on interface, I/O cards, network switches, wired and terminated, ready to configure and use.
- 25% expansion space capacity provided in cabinets and racks for cards, terminations and termination space in the cabinets, but no hardware supplied.
- 10% Engineering Spare shall be considered for each system or at least one I/O module of each type, whichever is higher.

6.21. STANDARDIZATION OF EQUIPMENT

All equipment including PLC's, HMI servers/workstations and all other equipment which form a part of the HMI system shall be standardized wherever possible to ensure:

- Commonality of spares throughout the Terminal;

- Minimized training required on same purpose equipment.
- Economies of scale when purchasing replacement components and maintaining spares across the HMI system.
- Greater economies for maintenance and servicing support for installed equipment.

The hardware selected for HMI system described in this document shall be selected, such that the system can be completely integrated, exploiting their essential as well as best features to the maximum limits. The selection shall also ensure that the hardware components used, follow the best current industry practices in configuration, performance, networking, distribution and considering all aspects of operation and maintenance.

6.22. UTILITY AVAILABLE

240 VAC, 50 Hz Power supply from Redundant UPS Feeder providing supply to the existing panels are available.

6.23. EMC COMPLIANCE

The DCS system and all its components shall be immune to interference from electromagnetic radiation. It shall be possible to operate radio transmitting equipment at 27 MHz, 160 MHz, 453 MHz, 467 MHz and 900 MHz close to the equipment without effecting the operation of the equipment. The equipment shall be tested to IEC 255-22-3, Electrical Disturbance Tests for Measuring Relays and Protection Equipment, Test Severity Class II and Test Method C

6.24. TIME SYNCHRONIZATION

Time synchronization between PLC's and DCS system shall be achieved via NTP servers.

Whenever the DCS system Date and Time is set or reset, an automatic synchronizing signal shall be transmitted by telemetry to all PLC locations. Any PLC station subject to a "Station Failure" shall automatically time synchronize on restoration.

The DCS scan system shall send time-based poll packets periodically every 1 hour interval (system configurable parameter) to maintain time synchronization with PLC's.

6.25. TRAINING SYSTEM

A dedicated Training system shall be provided with the HMI system consisting of:

- A standalone HMI server
- A standalone Engineer's workstation
- 2 X Operator workstations on PCN network.
- 2 X Operator workstations on Safety Network.
- A PLC with one I/O module for each type of I/O configured for the system, completely wired to I/O Simulation panel and ready to use.

- An F&G PLC with one I/O module for each type of I/O configured for the system, complete wired to I/O simulation panel and ready to use. F&G PLC shall also be interfaced with HMI network, to study and train on interface functionalities.

- A Serial Interfaces/MODBUS simulator desktop computer for I/O testing of serial devices.

- I/O Simulation kits/current sources (4-20mA), Digital I/O simulation boards wired with toggle switches and indication lamps.

- A colour laser printer

The Training shall rest on its own dedicated LAN.

The Training system shall be a replica of the installed system including the entire software and logic configuration implemented in the live system. Using simulation, a trainee shall be able to generate Cause & Effects, Functionalities, Control sequences, alarm … and be able to do system programming functionalities (I/O addition, database configuration, control program, graphics, trends, reports etc.).

Contractor shall provide a simulation program which shall replicate the entire HMI, Control and F&G systems to be used by operator to gain experience on the operation, control and maintenance of the above mentioned systems.

The components and software included in the training system shall be identical with the ones provided for the online system.

The system shall allow “what if “scenarios to be applied by the trainee and provide online tests for trainees.

6.26. CONSTRUCTION OF CABINETS

Marshalling and system cabinets shall be constructed from sheet steel be insect-, weather- and vermin-proof and conform at a minimum to IP42 protection.

For outdoor installation cabinets (RIO Cabinets) shall be of SS 316L

Indoor Enclosures shall be corrosion resistant and painted to RAL 7035 with front access or dual (front & rear) access (if required), and lockable with a cam lock. All enclosures located outdoors shall be fitted with a sunshade to shield all vertical and horizontal surfaces of the cabinet.

A document pocket shall be provided in each cabinet for storage of documentation.

All cabinets shall be fitted with ventilation louvers and cooling fan arrangement to create forced draft ventilation through the cabinet. Each equipment cabinet shall contain an internal temperature sensing device and loss of cooling airflow detector. Both will alarm on the associated operator’s console and also log at the alarm logger in the event of abnormal rack or cabinet temperature.

All cabinets shall be provided with anti-condensation heater automatically operated via the hydrostat/humidity sensor installed within each cabinet. This arrangement maintains the relative humidity in the cabinet above the dew point and prevents condensation in the cabinet or on other devices installed inside the cabinet (e.g. CPU, cards, modules …).

All castings used for cabinet construction shall be free from surface defects or other evidence of poor quality materials or poor handling or storage conditions. All edges, folds and bends shall be free from irregularities and stress cracks. The doors shall use a 3 point latching arrangement.

The configuration of all cabinets' enclosure, electronic chassis, modules and cabling shall permit ease of access to all serviceable equipment. Test equipment connections shall be adequately labelled and shall be readily accessible without the need to remove any board or portion of the equipment or power supply. All cabling, fastenings, fittings, screw heads, nuts and bolts shall be International Standard preferred sizes suitable for prolonged use in the specified field environment.

The equipment and all modules therein shall be clearly labelled in English for ease of recognition without module removal.

Power cables shall enter the bottom of the cabinets via suitable termination assemblies and internal power distribution wiring shall be installed in separate conduits. Signal cables shall enter the bottom of the cabinets via suitable termination assemblies.

The exposed surfaces of equipment enclosures shall exhibit a uniform finish and appearance. All metal parts shall be treated to prevent corrosion. Painted surfaces shall be cleaned, primed and undercoated prior to painting to ensure a wear resistant finish. A preparatory powder coating process is preferred.

Contact of dissimilar metals shall be avoided wherever possible and where contact unavoidably occurs, manufacturer shall state what precautions against galvanic action are proposed.

6.26.1. System Cabinet Requirements

The Control System VENDOR'S standard system cabinets shall normally be used provide the following minimum requirements:

Cabinets to be free standing and constructed taking into account delivery and installation requirements (multi-pin plug and sockets shall be used between shipping breaks e.g. Elco plugs)

The cabinet installation shall be finalized subject to final installations method.

Overall cabinet dimensions to be 2100mm high x 800mm wide and 600/800mm deep with double front and rear (if required) removable and lockable hinged door OR only front

Cabinet protection class IP 42 minimum

Separate and isolated cabinets earthing connections shall be provided as follows:

- Safety earth (cabinets and steelwork)

- Signal earth (cable screens and signal common)

The cabinet layouts are to allow full and easy access for installation and maintenance requirements

Cabinet's cable entry shall be finalized during detailed design based on the approved cable entry installation method.

Utility power supplies shall be provided separated from UPS such as conventional type receptacles, fluorescent Lighting.

6.26.2. Terminal Blocks

A terminal block shall be provided for every core entering or exiting the cabinet and for each wiring splice.

Internal wiring and terminal blocks shall be segregated by voltage level and type as follows:

- AC power
- DC power
- Status input
- Control output
- Analogue input
- Analogue output

All of the connections including the PC boards and the power plugs must be equipped with Locking/latching mechanism.

A barrier shall separate terminal blocks for each type of I/O signal. Terminal blocks for AC power, DC power, and I/O signals shall be separated by a minimum 25 mm space, and preferably should be on separate mounting rails.

Terminal block groups shall be labelled. Each terminal in a group shall be numbered.

Terminal blocks shall be arranged within the cabinet in vertical columns on a steel plate / panel from the cabinet sub-VENDOR.

Every I/O point shall be wired to terminals, including spare I/O points. Wiring from the I/O card to the terminal block shall utilize VENDOR supplied pre-connected multi-core cable.

Every terminal (three each for analog input / output and control output, two each for status input) of each I/O point shall be wired to terminal blocks.

The VENDOR'S internal wiring shall be restricted to the system side of the terminal blocks. The VENDOR shall connect no more than two wires to any terminal block. The field side of the terminal blocks shall be left completely free of any wires and jumpers.

Fused terminal blocks with blown fuse indicators shall be provided for all devices requiring 24VDC power. Each device shall have an individual fused terminal block. Daisy chaining of 24VDC power from device to device shall not be accepted.

Connection of 24VDC between fused terminal blocks on the supply side shall be made by metallic jumper bar, specifically made for the purpose by the VENDOR of the terminal blocks.

AC power wiring terminal blocks shall be segregated from the control signal wiring terminal blocks.

6.26.3. Wiring and Terminations

Covered PVC ducts/wire-ways shall be provided between terminal blocks for wiring. Ducts/Wire way loading shall not exceed 30% fill at any point.

AC power and control wiring shall utilize separate wire-way from DC and I/O wiring.

I/O signal termination shall be able to accept a minimum of 1 mm2 and a maximum of 2.5 mm2 stranded copper with PVC insulation.

Power wiring shall accept a minimum of 4.0 mm2 stranded copper, 600 volt insulation. All power wiring shall be via suitable MCB's and fused terminal blocks with proper labelling of the consumers.

Wire termination shall be crimped solder-less compression spread or pin type insulated terminal lug. Any other type shall be subjected to PURCHASER approval. Non-terminated or soldered connections shall not be accepted.

Heat shrink sleeves with permanently printed wire numbers shall be placed at each end of every wire.

There shall be and adequate segregation between terminals and cables in the following categories:

- Analogue
- Digital
- Intrinsically Safe
- Serial Communication

The PLC shall contain terminal facilities for connection of 1 mm2, 1.5 mm2 and 2.5 mm2 field wiring for each I/O point. The terminations shall provide a means of circuit isolation and test access without the need for disconnection of wires.

Captive screw and saddle compression connections made from parts that are suitably treated to resist corrosion shall be used. The terminations shall be segregated according to signal type. Each terminal shall be clearly marked using a permanent marker to provide for its unique identification.

I/O board termination assemblies shall be of the plug-in variety using a suitable modular plug and socket arrangement. It shall be possible to remove and replace a faulty I/O board without the need to individually unmake and remake each circuit connection. Ribbon cable connectors shall not be used at the I/O termination boards.

A single point earth shall be provided in the PLC in the form of a bolt compression type earth lug capable of accommodating 6 mm2 earthing lugs bolted to the cabinet frame. All cabinet shall be provided with three earthing systems (Intrinsic safety earth, Instrument

Earth and Dirty earth) for earthing the cabinet and Instrument earth for earthing the shielded I/O cables via suitable terminal blocks. Instrument earth shall be terminated in a dedicated, insulated bus bar inside each cabinet.

Wiring within the enclosure shall be protected from wear and tear, against accidental cuts, and from contact with enclosure parts or surfaces.

Wiring between marshaling racks to equipment rack shall be continuous runs and not be joined. No more than two wires to be connected to one terminals and only wire to be connected to each side of the terminal block, except for terminal jumpers, provided they are crimped together by the same cable lug or wire pin.

6.27. HMI AND ENGINEERING WORKSTATION

The HMI and Engineering Workstation for Process PLC and F&G system shall have minimum specifications as below.

6.27.1. HMI Workstation

Processor -Intel® Xeon® processor E5-1603 with up to six cores

Redundant, hot-pluggable Network interface cards

Four Ethernet ports

6 USB ports on back panel

Memory – Quad channel; Up to 128GB DDR3 memory; 8 DIMM slots

Hard drive – 2- 500GB or greater hard drives – Installed in a RAID 1 configuration

DVD-RW drive

USB mouse (2 button w/ scroll) and USB keyboard

OS License Certification Label

On-board integrated audio

Video: Dual graphics card (dual monitor capable) each video card provides one DVI and 2-DisplayPort outputs.

Speakers: Two-piece stereo speakers

Monitor – Dual, 26" TFT LCD, 1280 x 1024 pixels or better (best resolution to be recommended)

6.27.2. Engineering Workstation

4 Ethernet ports 2 on motherboard and 2 on an add-in dual-port NIC

6 USB ports on back panel

Processor - Intel® Xeon® 5500 and 5600 series or later

Redundant, hot-pluggable Network interface cards

Memory –192GB (18 DIMM slots), DDR3 800MHz, 1066MHz or 1333MHz

Hard drive – Hot pluggable, Internal storage 24TB or more, RAID 1 configuration

DVD-RW drive

Backup storage unit and removable 160GB cartridge

USB mouse (2 buttons w/ scroll) and USB keyboard

OS License Certification Label

Monitor – 26" TFT LCD, 1280 x 1024 pixels or better (best resolution to be recommended)

6.27.3. Maintenance Laptop

Processor - Intel® Core™ i7 or more

Ethernet ports

4 USB ports

Memory –8GB DDR3L at 1600Mhz - 2 DIMMS

Hard drive – 500GB or greater hard drives

DVD-RW drive

USB wireless mouse

OS License Certification Label

7. QUALITY ASSURANCE

The VENDOR shall demonstrate that he operates a quality system in accordance with the ISO 9001:2000 series of requirements. The VENDOR shall ensure that his sub-suppliers operate a Quality System meeting the specified conformance criteria to ISO 9001:2000. The effectiveness of the quality system and the VENDOR's compliance with it shall be subject to monitoring by PURCHASER and in addition, may be audited following an agreed period of notice.

The VENDOR shall submit a quality control program for PURCHASER review at the time of tender.

The VENDOR shall provide facilities for and cooperate with PURCHASER and statutory authority inspectors during manufacturing, assembly and testing.

8. INSPECTION AND TESTING

8.1. GENERAL

This section describes the minimum requirements for inspection and testing and does not relieve the VENDOR of its obligations to carry out inspections required under the codes, standards and specifications listed in the enquiry documents.

All equipment supplied by the VENDOR should be subject to inspection and witness by the PURCHASER inspector and/or their authorized representative. For this purpose, the VENDOR shall submit an inspection test plan for PURCHASER's approval.

The VENDOR shall allow access and facilities to the inspectors to perform the inspections. This includes all sub-VENDORs supply.

Inspection & Testing of whole system including FAT & SAT shall be made in accordance with latest applicable standards mentioned in this document.

8.2. TESTING REQUIREMENT

All testing prior to delivery shall be carried out at the VENDOR's test facilities. Test equipment shall be supplied by the VENDOR and shall be have valid calibration certificate. The minimum scope of testing is summarized below. The VENDOR shall supply an ITP with the Tender.

The VENDOR shall provide the PURCHASER with at least one month advance notice to witness tests performed in either the VENDOR's shop. Testing shall be carried out by the VENDOR and shall be witnessed at any time by the PURCHASER or the PURCHASER's representative (the Inspector) at various stages as the system is manufactured and assembled.

Locations are detailed below:

- Pre-factory acceptance test - Conducted at the Sub-Contractors Premises
- Factory Acceptance Test (FAT) - Conducted at the Sub-Contractors Premises
- Integrated Factory Acceptance Test (IFAT) - Conducted at the Sub-Contractors Premises
- Site Acceptance Test (SAT) - Conducted at site
- Performance Test - Conducted at site.

8.2.1. Pre-FAT Testing

Prior to the FAT the VENDOR shall complete a Pre-FAT to provide in-house validation testing and quality checks to ensure the system fully complies with the requirements as specified in codes and standards and this specification.

Pre-FAT Inventory Checks

The objective of the PLC System Pre-FAT is to ensure and confirm the following:

That all equipment specified in the Purchaser's documentation is present for inspection.

That PLC System Vendor identification and labelling of all equipment is correct.

That all equipment is presented in good condition and as per the specification.

That all hardware addressing and settings are correct and as per the specification.

That all required documentation has been submitted and approved by the Purchaser and matches the hardware delivered. A full set of approved documentation required for use during the test shall be made available by Vendor.

That all test equipment required to carry out the FAT is available and correctly certified for use.

System "Burn In" Period

To ensure that systems are correctly burned-in and to prevent spurious failures, all components forming the PLC System are to be continually energized for a period of 48 hours at operating temperature and maximum rated load. This will require that load sinking devices shall be simulated at the I/O terminals. The PLC System Vendor is to advise the room environmental conditions during the burn-in test period, i.e. ambient temperature and humidity.

The DCS & PLC System Vendor shall make available to the Purchaser representative written confirmation of the test results including a listing of any component failures during the test and details of the failure specifics.

The QA and testing program for printed circuit boards (PCBs) electronic components, modules and sub modules should include as a minimum:

Physical inspection after initial assembly.

Initial functional test under power (100% of all PCBs).

Unit assembly and coating (inspection).

Final test and inspection (signed off by test engineer).

These tests need not be witnessed by the Company, but certification along with a detailed report on the tests shall be provided. On completion of testing the serial numbers of all equipment shall be recorded for checking on arrival at site. The results of the pre-FAT shall form part of the Manufacturers Data Report.

8.2.2. Factory Acceptance Test

The objective of the FAT of PLC System is to ensure and confirm the following:

All deliverable items, i.e. hardware, operating system software, documentation, media etc, are present and acceptable.

The correct functioning of the PLC System is in accordance with the functional specification, including all interfaces to other equipment and sub-systems.

The system operates under simulated load conditions over the test period at or better than design availability.

The system can tolerate failure of individual modules and sub-systems and be recovered to full function following repair and reinstatement of such items.

The VENDOR shall be responsible for generating the FAT procedures. The VENDOR shall submit the proposed FAT procedures to the PURCHASER approval 3 months before scheduled date of FAT commencement.

The FAT shall include the testing and acceptance of both hardware and proprietary system software. All proprietary system software shall be complete and resident in the System prior to the start of FAT.

All equipment shall be energized and remain energized for the duration of this test. This includes any externally powered equipment.

The FAT of both DCS and PLC System shall include the testing and acceptance of both hardware and proprietary system software. All proprietary system software shall be complete and resident in the System prior to the start of FAT. All documentation and listings must be free of mark-ups.

All equipment shall be energized and remain energized for the duration of this test. This includes any externally powered equipment. Dummy loads shall be fitted in all loops where this is necessary for observing the correct functioning of a loop. These dummy loads shall remain fitted to all circuits except the circuit under test. Outputs shall be connected to a device as similar as possible to the final field element (e.g. relay coil etc.).

All loops in the system shall be tested by applying a simulated signal (or signals in the case of complex loops) at the terminal strip on a panel and observing the effect on the Engineering Workstation. Outputs should also be manipulated and the result measured again from a marshaling panel.

The Purchaser will reserve the right to witness the entire FAT as a non-participating observer. The FAT procedure will be signed off by the Vendor and the Purchaser and a copy of the signed off FAT procedures and related printouts shall be furnished to the Purchaser at the successful conclusion of the FAT.

8.2.3. FAT Hardware Testing

The testing of the hardware shall be detailed on the approved testing procedure and shall include the following as a minimum:

Module Testing
Diagnostic routines

Redundant module software download testing

Power failure and recovery testing of redundant modules.

Power failure and recovery testing of single modules.

On-Line replacement testing.

Battery backup tests.

Black start recovery testing.

Field Terminations Testing

Termination and panel wiring insulation tests.

Power, Fusing & Earthing Checks

Safety earth continuity tests

Instrument earth continuity checks

Power supply redundancy tests

Power supply over current protection tests

Power supply over voltage protection tests.

8.2.4. EMC Emission and Susceptibility Testing

The PLC System Vendor shall demonstrate that a representative configuration of the equipment, sub-system or system required is capable of meeting the test requirements described in the EMC requirements part of this document. Tests shall be carried out by the PLC System Vendor on individual items of equipment or assembled sub-systems with all ancillary items and interconnecting cables connected and tested in accordance with the test procedure and conditions specified.

Alternatively a certificate confirming compliance to the tests shall be supplied for each item of equipment or sub-system tested, giving details of all test equipment used with type and calibration details, the test configuration arrangement, the test site used and the name of the testing authority.

Vendor shall supply a hand-held UHF radio for use in the vicinity of the PLC System to demonstrate that RFI does not affect the system. No other non-standard tests are required.

I/O Testing

Vendor shall test all I/O from the field cable terminals of the cabinet terminals, and observe all responses within the logic using the Engineering Work Station.

The I/O tests shall ensure that:

All I/O are correctly addressed and connected to designated field cabinet terminals.

Mainly all I/O are supplied with field circuit power from the PLC System power supplies.

All Inputs respond correctly to Open circuit and Closed Circuit at the field terminals.

All Analog Inputs respond correctly over the full range of signal input and monitored contact switching thresholds (between Open Circuit, Open Contact, Closed Contact and Short Circuit) are in accordance with the design.

All monitored Outputs provide correct alarm response to open circuit at the field terminals.

All Digital Outputs can be forced On/Off from the EWS.

8.2.5. Integrated Factory Acceptance Test

After completion of the satisfactory system FAT of the DCS and PLC systems test the systems will be delivered to, assembled and interconnected at a staging facility nominated by the Contractor and approved by Company.

The assembled systems shall be tested under conditions that reproduce as nearly as practicable the conditions anticipated at site, and will demonstrate that the overall system operates as specified.

All I/O from all systems shall be connected either to field devices or test equipment to accurately emulate operating conditions.

System Integration Testing will involve testing teams from multiple Vendors, and will require cooperation and co-ordination.

The DCS and PLC Vendor shall be responsible for providing the test procedures, test equipment and suitably qualified personnel to carry out the system testing, including monitoring of relevant DCS displays. The DCS vendor will be responsible for correcting any DCS configuration errors identified by the F&G or other testing teams.

VENDOR shall provide all necessary hardware, software and technical assistance to troubleshoot hardware, software issues during IFAT.

IFAT procedure shall be issued for Company approval.

8.2.6. Site Acceptance Tests

The site acceptance test procedure shall be developed by the VENDOR and approved by PURCHASER and shall demonstrate that the completely assembled and installed system operates successfully under real conditions on the real process fluid, and communicates properly with the live control system.

The purpose of the SAT is also to establish that the system cabinets/equipment has been shipped without damage, has been correctly installed, and operates reliably to specification in its final environment.

The VENDOR shall be responsible for maintaining detailed test records for all inspection and testing carried out in the format agreed in the SAT procedures documentation.

The SAT test specification shall reflect the structure and the phasing of the testing starting with inventory checks and hardware tests through software testing to final testing of a fully integrated system of hardware and software.

Objectives

Ensure that all deliverable items, hardware, software, documentation, media, etc are present and acceptable.

The correct functioning of the overall DCS and PLC System in accordance with the applicable functional specifications, including all interfaces to other equipment and sub-systems on the final power supply and earthing system.

The system operates under load conditions over the test period at or better than design availability.

The system can tolerate failure of individual modules and sub-systems and be recovered to full function following repair and re-instatement of such items.

That all timer settings and alarm/trip set points that may have been modified for the purposes of FAT have been re-configured to their correct values.

That all remedial punch-list work agreed at the FAT has been satisfactorily completed by Vendor and the systems meet its design specification in full.

The Operator interface is both safe and operable with respect to the presentation of data and alarms and the implementation of control.

Hardware Testing

Test for correct installation and configuration of all redundant equipment by carrying out forced failure and recovery testing. This testing is to extend to all network communications cables, power distributions, gateways and switches, hubs and media converters.

Any equipment added or replaced since the FAT shall be fully tested.

Power distribution, fusing, segregation and earthing checks.

DCS - PLC/UPS tests including in-rush, mains failure, static switch failure, battery discharge, voltage and frequency variation.

Check for ancillary equipment interference, e.g. HVAC thermostats, lighting dimmers, radios.

Check operation and performance of all connected sub-systems. In particular those not previously tested.

Software Testing

Any software which has been subject to remedial work since FAT should be thoroughly re-tested including any potential impacts on unmodified software. Similarly any software added since FAT shall be fully tested.

A random sample of Loops, to be chosen by the Purchaser, representing approximately 50% of the total user software shall be retested during SAT, requiring manipulation in the field of physical input devices (transmitters and other sensors) and field observation of the actions of final output devices (valves etc).

These tests shall be conducted without the use of the DCS and PLC System Engineering Workstation or any other simulation devices, and shall use the time delays and set-points specified for final operation.

8.2.7. Performance and Availability Test

After the completion of the Site Acceptance Test, entire system shall be subject to a performance test. CONTRACTOR shall start up and operate the system for a minimum trial period to ensure that it operates correctly, and shall test all functions of the system, including the software, to and ensure that it operates in accordance with the requirements of the design specification/relevant standards, prior to actual commissioning and handing over to ADCO.

The duration for performance test shall be agreed between PURCHASER and VENDOR at Bid stage (however not less than two weeks).

The availability test will be conducted by the PURCHASER and will consist of monitoring the system availability during the sixty-day period.

If the system does not meet the availability and performance requirement during the test conducted by the PURCHASER, the VENDOR shall be responsible for repairing or upgrading the system (at the VENDOR's expense) in order to meet the requirement.

The PURCHASER will then repeat the availability test.

9. SITE SERVICES

The contractor shall provide the following services as per contract:

- Manpower for all site activities
- Pre installation checks
- Execution of the scope,
- Pre-power on checks, and power up
- Pre-commissioning
- System Start Up/Commissioning
- Site Acceptance Testing /System handover

9.1. INSTALLATION, START-UP, COMMISSIONING & HANDOVER

The VENDOR, in their tender, shall identify any special requirements or recommendations for VENDOR support during commissioning and start-up of the equipment supplied. The PURCHASER's final acceptance of the equipment will be subject to a performance and availability tests once the equipment has been installed and commissioned.

Both the installation and the commissioning activities shall be undertaken as a single continuous operation. Upon completion of the installation activity, EPC SUB CONTRACTOR shall Test, Start-up, Commission and Handover the system to ADCO.

The VENDOR shall make available the services of experienced start-up engineers to assist with the installation of the system in addition to the initialization of system power and provide support during the commissioning of the system and also ensure general system troubleshooting assistance.

9.2. COMMISSIONING

Commissioning of the system shall constitute practical completion following the satisfactory completion of installation, testing and start up.

EPC SUB CONTRACTOR shall demonstrate to the client that the system successfully performs all of the functions set out in the design specification.

Complete Commissioning reports shall be submitted as part of Project Dossier.

EPC SUB CONTRACTOR shall present an Acceptance Certificate for signature by ADCO.

9.3. HANDOVER

EPC SUB CONTRACTOR, upon completion of the commissioning activity, shall hand over the system to the client. At the time of hand over, EPC SUB CONTRACTOR shall provide the client with the following documentation:

Project Dossier (as per ADCO standards) which shall include as minimum:

- Construction Records
- Component and equipment list
- Product description sheets
- System design specification / System design drawing(s)
- As built drawings and power distribution
- System schematic diagram(s)
- System operating and service manuals
- Spare parts list
- Certificate of commissioning

10. TRAINING

CONTRACTOR shall provide training to personnel who operate and maintain the DCS and PLC system and provide the training manuals as part of final documentation – both hard and soft copies.

Work Group	Level (with the number of attendees)	
	Basic	Advanced (Engineering)
Maintenance Training	15	10
Operation Training	30	0

10.1. OPERATION TRAINING

System Overview User Interface

Regional, Language, Video, Display Settings; Sound and Audio Devices; Help Functions; Printers

Menu Navigation System Menus

User, Roles and Groups, Point of Control

Alert and Alarm Handling; Filtering, Alert Tracking

Process Panels

Process Typical and their Operation

Trend Viewer, Reports

System Diagnosis Screens

System Interfaces from an Operators point of view

10.2. MAINTENANCE TRAINING BASIC LEVEL

Technical System Overview

System Menu Options

System and Process Start-up / Shutdown

System Back-Up

Basics of Monitoring and Diagnosis

Overview of redundant systems (H/F differences, availability, redundant systems)

PLC system design and I/O, synchronization, connection and updating of the system, principle of operation, error handling

Hardware configuration (system parameterization, system handling, fault diagnostic, documentation)

Exercise of I/O configuration and troubleshooting, programming examples

PLC software basic operations

PLC software block types and program structure

Programming parameter-assignable blocks

Data management with data blocks

Programming organization blocks

Testing (debugging) tools for system info, troubleshooting and diagnostics

Hardware configuration Program documentation and backup

10.3. MAINTENANCE TRAINING ADVANCED LEVEL

- Technical System Overview
- System concept
- System Menu Options
- System and Process Start-up / Shutdown
- System Back-Up
- Restore Operations
- System Upgrades, Patches, Service Packs
- Redundancy, Automatic and Manual Switch Over
- System Monitoring and Diagnosis
- Point of Control Maintenance
- OPC interface
- Application Errors and Trouble Shooting
- Fault Diagnosis and Log Files
- Settings and Parameters
- System Interfaces
- Software Architecture, used / configured project Modules
- Control programming
- Defined scripts
- Use libraries and functions
- Graphical objects
- Panels
- Database
- Panel Topology
- Test and Introduction of Changes to the System
- PLC system
- Aids for program creation (e.g. structure program)
- Functions, function blocks and multi-instances
- Jump commands and accumulator operations
- Indirect addressing

- Error handling with error organization blocks
- Evaluating diagnostics data
- Troubleshooting and messages
- Analog value processing
- Test and Introduction of Changes to the System

11. EXECUTION WORK PROGRAM

The bidder shall submit work execution program as part of his technical offer indicating the required partial / complete shutdown of the existing system and indicating any temporary measures which may be implemented to reduce the partial / complete shutdown period(s).

12. SPARE PARTS AND SPECIAL TOOLS

12.1. SPARE PARTS

The Vendor shall identify and supply the following spares as noted below:

Pre-commissioning, commissioning and start-up spares including software licenses (Supply is included in the scope of VENDOR)

Recommended spares list for two years operation (Submission of Priced SPIR only).

The Vendor shall supply the following spares for DCS and PLC system as below;

15% spares supplied for each type of cards, terminations and physical slots available for use, but not installed. Note: This spare does not constitute of two (2) year operational spare parts which shall be recommended by the VENDOR.

The spare parts list (SPIR) shall be submitted for Company approval following ADCO SPIR format.

12.2. SPECIAL TOOLS

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 specialized procedures.

Standard equipment includes items available from standard catalogues. The list of the standard tools and testing and calibration equipment required shall state the following:

- Description of its service or simulation application
- Manufacturer and Catalogue No.
- Quantity recommended.
- Special tools shall be itemized and priced with the Tender.
- The PURCHASER shall agree the Special Tools to be included in Purchase Order.

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

13. SPECIAL REQUIREMENTS

13.1. SURFACE PREPARATION FINISH

Painting shall in accordance with ADCO Spec. ES 30.99.37.0013 - Painting & Coating of New Equipment. The paint system shall be selected as per the referred ADCO spec.

Where operating conditions are not suitable for the specified system, VENDOR shall specify a suitable alternative (subject to ADCO's approval)

The final color shall be selected as per the ADCO specification.

MANUFACTURER own standard, with PURCHASER's approval, may be used if it meets or exceeds the ADCO Spec. ES 30.99.37.0013.

13.2. NAME PLATE DETAIL

All equipment's shall be supplied tagged in accordance with ADCO EP 30.99.00.0001 Engineering Specification - Tag Plates for Field & Indoor Equipment's.

Tag plates shall be manufactured from 316L stainless steel. Text and numbering shall be clearly engraved, paint filled and a minimum of 6mm high.

Tag plates for accessories shall be secured using stainless steel screws, stainless steel wire or stainless steel chain.

The primary nameplate shall be mounted in a prominent location secured by stainless steel screws or rivets. The nameplate shall contain the following minimum information:

- Client name
- Project name
- Purchase order number
- Equipment title
- Equipment tag number
- Manufacturer's Name
- Serial number
- Year built
- Certified Weight (kg)

14. ORIGINAL EQUIPMENT'S MANUFACTURER

The contractor shall execute the installation; start up, commissioning and the trial period under the direct supervision of the original equipment manufacturer.

The required training shall be carried out by the OEM.

15. PACKING, PRESERVATION AND PREPARATION FOR SHIPMENT

The VENDOR shall prepare the equipment for export shipment, in accordance with the applicable QA/QC procedures.

Documents, including unloading, unpacking and lifting instructions, a description of the reassembly steps required for installation and pre-commissioning and start up instructions shall be included with the package. The number of copies of documents to be provided shall be as stated in the Contract.

VENDOR shall ensure the equipment is suitably supported and braced for transport. Prior to shipment, all high accuracy skid mounted instrumentation and other equipment vulnerable to damage shall be disassembled and boxed separately and send with the skid

The VENDOR shall recommend preservation requirements for idle periods of non-operation up to 6 months for protection against rain, moisture, dirt, blasting grit etc.

VENDOR shall provide all necessary documentation for import of equipment into UAE.
The MANUFACTURER shall provide a complete packaging and handling specification to cover both skid and electronic panels.

One copy of the IOM manual shall be shipped with the systems.

16. DOCUMENTATION

The Contractor shall be responsible for providing all documentation in accordance with the Contract,

The contractor shall provide any document required to design, construct and test the system and as minimum to supply the followings:

- Datasheets
- Specifications
- General Arrangement Drawings
- Wiring Diagrams
- Cable Schedule
- I/O List
- Electrical Power Distribution Diagram
- Bill of Materials
- Functional Design Specifications
- Factory Acceptance Test Plan
- Factory Acceptance Test Procedure
- Site Acceptance Test Plan
- Site Acceptance Test Procedure
- System Performance Specifications
- Recommended Start-Up/Commissioning and Operational Spare Parts List (as per ADCO template)

- Functional Test Certificates
- Installation Operating Manual
- Vendor Data Books
- Manufacturer Data Books
- Maintenance Manuals
- As-Built Mark up and Project Dossier

Tender-(Proposal) Documentation

Tender proposal documentation shall include the following:

- Full technical literature for the equipment offered.
- A list of all accessory items together with MANUFACTURER's name and part number.
- The VENDOR shall provide a completed copy of the data sheets with all changes entered.
- Fabrication / Production schedule
- The VENDOR shall separately detail each proposed deviation from the specification, data sheets,
- Technical Requisition, and submit to the PURCHASER for approval.

APPENDIX 2: SPECIFICATION FOR F&G PLC SYSTEM

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae
أدنوك البرية
ADNOC Onshore

شـركة أبـوظبي للعمليـات البتـرولية البـرية المحـدودة (أدكـــو)

Abu Dhabi Company for Onshore Petroleum Operations Ltd. (ADCO)

Project No. P03404

Replacement of DCS, PLC, F&G and Automatic Sampling System at Jebel Dhanna

ES 03-99-39-1605

(SILVERTECH DOCUMENT NO.: PRJ198-STME.P-JD-IC-SPC-0007)

SPECIFICATION FOR F&G PLC SYSTEM (MCR, Tank Farm)

1	15-June-2016	BN	FA	JS	FJ	Issued For Purchase
C	31-May-2016	BN	FA	JS	FJ	Issued For Approval
B	23-May-2016	BN	FA	JS	FJ	Issued For Approval
A	20-Apr-2016	BN	FA	JS	FJ	Issued For Review
REV.	DATE	ORIGINATOR	REVIEWED	APPROVED	APPROVED	DESCRIPTION

CHANGE HISTORY

Rev.	Date of Issue	CR/DR Numbers	No. of Pages	Pages Changed and Reasons for Change
A	20-Apr-2016	-	37	Issued for Review
B	23-May-2016	DR-0032	38	ADCO comments incorporated
C	31-May-2016	DR-0036	38	ADCO comments incorporated
1	15-June-2016	DR-0044	38	Issued for Purchase

Distribution List

Copy	Registered Holder
Master	SILVERTECH MIDDLE EAST FZCO
Copy 1	TELECTRON AGENCIES & TRADING
Copy 2	ADCO

Questions or comment regarding this document or the product to which it relates should be directed to:

Silvertech Middle East FZCO
P.O. Box: 17910
Jebel Ali, Dubai,
United Arab Emirates
Ph: +971-4-8995000
Fax: +971-4-8995001
Email: stme@silvertech-dubai.com
www.silvertech-me.com

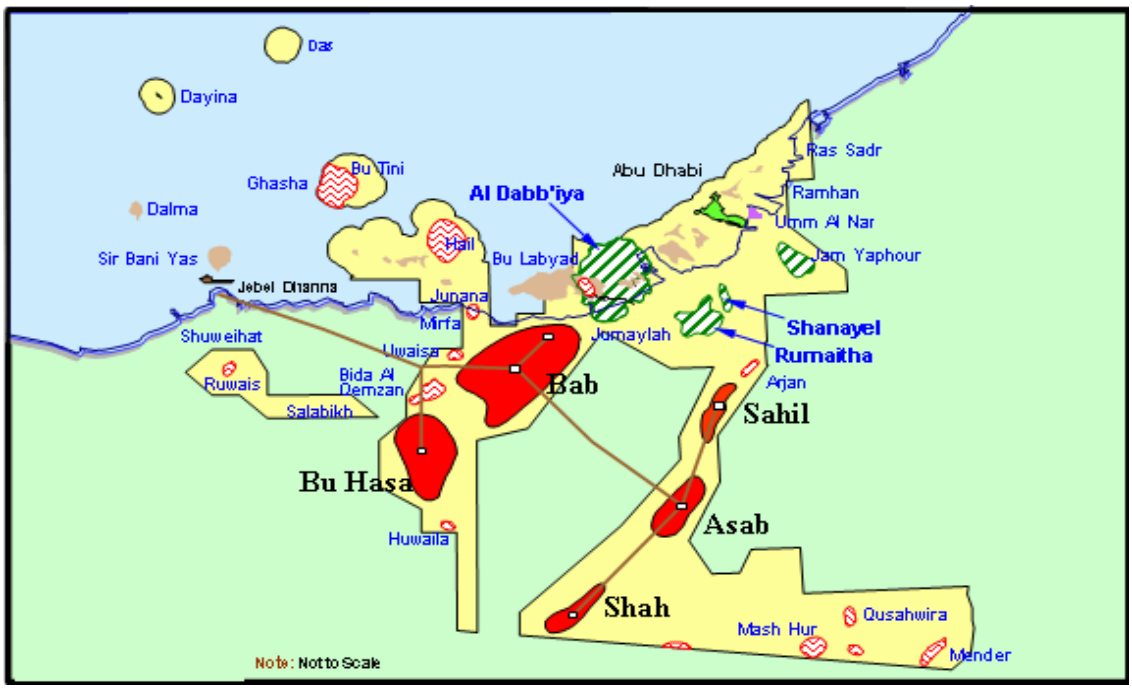
TABLE OF CONTENTS

1. SCOPE

Jebel Dhanna is the storage and export terminal for crude oil produced by Abu Dhabi Company for Onshore Petroleum Operations (ADCO). Its location was chosen because of its proximity to relatively deep seawater and the Jebel being the most appropriate high rock formation on the coast to provide the necessary height for oil gravity feed from the tanks to the shore and outward to the three offshore berths (SPMs), where very large crude carriers can be loaded.

The crude oil is received in the Jebel Dhanna Tank Farms from the crude oil stations: Asab, Sahil, Shah, Bab, NEB and Bu Hasa. This crude oil enters the JD tank farms along three Main Oil Lines, MOL-1, MOL-3, and MOL-4.

The above three incoming MOLs deliver the stabilized crude into JD for storage in sixteen tanks. The crude oil is loaded into oil tankers via three 48" gravity lines supported by diesel turbine driven loading pumps (4 Working +1 Standby), for pressure loading when required. The gravity lines are further branched into four meter banks, four sea lines which finally feed three berths (SPM) serving the oil tankers.



ADCO has awarded this CONTRACT to Telectron Agencies and Trading as an EPC contract. Telectron has selected Silvertech Middle East FZCO as primary EPC SUBCONTRACTOR, responsible for the bulk of the project scope.

The replacement of DCS hardware and software, including workstations, servers, furniture, networking, Field Data Integration System, cyber security, and communication with Process and F&G PLC's will be provided by Invensys (now part of Schneider Electric).

This specification covers the minimum requirements for design, engineering, materials, selection, manufacture/assembly, hardware and software configuration, inspection, testing at factory (FAT), documentation and preparation for shipment, supply, Installation, Pre-commissioning, commissioning, field calibration, interface with other systems, supply of spares and site acceptance test, Performance guarantee test of the Fire and Gas (F&G) PLC System to be used at Jebel Dhanna Terminal.

2. DEFINITIONS

To match the definitions, as used in the Specification, the following terminology shall be used:

PROJECT	Replacement of DCS, PLC, F&G and Automatic Sampling System at Jebel Dhanna
CLIENT / COMPANY / PURCHASER	Abu Dhabi Company for Onshore Petroleum Operations (ADCO)
EPC CONTRACTOR	Telectron Agencies & Trading
EPC SUBCONTRACTOR	Silvertech Middle East FZCO This Entire Document is developed by SUBCONTRACTOR
Vendor	Company which builds the panels and develops the software for the PLC System.
Supplier	Company which supplies the hardware and software to build the PLC System.
Must	Signifies a legal or statutory requirement
Shall	Signifies a requirement made mandatory by this Specification
May	Signifies a feature which is discretionary in the context in which it is applied
Will	Signifies a feature which the Supplier may assume to be already present
Should	Used where a provision is preferred; strong recommendation

3. ABBREVIATIONS

ADCO	Abu Dhabi Company for Onshore Petroleum Operations
BS	British Standard
C&ED	Cause and Effect Diagrams
CMMS	Computerized Maintenance management System
CFM	Configurable Flow Meter
DEP	Design and Engineering Practice
DSA	Distributed Server Architecture
ESD	Emergency Shutdown System
EMI	Electromagnetic Interference
FAT	Factory Acceptance Tests
FEED	Front End Engineering and Design
F&G	Fire and Gas System
FGDS	Fire and Gas Detection System
FO	Fibre Optic Cable
GPS	Global Positioning System
HMI	Human Machine Interface
HSC	High Speed Counter
ICSS	Integrated Control and Safety System
ICS	Integrated Control System
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISS	Integrated Safety System
IFAT	Integrated Factory Acceptance Tests
IED	Intelligent Electronic Device
I/O	Input/Output
LAN	Local Area Network

LCP	Local Control Panel
MCC	Motor Control Centre
MCN	Master Control Network
MCR	Master Control Room
MOL	Main Oil Line
MOV	Motor Operated Valve
ODBC	Open Database Connectivity
OEM	Original Equipment MANUFACTURER
OPC	OLE for Process Control
OSI	Open Systems Interconnect
PAT	Performance Acceptance Tests
PLC	Programmable Logic Controller
PCN	Process Control Network
RBE	Report By Exception
RFI	Radio Frequency Interference
RTU	Remote Terminal Unit
SAT	Site Acceptance Tests
SDRL	Supplier Data Requirements List
SIL	Safety Integrity Level
SBO	Select Before Operate
SCN	Supervisory Control Network
SCR	Station Control Room
SMS	Safety Management Station
SOE	Sequence of Events
UCP	Unit Control Panel
U/G	Under Ground
UPS	Uninterruptible Power Supply
VTA	Vendor to advice

4. CODES AND STANDARDS

4.1. ORDER OF PRECEDENCE

The Standards and Codes shall be applicable in accordance with COMPANY requirements. Should conflict arise between the statements of different specifications, codes or standards, the following precedence shall be applied:

- The laws, standards and regulations of the United Arab Emirates
- Contract Terms and Conditions
- Project Documents
- ADCO Procedures, Codes and Standards
- ADCO specifications and Engineering Practices.
- ADCO amendments and supplements to Shell DEPs
- Latest Shell Design Engineering Practice (DEP)
- International oil and gas industry Codes and Standards and recommended practices

Should different, non-conflicting requirements be made by different specifications, codes or standards, the most stringent one shall apply, and clarification should be sought from COMPANY.

VENDOR shall inform the COMPANY in writing about any deviation from Shell DEPs or COMPANY engineering standards and amendments which it shall be subject to COMPANY's approval.

4.2. SHELL DEP'S

Design shall be in accordance with latest Shell DEP's version. ADCO has documented specific amendments to Shell DEP's, and where identified, shall be applied. Some of the applicable Shell DEP's and ADCO amendments are listed below:

31.10.00.31	Noise Control (amendments/supplements to ISO 15664)
30.00.60.15	Human-Factors Engineering - Control Room Design
32.31.00.10	Instrument Engineering Procedures
32.31.00.34	Instrumentation Documentation and Drawings
32.31.09.31	Instrumentation for equipment packages
70.10.90.11	Spare Parts

4.3. ADCO SPECIFICATIONS AND PROCEDURES

ES 30.99.00.001	Engineering Specification – Tag Plates for Field & Indoor Equipment
EP 30.99.90.001	Engineering Procedure – ADCO Drawing Office Practice
EP 30.99.90.002	Engineering Procedure for the Preparation of Project As Built Drawings/Documents for Vol. 1 and 2.
EP 30.99.90.0024 Rev 2	Procedure for Preparation of Supplier's Vendor's Engineering Drawings and Documents.
EP 30.99.90.027	Submission of Drawings and Engineering Schedule in Electronic Format
EP 30.99.95.004	Engineering Manual-ADCO CAD Manual for Consultants
EP 30.99.90.0006	Submission Of electronic document
EP 30.99.00.004	Procedure for Preparation of Supplier's/CONTRACTOR'S Engineering Drawings and Documents.
30.99.00.0034	Fire, Gas and Smoke Detection Systems
30-99-00-0037-1	Amendment/supplement to DEP No. 32.31.00.32 Instruments for Measurement and Control

4.4. INTERNATIONAL DESIGN CODES AND ENGINEERING STANDARDS

The latest editions of the International Design Codes and Engineering Standards as referenced shall be used:

4.4.1. API - American Petroleum Institute

API RP 551	Process Measurement Instrumentation
API RP 552	Transmission Systems
API RP 554	Process Instrumentation & Control.

4.4.2. CENELEC –European Committee for Electrotechnical Standardizations

EN 50014	Electrical Apparatus for Potentially Explosive Atmospheres General Requirements
EN 60079-0	Electrical Apparatus for Potentially Explosive Atmospheres General Requirements
EN 60079-1	Electrical Apparatus for Potentially Explosive Atmospheres – Flameproof Enclosures 'd'
EN 60079-7	Electrical Apparatus for Potentially Explosive Atmospheres – Increased Safety 'e'

EN 60079-11	Electrical Apparatus for Potentially Explosive Atmospheres – Intrinsic Safety 'i'
EN 60079-15	Electrical Apparatus for Potentially Explosive Atmospheres, Type of Protection 'n'
EN 55022	Limits & Methods of measurement of radio interference characteristics of information technology equipment.
EN 50.039 (BS 5501: Part 9: 1982)	Intrinsic Safety Systems
EN 10204	Metallic Products-Type of Inspection Documents

4.4.3. ISA - Instrument Society of America

ISA S5.1	Instrument Symbols and Identification
ISA-S84.01-1996	Application Of Safety Instrumented Systems for the Process Industries
ISA S51.1	Process Instrumentation Terminology
ISA-S5.4	Instrument Loop Diagrams

4.4.4. IEC-International Electrotechnical Commission

IEC 60529	Classification of Degrees of Protection Provided by Enclosures (IP code
IEC 61000 6-2	Electromagnetic Compatibility (EMC) – General Standard – Immunity for Industrial Environments
CISPR 61000 6-3	Electromagnetic Compatibility (EMC) – Part 6 Generic Standards – Section 3 : Emission Standard for residential, commercial and light industrial environments
IEC 61131: Part 1 Part 2 Part 3 Part 4 Part 5 Part 8	Programmable Controllers: General Equipment Information Programming User Guidelines Communications Guidelines for the application and implementation of Programming languages
IEC 61508 Parts 1to 7	Functional Safety Of Electrical/Electronic/Programmable Electronic Safety-Related Systems
IEC 61511	Functional Safety Instrumented Systems for the Process Industry Sector
IEC 60255-22-3	Electrical Disturbance Tests for Measuring Relays and Protection Equipment
IEC 60255-5	Electrical Insulation Coordination for Measuring Relays and Protection Equipment
IEC 60255-4	Electrical Isolation
IEC 60529-1	Degrees of Protection provided by Enclosures
IEC 60079	Electrical Apparatus for Explosive Gas Atmospheres – Intrinsic Safety 'i'

4.4.5. ANSI / NFPA – American National STDS Institute/National Fire Protection Agency

ANSI/NFPA 70	National Electrical Code (NEC)
ANSI/NFPA 75	Standard for the Protection of Electronic Computer / Data Processing Equipment
ANSI/ISA S18.1	Annunciator Sequences and Specifications
ANSI/ISA S5.5	Graphic Symbols for Process Display

4.4.6. NEMA – National Electrical Manufacturer's Association

NEMA ICS 1	General Standards for Industrial Control and Systems
NEMA ICS 2-230	Components for Solid-State Logic Systems
NEMA ICS 3-304	Programmable Controllers
NEMA ICS-6	Enclosures for Industrial Controls and Systems

4.4.7. IEEE – Institute of Electrical and Electronic Engineers

IEEE C37.1	Automatic and Supervisory Station Control and Data Acquisition
IEEE 730	Software Quality Assurance Plan
IEEE 830	Software Requirement Specification
IEEE 802.3	Standard CSMA/CD Media Access Control (Ethernet)
IEEE 829	Software Test Documentation

4.5. CONFLICTS, DEVIATIONS, AMENDMENTS, AND VENDOR EXCEPTIONS

VENDOR's offer/tender shall clearly state and list exceptions to this specification and all referenced documents. In the event of any conflict arising between this specification and other documents listed herein, refer comments to PURCHASER for clarification before design or fabrication commences.

5. ENVIRONMENTAL CONDITIONS

The site is in desert locations with frequent sandstorms. Rainfall is infrequent but at times can be very heavy.

Wind: Prevailing direction is from NW
Mean Speed: 8 m/s
Max Speed I Design Speed: 44.7 mls

Particulates borne: Saliferous dust and sand

Temperature	Max Solar	85°C
	Max Shade	58°C
	Min Shade	40°C
Temperature	Average Shade	
	Summer	36°C
	Winter	22°C
	Yearly	28°C

Air Temperatures for design of various equipment under shade or indoor:

Air Coolers in main process	46°C
Air Coolers - others	58°C

Air Coolers, Process design approach to ambient	10°C
Gas Turbines	55°C
Electrical generators /motors	55°C
Electrical equipment	52°C
Instrumentation Equipment	55°C
Air compressor	46°C
Diesel / gas engines	58°C
Relative humidity maximum at 43°C:	95%
Average at 53°C:	60%
Solar Radiation	946 W/m2 (300 BTU/hlfe)

Rainfall Infrequent

Maximum	51 mm per year
Minimum	trace

Highest rate in January –April
Heavy dew daily
Early morning mists cause an evaporative cooling loss.

Design ambient temperatures for electrical cables:

Underground cable (buried)	40°C
In concrete trench	54°C
Soil thermal resistivity	2SC mlw

6. DESIGN REQUIREMENTS

This section describes the general specifications, capabilities, programming and control capability, communication capability as well as physical layout characteristics like enclosures, wiring and termination etc of the F&G PLC System (MCR, Tank Farm). This section describes the minimum requirements of PLC's.

6.1. PLC CONFIGURATION

All the PLC's shall have redundant (hot standby) processors, redundant power supplies and dual redundant communication cards (each CPU shall be provided with a set of redundant communication cards). In case of failure of any of these main component, the changeover to the standby shall be bump less, e.g.. Without any process disturbance.

The PLC's provided shall be self-contained units capable of collecting and processing data from intelligent devices through Ethernet, serial interfaces from third party systems like Remote I/O system, FACPs etc from dry contacts, current or voltage signals, and contact-making pulsing devices.

All PLC's shall include the following features:

- No false outputs shall occur during power up or power down
- Capable of handling up to 256 Nodes

- Remote I/O Bus on Ring Topology

No single component logic failure shall result in a false output operation. The failure of the first component, which in conjunction with a second component failure could cause a false command, shall be detectable in the course of normal PLC operation.

6.2. PLC PROGRAMMING

System configuration, Logic Programming and database editing shall be performed using a Windows-based user interface. Programming, monitoring, search, and editing shall be accomplished with a dedicated workstation permanently connected to the PLC. These functions shall be capable of being carried out while the controller is off-line or on-line.

It shall be possible to remotely access all PLC's from Engineering workstations at Main Control Room.

The engineering workstation shall be identical to the operator workstation hardware and shall consist of a single non-redundant machine that is equipped with sufficient memory and disk for performing engineering functions.

The "look and feel" shall follow the same general style as typical Windows based application programs and shall make extensive use of functions such as drop down lists, drag-and-drop features for standard function blocks and windows system features for data selection, editing etc. All configuration, logic programming and data entry functions shall be password protected with appropriate access control methods.

Data import/export functions shall be provided. The system shall be capable of exporting the database or a selective subset of the database to a file in plain ASCII format, Microsoft Excel and Microsoft Access formats. Similarly, the system shall support importing of data from ASCII text files and Excel and Access worksheets to facilitate large-scale data changes.

The screen format shall display program functions using functions based on IEC 61131-3. The logic editor must allow the use/creation/editing of function blocks and support use of a central code library (whereby applications that are using function blocks from the code library can be updated on a global basis if the function block in the code library is modified).

The Engineer shall be able to monitor and set the status of all inputs, outputs, timers, counters, and coils; the contents of all registers in decimals, and hexadecimal; disable and force all inputs, outputs, and coils to simulate system operation through the engineering workstation.

The programming device shall be capable of indicating "power flow" through all elements and include a search and trace function to locate any element and its program locations.

Machine status information such as error indication and amount of memory used shall be available on the screen.

The system shall be able to compare versions of the programmed ladder logic with the program executing in memory and provide a summary printout of differences.

The following shall be the preferred methods of programming tools:

- Software packages for programming of the PLC shall be able to run on a compatible personal computer or Laptop running Microsoft Windows based OS (latest version).

It shall be possible to:

- Program in ladder logic, text as well as "drag and drop" function block format and other formats supported by IEC 61131.
- Enter program titles, comments, and I/O lists

- Modify the program off-line, whilst the system is on-line. The changes made to be stored permanently and not lost when the PLC does a reboot.
- Modify the program on-line, whilst the system is on-line. The changes made to be stored permanently and not lost when the PLC does a reboot.

6.3. PLC COMMUNICATIONS INTERFACE

The PLC's shall be capable of communicating peer-to-peer with other PLC's over the PCN, over 10/100 Ethernet. The DCS VENDOR shall be responsible for providing and enabling the communication interfaces with the F&G PLC.

In case of failure or malfunction, overloading or breakdown of any communication links, the DCS system shall generate appropriate priority of system alarms.

Interface to the third party systems like FACPs (Fire Alarm Control Panels) through the below mentioned networks;

- MODBUS TCP/IP
- MODBUS Serial (RS232/RS485)
- CANBUS

6.4. PLC I/O & HARDWARE SPECIFICATION

I/O points shall be logically grouped and appropriately segregated between I/O modules to build the system flexibility. Mixing of different types of I/O cards shall be avoided.

I/O designs shall be modular with quick–connect wiring terminations that allow replacement of modules without disturbing field wiring. I/O modules shall be provided with status LED's for each discrete I/O and module "health" status LED for analogue and specialized I/O.

All discrete I/O shall be optically isolated and provide a minimum of 1500V channel to chassis isolation. I/O circuit designs shall be based on 24V DC. All output circuits shall be individually fused with fuse status indication. All input circuits shall be fuse protected to minimize impact to the control system where there is an input short circuit. Individual fusing of each input is required if analysis of logical grouping of inputs is unclear.

Outputs that shut in equipment or fail-safe valves shall be designed fail-safe. Interposing relays are required for AC switching or when the on-board relay capacity is insufficient for the task.

Unless specified, all analogue and digital input / outputs shall be powered by the PLC system. The system shall be able to interface the following types of I/O:

- 4-20 mA, 24V DC analogue inputs / outputs powered by the system
- Digital inputs, 24V DC volt free contacts powered by the system
- Digital outputs, 24V DC (1 amp resistive) volt free contacts or 24V DC externally powered (for Solenoid Valve)
- RS-232/RS-485 Modbus PLC communication Interface.
- Zener barriers requirement as per the existing system shall be considered.

Line Monitoring feature/diagnostic shall be provided for all analog input/output and digital input/output signals. Related Line monitoring Alarms along with other system alarms (eg: Module failure, Processor related alarms, system communication, power supply failures etc.) shall provide via dedicated diagnostic graphics.

It is EPC Subcontractor's responsibility to make sure that the quantity of I/Os matches the project requirements.

6.4.1. Analog Input Requirements

The hardwired analogue inputs shall be wired to the PLC through individually isolated inputs and not input multiplexers.

The A/D converter(s) shall have the following characteristics as a minimum:

- Resolution: 16 bits (15 plus one sign bit)
- RTD inputs
- 4 to 20 mA differential isolated input (high level)
- 0 to 10 VDC differential isolated input (high level)
- 0 to 50 mV thermocouple inputs with cold junction reference (low level)
- Input impedance greater than 250 Ohms
- Common mode noise rejection radio: 80 dB or more
- Differential mode noise rejection 85 dB at 50 Hz
- Accuracy: ± 0.1% or better from 0 to 50oC and over the full range of the power supply
- A/D drift detection/correction.

The PLC shall provide linearization of standard thermocouple signals.

The 4-20 mA signals shall be converted to 1-5 VDC at the input terminals by means of a conditioning resistor which maintains an accuracy of at least + 0.1%.

If the A/D operates in under or over-range conditions, for samples less than the minimum values specified above, the PLC shall report 0%, and, for samples greater than the maximum values specified, the PLC shall report 100%.

The update rate of all hardwired analogue input module must not be worse than 2 ms for all channels.

All Analog inputs shall follow the Report-By-Exception (RBE) protocol, to minimize network polling, thereby reducing network bandwidth. The analog input percentage of change in value to which reporting occurs shall be user configurable.

6.4.2. Analog Output Requirements

The analog output modules must allow connection of at least 4 outputs from a multi-channel Digital to Analog Converter (DAC) with a minimum of 12 bits resolution, overall accuracy of at least 0.1% of full scale and output 0/4 to 20mA in to a load of up to 850 ohms. The update rate of the analog module must be no worse than 250mSec for all channels.

The analog output modules shall provide isolated 24VDC loop power for each output channel.

6.4.3. Digital Input Requirements

The digital input modules must allow connection of at least 16 inputs, with configurable frequency / pulse / quadrature counting, and sequence of events (SOE) recording.

Features shall include,

- Wide ranging AC or DC inputs (18-250V AC or 12-180VDC),
- Sequence of events (SOE) recording on any input channel (to 1ms resolution) with sufficient memory capacity on the input module to store at least 1000 SOE records,
- Configurable de-bounce filtering (filter time constant of 1ms – 250ms) for all/any input channels,
- Configurable logical channel inversion for all/any input channels

Visual indication by means of LEDs shall be provided for each input to indicate the condition of all hardwired digital inputs. A lit LED shall indicate that the external contact is closed. Serially linked digital input signals shall be monitored directly from the operator workstations.

Each digital input shall be isolated from high electrical noise and properly filtered for contact bounce such that contact transitions must last for a minimum of time before a change is reported. The time of the change is at the initial contact.

The PLC shall provide a 24 V DC interrogation voltage as a standard for the status of all hardwired input contacts.

All digital inputs shall follow the Report-By-Exception (RBE) protocol, to minimize network polling, thereby reducing network traffic.

6.4.4. Digital Output Requirements

The digital output modules must allow connection of at least 8 or 16 outputs. Where 8 channel modules are used, each output channel shall provide both NO and NC contact pairs, with no more than 2 channels sharing a common. Where 16 channel modules are used, each output shall provide NO contacts, with no more than 8 channels sharing a common. Each output shall have a contact rating of at least 2A.

The PLC shall have the ability to connect to an external DIN rail mounted relay board with screwed terminals for field wiring and connection for 16 on board relays. These relay boards could be used when higher rated relay contacts are required for switching up to 16A @ 250VAC, 16A @ 30VDC or 1A @ 125VDC.

6.4.5. Removal of I/O Modules

The equipment shall make extensive use of plug in modules. Input and output modules shall be capable of being removed from or inserted into a fully powered and operational rack without risk of damage.

Failure and subsequent replacement of an input or output module shall not affect other modules or cause a system failure.

Modules shall be arranged so that they may be removed without unsoldering or unscrewing wires or breaking any other kind of permanent fastening.

For output modules associated with analogue control, the system shall include an optional standby manual station. This station shall be capable of installation in any input/output rack where it shall receive DC power and provide an adjustable 4-20 mA output in place of a defective analogue output module. The main function of the manual station shall be to ensure bump-less changeover of an output module i.e. there must be a method of sending a subtitle signal to all output devices driven from the module and there must be an automatic means of balancing them to match the output of output module before it is removed.

The hardware shall be modular in construction and replacements and adjustments can be made as far as possible with the system on-line.

6.5. PLC DIAGNOSTICS

The PLC shall have in-built diagnostics that allow local and remote interrogation of diagnostic information. Basic diagnostic information shall be presented to the user via the module LEDs or display the error message/code on a single line display and advanced diagnostic information via the PLC programming and configuration interface program.

The advanced diagnostic information for I/O modules should include the health/presence of each PLC module and the current state/value of each I/O channel (including power supply I/O data).

Diagnostic information specific to the processor module and PLC in general should include the scan rate of I/O and logic, the current time and date, the PLC firmware version, firmware options (ie. protocols, application extensions etc), list error status flags. Communications statistics should be accessible for each PLC in the network that includes the number of message successes; message fails and fails since last success.

The PLC shall have port monitoring capability that allows local and remote capture of data packet messages to/from any PLC port for display in the programming and configuration interface. These captured messages should be able to be saved to a text file for viewing at a later date.

All the PLC diagnostics shall be logged to Engineering station and the same shall be retrievable when required for Alarm/Event analyzing.

6.6. PLC SECURITY

The PLC shall have two types of security, one for the programming and configuration interface and the other for the PLC ports.

Programming and Configuration Interface - User Security.

The programming and configuration interface shall support at least six levels of user access that can be configured by a system administrator. These should include as a minimum;

- Unlimited Access: Allows unlimited access, can read and write all PLC parameters including configuration parameters. PLC parameters include :- Local Registers, Network Registers, System Registers, Hardware (I/O) Registers, Event Logs, and Logic Program/s.
- Read All, Write All (except configuration): Allows reading and writing of all PLC parameters, except for System Registers and Ladder Logic. Thus reconfiguring a PLC is not possible from this access level.
- Read All, Limited Write Access: Allows reading all PLC parameters. Writing is limited to some Local Registers. No other parameters can be written at this access level.
- Read-Only Access: Allows reading all PLC parameters. No parameters can be written at this access level.

- Limited Read Access only: This access level allows reading some Local Registers. No parameters can be written.

- No Access: No PLC parameters can be read or written. This access level is useful only for PLC port configuration.

The user interface program shall be protected by access control logon permissions. This is checked against the User Database, to verify the password, and to provide the authorized access level. Alternatively, the user can select 'View-Only' mode.

Each PLC Communication Port shall have a configurable access level. The default access level can be any of the levels specified above to control read and write access to that port.

Thus, if a PLC port has default access level “Read-Only”, then only some of the local data registers can be read via that port (e.g. in energy delivery applications this functionality allows the energy VENDOR to allow the customer to access some of the PLC data).

6.7. PLC POWER SUPPLIES

The PLC power supply shall accept AC or DC input and provide all necessary power to support the PLC operation. The PLC power supply shall be redundant and to be installed on the PLC/IO Chassis or in a separate power supply rack.

The power supply outputs shall be fully isolated from the input power source and include both monitoring and control of the various outputs to allow advanced power management functionality.

Power supply inputs shall include,

- AC Input – a wide ranging input of 90-260VAC 50/60Hz from a UPS based power source.

- DC Input – a wide ranging input of 20-60VDC, nominally 24VDC.

The Chassis Power supply outputs shall cater to the PLC system requirements and feed the complete PLC or I/O Racks/Chassis.

Monitoring and control of power supply (UPS or any power source) operations via the PLC logic shall include the following, but not limited to;

Monitoring: The power supply shall allow monitoring of status and analogue values,

- Incomer Supply failure

- 24VDC Power Supply failure

6.8. INSULATION AND ISOLATION REQUIREMENTS

The PLC, including all Status inputs, control outputs analog inputs, power supply inputs and communications inputs/outputs shall meet the following insulation and isolation levels specified in IEC 255-5.

Insulation: The PLC shall be designed to withstand a Power Frequency withstand test voltage of 1.5 kV rms and shall conform to IEC 255-5 test standards.

Isolation: The PLC shall have an insulation resistance of more than 5 Mega ohms. It shall also pass an impulse withstand test of 5 kV and shall conform to IEC 255-4 test standards.

High Frequency Disturbance: The PLC shall be designed to pass a high frequency disturbance test to a 5 kV impulse test voltage and shall conform to IEC 255 test standards.

6.9. GALVANIC ISOLATOR PROTECTION

Galvanic Isolators shall be provided in PLC I/O circuits to protect the system from lightning or switching transient exposure; all analogues I/O, installed as per manufacturer specifications.

6.10. SURGE PROTECTION DEVICES

Surge protection devices (arrestors) shall be provided (on the system side) for all I/O's installed in outdoor areas.

6.11. OUTPUT ISOLATION

Isolated relay outputs shall be provided for all other discrete output requirements. Outputs that drive inductive loads shall be equipped with external "fly-back diodes circuits" designed into the output module.

6.12. FUSE PROTECTION

All output circuits shall be individually fused with fuse-status indication.

All input circuits shall be fuse-protected to minimize impact to the control system when there is an input short circuit. Individual fusing of each input is required if analysis of logical grouping of inputs is unclear.

6.13. INTERPOSING RELAYS

Interposing relays are required for all digital outputs

Interposing relays shall be grouped into AC and DC in different racks. AC switching 110 V and above shall be identified indicating the AC voltage hazard. Solenoid valves power shall be fed from the PLC cabinet.

6.14. OUTPUT FORCING

Output forcing functions shall be provided. Security measures to prevent unauthorized access by password controls shall be part of the feature.

6.15. DIAGNOSTICS

The PLC's must be capable of providing detailed system diagnostics including "smart" field device integrity from the operator and engineering workstation.

6.16. PLC OPERATING ENVIRONMENT

The PLC shall operate over the temperature range of –20deg C through to +70deg C. The PLC shall be suitable for storage over a temperature range of –20 deg C through to +80 deg C.

The PLC shall meet all relevant local requirements for noise immunity and noise emissions.

6.17. SYSTEM AVAILABILITY

The availability of the PLC systems shall be 99.99%. All single points of failures shall be eliminated.

6.18. DESIGN LIFE

PLC equipment and components shall be suitable for continuous design duty operation for a period not less than 30 years, without the need for a complete system revamp due to technological obsolescence.

6.19. SYSTEM SPARE CAPACITY AND SPARES

The system will be supplied with the following amounts of spare capacity as a minimum:

For PLC Hardware (interface, I/O cards, slots, wiring, termination and cabinet space):

- 20% spare capacity on interface, I/O cards, network switches, wired and terminated, ready to configure and use.
- 25% expansion space capacity provided in cabinets and racks for cards, terminations and termination space in the cabinets, but no hardware supplied.
- 10% Engineering Spare shall be considered for each system or at least one I/O module of each type, whichever is higher.

6.20. STANDARDIZATION OF EQUIPMENT

All equipment including PLC's, HMI servers/workstations and all other equipment which form a part of the HMI system shall be standardized wherever possible to ensure:

- Commonality of spares throughout the Terminal;
- Minimized training required on same purpose equipment.
- Economies of scale when purchasing replacement components and maintaining spares across the HMI system.
- Greater economies for maintenance and servicing support for installed equipment.

The hardware selected for HMI system described in this document shall be selected, such that the system can be completely integrated, exploiting their essential as well as best features to the maximum limits. The selection shall also ensure that the hardware components used, follow the best current industry practices in configuration, performance, networking, distribution and considering all aspects of operation and maintenance.

6.21. UTILITY AVAILABLE

240 VAC, 50 Hz Power supply from Redundant UPS Feeder providing supply to the existing panels are available.

6.22. EMC COMPLIANCE

The PLC system and all its components shall be immune to interference from electromagnetic radiation. It shall be possible to operate radio transmitting equipment at 27 MHz, 160 MHz, 453 MHz, 467 MHz and 900 MHz close to the equipment without effecting the operation of the equipment. The equipment shall be tested to IEC 255-22-3, Electrical Disturbance Tests for Measuring Relays and Protection Equipment, Test Severity Class II and Test Method C

6.23. TIME SYNCHRONIZATION

Time synchronization between PLC's and DCS system shall be achieved via NTP servers.

Whenever the DCS system Date and Time is set or reset, an automatic synchronizing signal shall be transmitted by telemetry to all PLC locations. Any PLC station subject to a "Station Failure" shall automatically time synchronize on restoration.

The DCS scan system shall send time-based poll packets periodically every 1 hour interval (system configurable parameter) to maintain time synchronization with PLC's.

6.24. CONSTRUCTION OF CABINETS

Marshalling and system cabinets shall be constructed from sheet steel be insect-, weather- and vermin-proof and conform at a minimum to IP42 protection.

Indoor Enclosures shall be corrosion resistant and painted to RAL 7035 with front access or dual (front & rear) access (if required), and lockable with a cam lock. All enclosures located outdoors shall be fitted with a sunshade to shield all vertical and horizontal surfaces of the cabinet.

A document pocket shall be provided in each cabinet for storage of documentation.

All cabinets shall be fitted with ventilation louvers and cooling fan arrangement to create forced draft ventilation through the cabinet. Each equipment cabinet shall contain an internal temperature sensing device and loss of cooling airflow detector. Both will alarm on the associated operator's console and also log at the alarm logger in the event of abnormal rack or cabinet temperature.

All cabinets shall be provided with anti-condensation heater automatically operated via the hydrostat/humidity sensor installed within each cabinet. This arrangement maintains the relative humidity in the cabinet above the dew point and prevents condensation in the cabinet or on other devices installed inside the cabinet (e.g. CPU, cards, modules …).

All castings used for cabinet construction shall be free from surface defects or other evidence of poor quality materials or poor handling or storage conditions. All edges, folds and bends shall be free from irregularities and stress cracks. The doors shall use a 3 point latching arrangement.

The configuration of all cabinets' enclosure, electronic chassis, modules and cabling shall permit ease of access to all serviceable equipment. Test equipment connections shall be adequately labelled and shall be readily accessible without the need to remove any board or portion of the equipment or power supply. All cabling, fastenings, fittings, screw heads, nuts and bolts shall be International Standard preferred sizes suitable for prolonged use in the specified field environment.

The equipment and all modules therein shall be clearly labelled in English for ease of recognition without module removal.

Power cables shall enter the bottom of the cabinets via suitable cable glands and connect to the suitable incomer terminals and internal power distribution wiring shall be installed in separate conduits. Signal cables shall enter the top of the cabinets via suitable termination assemblies.

The exposed surfaces of equipment enclosures shall exhibit a uniform finish and appearance. All metal parts shall be treated to prevent corrosion. Painted surfaces shall be cleaned, primed and undercoated prior to painting to ensure a wear resistant finish. A preparatory powder coating process is preferred.

Contact of dissimilar metals shall be avoided wherever possible and where contact unavoidably occurs, manufacturer shall state what precautions against galvanic action are proposed.

6.24.1. System Cabinet Requirements

The VENDOR'S standard system cabinets shall normally be used provide the following minimum requirements:

- Cabinets to be free standing and constructed taking into account delivery and installation requirements (multi-pin plug and sockets shall be used between shipping breaks e.g. Elco plugs)
- The mounting shall be finalized subject to final installations method.
- Overall cabinet dimensions to be 2100mm high x 800mm wide and 600/800mm deep with double front and rear (if required) removable and lockable hinged door OR only front Cabinet protection class IP 42 minimum

- Separate and isolated cabinets earthing connections shall be provided as follows:
  - Safety earth (cabinets and steelwork)
  - Signal earth (cable screens and signal common)
- The cabinet layouts are to allow full and easy access for installation and maintenance requirements
- Cabinet's cable entry shall be finalized during detailed design based on the approved cable entry installation method.
- Utility power supplies shall be provided separated from UPS such as conventional type receptacles, fluorescent Lighting.

6.24.2. Terminal Blocks

A terminal block shall be provided for every core entering or exiting the cabinet and for each wiring splice.

Internal wiring and terminal blocks shall be segregated by voltage level and type as follows:

- AC power
- DC power
- Status input
- Control output
- Analogue input
- Analogue output

All of the connections including the PC boards and the power plugs must be equipped with Locking/latching mechanism.

A barrier shall separate terminal blocks for each type of I/O signal. Terminal blocks for AC power, DC power, and I/O signals shall be separated by a minimum 25 mm space, and preferably should be on separate mounting rails.

Terminal block groups shall be labelled. Each terminal in a group shall be numbered.

Terminal blocks shall be arranged within the cabinet in vertical columns on a steel plate / panel by the VENDOR.

Every I/O point shall be wired to terminals, including spare I/O points. Wiring from the I/O card to the terminal block shall utilize VENDOR supplied pre-connected multi-core cable.

Every terminal (three each for analog input / output and control output, two each for status input) of each I/O point shall be wired to terminal blocks.

The VENDOR'S internal wiring shall be restricted to the system side of the terminal blocks. The VENDOR shall connect no more than two wires to any terminal block. The field side of the terminal blocks shall be left completely free of any wires and jumpers.

Fused terminal blocks with blown fuse indicators shall be provided for all devices requiring 24VDC power. Each device shall have an individual fused terminal block. Daisy chaining of 24VDC power from device to device shall not be accepted.

Connection of 24VDC between fused terminal blocks on the supply side shall be made by metallic jumper bar, specifically made for the purpose by the VENDOR of the terminal blocks.

AC power wiring terminal blocks shall be segregated from the control signal wiring terminal blocks.

6.24.3. Wiring and Terminations

Covered PVC ducts/wire-ways shall be provided between terminal blocks for wiring. Ducts/Wire way loading shall not exceed 30% fill at any point.

AC power and control wiring shall utilize separate wire-way from DC and I/O wiring.

I/O signal termination shall be able to accept a minimum of 1 mm2 and a maximum of 2.5 mm2 stranded copper with PVC insulation.

Power wiring shall accept a minimum of 4.0 mm2 stranded copper, 600 volt insulation. All power wiring shall be via suitable MCB's and fused terminal blocks with proper labeling of the consumers.

Wire termination shall be crimped solder-less compression spread or pin type insulated terminal lug. Any other type shall be subjected to PURCHASER approval. Non-terminated or soldered connections shall not be accepted.

Heat shrink sleeves with permanently printed wire numbers shall be placed at each end of every wire.

There shall be and adequate segregation between terminals and cables in the following categories:

- Analogue
- Digital
- Intrinsically Safe
- Serial Communication

The PLC shall contain terminal facilities for connection of 1 mm2, 1.5 mm2 and 2.5 mm2 field wiring for each I/O point. The terminations shall provide a means of circuit isolation and test access without the need for disconnection of wires.

Captive screw and saddle compression connections made from parts that are suitably treated to resist corrosion shall be used. The terminations shall be segregated according to signal type. Each terminal shall be clearly marked using a permanent marker to provide for its unique identification.

I/O board termination assemblies shall be of the plug-in variety using a suitable modular plug and socket arrangement. It shall be possible to remove and replace a faulty I/O board without the need to individually unmake and remake each circuit connection. Ribbon cable connectors shall not be used at the I/O termination boards.

A single point earth shall be provided in the PLC in the form of a bolt compression type earth lug capable of accommodating 6 mm2 earthing lugs bolted to the cabinet frame. All cabinet shall be provided with three earthing systems (Intrinsic safety earth, Instrument Earth and Dirty earth) for earthing the cabinet and Instrument earth for earthing the shielded I/O cables via suitable terminal blocks. Instrument earth shall be terminated in a dedicated, insulated bus bar inside each cabinet.

Wiring within the enclosure shall be protected from wear and tear, against accidental cuts, and from contact with enclosure parts or surfaces.

Wiring between marshalling racks to equipment rack shall be continuous runs and not be joined. No more than two wires to be connected to one terminals and only wire to be connected to each side of the terminal block, except for terminal jumpers, provided they are crimped together by the same cable lug or wire pin.

6.25. HMI AND ENGINEERING WORKSTATION

The HMI and Engineering Workstation for Process PLC and F&G system shall have minimum specifications as below.

6.25.1. HMI Workstation

- Processor -Intel® Xeon® processor E5-1603 with up to six cores
- Redundant, hot-pluggable Network interface cards
- Four Ethernet ports
- 6 USB ports on back panel
- Memory – Quad channel; Up to 128GB DDR3 memory; 8 DIMM slots
- Hard drive – 2- 500GB or greater hard drives – Installed in a RAID 1 configuration
- DVD-RW drive
- USB mouse (2 button w/ scroll) and USB keyboard
- OS License Certification Label
- On-board integrated audio
- Video: Dual graphics card (dual monitor capable) each video card provides one DVI and 2- DisplayPort outputs.
- Speakers: Two-piece stereo speakers
- Monitor – Dual, 26” TFT LCD, 1280 x 1024 pixels or better (best resolution to be recommended)

6.25.2. Engineering Workstation

- 4 Ethernet ports 2 on motherboard and 2 on an add-in dual-port NIC
- 6 USB ports on back panel
- Processor - Intel® Xeon® 5500 and 5600 series or later
- Redundant, hot-pluggable Network interface cards
- Memory –192GB (18 DIMM slots), DDR3 800MHz, 1066MHz or 1333MHz
- Hard drive – Hot pluggable, Internal storage 24TB or more, RAID 1 configuration
- DVD-RW drive
- Backup storage unit and removable 160GB cartridge

- USB mouse (2 button w/ scroll) and USB keyboard
- OS License Certification Label
- Monitor – 26" TFT LCD, 1280 x 1024 pixels or better (best resolution to be recommended)

7. QUALITY ASSURANCE

The VENDOR shall demonstrate that he operates a quality system in accordance with the ISO 9001:2000 series of requirements. The VENDOR shall ensure that his sub-suppliers operate a Quality System meeting the specified conformance criteria to ISO 9001:2000. The effectiveness of the quality system and the VENDOR's compliance with it shall be subject to monitoring by PURCHASER and in addition, may be audited following an agreed period of notice.

The VENDOR shall submit a quality control program for PURCHASER review at the time of tender.

The VENDOR shall provide facilities for and cooperate with PURCHASER and statutory authority inspectors during manufacturing, assembly and testing.

8. INSPECTION AND TESTING

8.1. GENERAL

This section describes the minimum requirements for inspection and testing and does not relieve the VENDOR of its obligations to carry out inspections required under the codes, standards and specifications listed in the enquiry documents.

All equipment supplied by the VENDOR should be subject to inspection and witness by the PURCHASER inspector and/or their authorized representative. For this purpose, the VENDOR shall submit an inspection test plan for PURCHASER's approval.

The VENDOR shall allow access and facilities to the inspectors to perform the inspections. This includes all sub-VENDORs supply.

Inspection & Testing of whole system including FAT & SAT shall be made in accordance with latest applicable standards mentioned in this document.

8.2. TESTING REQUIREMENT

All testing prior to delivery shall be carried out at the VENDOR's test facilities. Test equipment shall be supplied by the VENDOR and shall be have valid calibration certificate. The minimum scope of testing is summarized below. The VENDOR shall supply an ITP with the Tender.

The VENDOR shall provide the PURCHASER with at least one month advance notice to witness tests performed in either the VENDOR's shop. Testing shall be carried out by the VENDOR and shall be witnessed at any time by the PURCHASER or the PURCHASER's representative (the Inspector) at various stages as the system is manufactured and assembled.

Locations are detailed below:

- Pre-factory acceptance test - Conducted at the Sub-Contractors Premises
- Factory Acceptance Test (FAT) - Conducted at the Sub-Contractors Premises
- Integrated Factory Acceptance Test (IFAT) - Conducted at the Sub-Contractors Premises
- Site Acceptance Test (SAT) - Conducted at site

- Performance Test - Conducted at site.

8.2.1. Pre-FAT Testing

Prior to the FAT, the VENDOR shall complete a Pre-FAT to provide in-house validation testing and quality checks to ensure the system fully complies with the requirements as specified in codes and standards and this specification.

Pre-FAT Inventory Checks

The objective of the PLC System Pre-FAT is to ensure and confirm the following:

- That all equipment specified in the Purchaser's documentation is present for inspection.
- Vendor identification and labelling of all equipment is correct.
- That all equipment is presented in good condition and as per the specification.
- That all hardware addressing and settings are correct and as per the specification.
- That all required documentation has been submitted and approved by the Purchaser and matches the hardware delivered. A full set of approved documentation required for use during the test shall be made available by Vendor.
- That all test equipment required to carry out the FAT is available and correctly certified for use.

System "Burn In" Period

To ensure that systems are correctly burned-in and to prevent spurious failures, all components forming the PLC System are to be continually energized for a period of 48 hours at operating temperature and maximum rated load. This will require that load sinking devices shall be simulated at the I/O terminals. The Vendor is to advise the room environmental conditions during the burn-in test period, i.e. ambient temperature and humidity.

The Vendor shall make available to the Purchaser representative written confirmation of the test results including a listing of any component failures during the test and details of the failure specifics.

The QA and testing program for printed circuit boards (PCBs) electronic components, modules and sub modules should include as a minimum:

- Physical inspection after initial assembly.
- Initial functional test under power (100% of all PCBs).
- Unit assembly and coating (inspection).
- Final test and inspection (signed off by test engineer).

These tests need not be witnessed by the Company, but certification along with a detailed report on the tests shall be provided. On completion of testing the serial numbers of all equipment shall be recorded for checking on arrival at site. The results of the pre-FAT shall form part of the Manufacturers Data Report.

8.2.2. Factory Acceptance Test

The objective of the FAT of PLC System is to ensure and confirm the following:

- All deliverable items, i.e. hardware, operating system software, documentation, media etc, are present and acceptable.
- The correct functioning of the PLC System is in accordance with the functional specification, including all interfaces to other equipment and sub-systems.
- The system operates under simulated load conditions over the test period at or better than design availability.
- The system can tolerate failure of individual modules and sub-systems and be recovered to full function following repair and reinstatement of such items.

The VENDOR shall be responsible for generating the FAT procedures. The VENDOR shall submit the proposed FAT procedures to the PURCHASER approval 3 months before scheduled date of FAT commencement.

The FAT shall include the testing and acceptance of both hardware and proprietary system software. All proprietary system software shall be complete and resident in the System prior to the start of FAT.

All equipment shall be energized and remain energized for the duration of this test. This includes any externally powered equipment.

The FAT of both DCS and PLC System shall include the testing and acceptance of both hardware and proprietary system software. All proprietary system software shall be complete and resident in the System prior to the start of FAT. All documentation and listings must be free of mark-ups.

All equipment shall be energized and remain energized for the duration of this test. This includes any externally powered equipment. Dummy loads shall be fitted in all loops where this is necessary for observing the correct functioning of a loop. These dummy loads shall remain fitted to all circuits except the circuit under test. Outputs shall be connected to a device as similar as possible to the final field element (eg. relay coil etc.).

All loops in the system shall be tested by applying a simulated signal (or signals in the case of complex loops) at the terminal strip on a panel and observing the effect on the Engineering Workstation. Outputs should also be manipulated and the result measured again from a marshalling panel.

The Purchaser will reserve the right to witness the entire FAT as a non-participating observer. The FAT procedure will be signed off by the Vendor and the Purchaser and a copy of the signed off FAT procedures and related printouts shall be furnished to the Purchaser at the successful conclusion of the FAT.

8.2.3. FAT Hardware Testing

The testing of the hardware shall be detailed on the approved testing procedure and shall include the following as a minimum:

- Module Testing
- Diagnostic routines
- Redundant module software download testing

- Power failure and recovery testing of redundant modules.
- Power failure and recovery testing of single modules.
- On-Line replacement testing.
- Battery backup tests.
- Black start recovery testing.
- Field Terminations Testing
- Termination and panel wiring insulation tests.
- Power, Fusing & Earthing Checks
- Safety earth continuity tests
- Instrument earth continuity checks
- Power supply redundancy tests
- Power supply over current protection tests
- Power supply over voltage protection tests.

8.2.4. EMC Emission and Susceptibility Testing

The Vendor shall demonstrate that a representative configuration of the equipment, sub-system or system required is capable of meeting the test requirements described in the EMC requirements part of this document. Tests shall be carried out by the PLC System Vendor on individual items of equipment or assembled sub-systems with all ancillary items and interconnecting cables connected and tested in accordance with the test procedure and conditions specified.

Alternatively a certificate confirming compliance to the tests shall be supplied for each item of equipment or sub-system tested, giving details of all test equipment used with type and calibration details, the test configuration arrangement, the test site used and the name of the testing authority.

Vendor shall supply a hand-held UHF radio for use in the vicinity of the PLC System to demonstrate that RFI does not affect the system. No other non-standard tests are required.

I/O Testing

Vendor shall test all I/O from the field cable terminals of the cabinet terminals, and observe all responses within the logic using the Engineering Work Station.

The I/O tests shall ensure that:

- All I/O are correctly addressed and connected to designated field cabinet terminals.

- Mainly all I/O are supplied with field circuit power from the PLC System power supplies.

- All Inputs respond correctly to Open circuit and Closed Circuit at the field terminals.

- All Analog Inputs respond correctly over the full range of signal input and monitored contact switching thresholds (between Open Circuit, Open Contact, Closed Contact and Short Circuit) are in accordance with the design.

- All monitored Outputs provide correct alarm response to open circuit at the field terminals.

- All Digital Outputs can be forced On/Off from the EWS.

8.2.5. Integrated Factory Acceptance Test

After completion of the satisfactory system FAT of the DCS and PLC systems test the systems will be delivered to, assembled and interconnected at a staging EPC subcontractor Workshop

The assembled systems shall be tested under conditions that reproduce as nearly as practicable the conditions anticipated at site, and will demonstrate that the overall system operates as specified.

All I/O from all systems shall be connected either to field devices or test equipment to accurately emulate operating conditions.

System Integration Testing will involve testing teams from multiple Vendors, and will require cooperation and co-ordination.

The DCS and PLC Vendor shall be responsible for providing the test procedures, test equipment and suitably qualified personnel to carry out the system testing, including monitoring of relevant DCS displays. The DCS vendor will be responsible for correcting any DCS configuration errors identified by the F&G or other testing teams.

VENDOR shall provide all necessary hardware, software and technical assistance to troubleshoot hardware, software issues during IFAT.

IFAT procedure shall be issued for Company approval.

8.2.6. Site Acceptance Tests

The site acceptance test procedure shall be developed by the VENDOR and approved by PURCHASER and shall demonstrate that the completely assembled and installed system operates successfully under real conditions on the real process fluid, and communicates properly with the live control system.

The purpose of the SAT is also to establish that the system cabinets/equipment has been shipped without damage, has been correctly installed, and operates reliably to specification in its final environment.

The VENDOR shall be responsible for maintaining detailed test records for all inspection and testing carried out in the format agreed in the SAT procedures documentation.

The SAT test specification shall reflect the structure and the phasing of the testing starting with inventory checks and hardware tests through software testing to final testing of a fully integrated system of hardware and software.

Objectives

- Ensure that all deliverable items, hardware, software, documentation, media, etc are present and acceptable.
- The correct functioning of the overall DCS and PLC System in accordance with the applicable functional specifications, including all interfaces to other equipment and sub-systems on the final power supply and earthing system.
- The system operates under load conditions over the test period at or better than design availability.
- The system can tolerate failure of individual modules and sub-systems and be recovered to full function following repair and re-instatement of such items.
- That all timer settings and alarm/trip set points that may have been modified for the purposes of FAT have been re-configured to their correct values.
- That all remedial punch-list work agreed at the FAT has been satisfactorily completed by Vendor and the systems meet its design specification in full.
- The Operator interface is both safe and operable with respect to the presentation of data and alarms and the implementation of control.

Hardware Testing

- Test for correct installation and configuration of all redundant equipment by carrying out forced failure and recovery testing. This testing is to extend to all network communications cables, power distributions, gateways and switches, hubs and media converters.
- Any equipment added or replaced since the FAT shall be fully tested.
- Power distribution, fusing, segregation and earthing checks.
- PLC/UPS tests including in-rush, mains failure, static switch failure, battery discharge, voltage and frequency variation.
- Check for ancillary equipment interference, e.g. HVAC thermostats, lighting dimmers, radios.
- Check operation and performance of all connected sub-systems. In particular those not previously tested.

Software Testing

Any software which has been subject to remedial work since FAT should be thoroughly re-tested including any potential impacts on unmodified software. Similarly any software added since FAT shall be fully tested.

A random sample of Loops, to be chosen by the Purchaser, representing approximately 50% of the total user software shall be retested during SAT, requiring manipulation in the field of physical input devices (transmitters and other sensors) and field observation of the actions of final output devices (valves etc).

These tests shall be conducted without the use of the DCS and PLC System Engineering Workstation or any other simulation devices, and shall use the time delays and set-points specified for final operation.

8.2.7. Performance and Availability Test

After the completion of the Site Acceptance Test, entire system shall be subject to a performance test. CONTRACTOR shall start up and operate the system for a minimum trial period to ensure that it operates correctly, and shall test all functions of the system, including the software, to and ensure that it operates in accordance with the requirements of the design specification/relevant standards, prior to actual commissioning and handing over to ADCO.

The duration for performance test shall be agreed between PURCHASER and VENDOR at Bid stage (however not less than two weeks).

The availability test will be conducted by the PURCHASER and will consist of monitoring the system availability during the sixty-day period.

If the system does not meet the availability and performance requirement during the test conducted by the PURCHASER, the VENDOR shall be responsible for repairing or upgrading the system (at the VENDOR's expense) in order to meet the requirement.

The PURCHASER will then repeat the availability test.

9. SITE SERVICES

The contractor shall provide the following services as per contract:

- Manpower for all site activities
- Pre installation checks
- Execution of the scope,
- Pre-power on checks, and power up
- Pre-commissioning
- System Start Up/Commissioning
- Site Acceptance Testing /System handover

9.1. INSTALLATION, START-UP, COMMISSIONING & HANDOVER

The VENDOR, in their tender, shall identify any special requirements or recommendations for VENDOR support during commissioning and startup of the equipment supplied. The PURCHASER's final acceptance of the equipment will be subject to a performance and availability tests once the equipment has been installed and commissioned.

Both the installation and the commissioning activities shall be undertaken as a single continuous operation. Upon completion of the installation activity, EPC SUB CONTRACTOR shall Test, Start-up, Commission and Handover the system to ADCO.

The VENDOR shall make available the services of experienced start-up engineers to assist with the installation of the system in addition to the initialization of system power and provide support during the commissioning of the system and also ensure general system troubleshooting assistance.

9.2. COMMISSIONING

Commissioning of the system shall constitute practical completion following the satisfactory completion of installation, testing and start up.

EPC SUB CONTRACTOR shall demonstrate to the client that the system successfully performs all of the functions set out in the design specification.

Complete Commissioning reports shall be submitted as part of Project Dossier.

EPC SUB CONTRACTOR shall present an Acceptance Certificate for signature by ADCO.

9.3. HANDOVER

EPC SUB CONTRACTOR, upon completion of the commissioning activity, shall hand over the system to the client. At the time of hand over, EPC SUB CONTRACTOR shall provide the client with the following documentation :

Project Dossier (as per ADCO standards) which shall include as minimum:

- Construction Records
- Component and equipment list
- Product description sheets
- System design specification / System design drawing(s)
- As built drawings and power distribution
- System schematic diagram(s)
- System operating and service manuals
- Spare parts list
- Certificate of commissioning

10. TRAINING

CONTRACTOR shall provide training to personnel who operate and maintain the DCS and PLC system and provide the training manuals as part of final documentation – both hard and soft copies.

Work Group	Level (with the number of attendees)	
	Basic	Advanced (Engineering)
Maintenance Training	15	10
Operation Training	30	0

10.1. OPERATION TRAINING

- System Overview User Interface
- Regional, Language, Video, Display Settings; Sound and Audio Devices; Help Functions; Printers
- Menu Navigation System Menus
- User, Roles and Groups, Point of Control
- Alert and Alarm Handling; Filtering, Alert Tracking
- F&G Panels
- Cause & Effect and Operation
- Bypass / Override
- Trend Viewer, Reports
- System Diagnosis Screens
- System Interfaces from an Operators point of view

10.2. MAINTENANCE TRAINING BASIC LEVEL

- Technical System Overview
- System Menu Options
- System Startup / Shutdown
- System Back-Up
- Bypass / Override
- Basics of Monitoring and Diagnosis
- Overview of redundant systems (H/F differences, availability, redundant systems)

- PLC system design and I/O, synchronization, connection and updating of the system, principle of operation, error handling
- Hardware configuration (system parameterization, system handling, fault diagnostic, documentation)
- Exercise of I/O configuration and troubleshooting, programming examples
- PLC software basic operations
- PLC software block types and program structure
- Programming parameter-assignable blocks
- Data management with data blocks
- Programming organization blocks
- Testing (debugging) tools for system info, troubleshooting and diagnostics
- Hardware configuration Program documentation and backup

10.3. MAINTENANCE TRAINING ADVANCED LEVEL

- Technical System Overview
- System concept
- System Menu Options
- System and Process Startup / Shutdown
- System Back-Up
- Restore Operations
- System Upgrades, Patches, Service Packs
- Redundancy, Automatic and Manual Switch Over
- System Monitoring and Diagnosis
- Point of Control Maintenance
- OPC interface
- Application Errors and Trouble Shooting
- Fault Diagnosis and Log Files
- Settings and Parameters

- System Interfaces
- Software Architecture, used / configured project Modules
- Control programming
- Defined scripts
- Use libraries and functions
- Graphical objects
- Panels
- Database
- Panel Topology
- Test and Introduction of Changes to the System

PLC system

- Aids for program creation (e.g. structure program)
- Functions, function blocks and multi-instances
- Jump commands and accumulator operations
- Indirect addressing
- Error handling with error organization blocks
- Evaluating diagnostics data
- Troubleshooting and messages
- Analog value processing
- Test and Introduction of Changes to the System

11. EXECUTION WORK PROGRAM

The bidder shall submit work execution program as part of his technical offer indicating the required partial / complete shutdown of the existing system and indicating any temporary measures which may be implemented to reduce the partial / complete shutdown period(s).

12. SPARE PARTS AND SPECIAL TOOLS

12.1. SPARE PARTS

The Vendor shall identify and supply the following spares as noted below:

- Pre-commissioning, commissioning and start-up spares including software licenses (Supply is included in the scope of VENDOR)
- Recommended spares list for two years operation (Submission of Priced SPIR only).

The Vendor shall supply the following spares for DCS and PLC system as below;

15% spares supplied for each type of cards, terminations and physical slots available for use, but not installed. Note: This spare does not constitute of two (2) year operational spare parts which shall be recommended by the VENDOR.

The spare parts list (SPIR) shall be submitted for Company approval following ADCO SPIR format.

12.2. SPECIAL TOOLS

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 specialized procedures.

Standard equipment includes items available from standard catalogues. The list of the standard tools and testing and calibration equipment required shall state the following:

- Description of its service or simulation application
- Manufacturer and Catalogue No.
- Quantity recommended.
- Special tools shall be itemized and priced with the Tender.
- The PURCHASER shall agree the Special Tools to be included in Purchase Order.

The VENDOR shall provide design and performance specifications for all Software, which is used for the F&G PLC System.

13. SPECIAL REQUIREMENTS

13.1. SURFACE PREPARATION FINISH

Painting shall in accordance with ADCO Spec. ES 30.99.37.0013 - Painting & Coating of New Equipment. The paint system shall be selected as per the referred ADCO spec.

Where operating conditions are not suitable for the specified system, VENDOR shall specify a suitable alternative (subject to ADCO's approval)

The final color shall be selected as per the ADCO specification.

MANUFACTURER own standard, with PURCHASER's approval, may be used if it meets or exceeds the ADCO Spec. ES 30.99.37.0013.

13.2. NAME PLATE DETAIL

All equipment's shall be supplied tagged in accordance with ADCO EP 30.99.00.0001 Engineering Specification - Tag Plates for Field & Indoor Equipment's.

Tag plates shall be manufactured from 316L stainless steel. Text and numbering shall be clearly engraved, paint filled and a minimum of 6mm high.

Tag plates for accessories shall be secured using stainless steel screws, stainless steel wire or stainless steel chain.

The primary nameplate shall be mounted in a prominent location secured by stainless steel screws or rivets. The nameplate shall contain the following minimum information:

- Client name
- Project name
- Purchase order number
- Equipment title
- Equipment tag number
- Manufacturer's Name
- Serial number
- Year built
- Certified Weight (kg)

14. ORIGINAL EQUIPMENT'S MANUFACTURER

The contractor shall execute the installation; start up, commissioning and the trial period under the direct supervision of the original equipment manufacturer.

The required training shall be carried out by the OEM.

15. PACKING, PRESERVATION AND PREPARATION FOR SHIPMENT

The VENDOR shall prepare the equipment for export shipment, in accordance with the applicable QA/QC procedures.

Documents, including unloading, unpacking and lifting instructions, a description of the reassembly steps required for installation and pre-commissioning and start up instructions shall be included with the package. The number of copies of documents to be provided shall be as stated in the Contract.

VENDOR shall ensure the equipment is suitably supported and braced for transport. Prior to shipment, all high accuracy skid mounted instrumentation and other equipment vulnerable to damage shall be disassembled and boxed separately and send with the skid

The VENDOR shall recommend preservation requirements for idle periods of non-operation up to 6 months for protection against rain, moisture, dirt, blasting grit etc.

VENDOR shall provide all necessary documentation for import of equipment into UAE.
The VENDOR/MANUFACTURER shall provide a complete packaging and handling specification to cover both skid and electronic panels.

One copy of the IOM manual shall be shipped with the systems.

16. DOCUMENTATION

The Contractor shall be responsible for providing all documentation in accordance with the Contract,

The contractor shall provide any document required to design, construct and test the system and as minimum to supply the followings:

- Datasheets
- Specifications
- General Arrangement Drawings
- Wiring Diagrams
- Cable Schedule
- I/O List
- Electrical Power Distribution Diagram
- Bill of Materials
- Functional Design Specifications
- Factory Acceptance Test Plan
- Factory Acceptance Test Procedure
- Site Acceptance Test Plan
- Site Acceptance Test Procedure
- System Performance Specifications
- Recommended Start-Up/Commissioning and Operational Spare Parts List (as per ADCO template)
- Functional Test Certificates
- Installation Operating Manual
- Vendor Data Books

- Manufacturer Data Books
- Maintenance Manuals
- As-Built Mark up and Project Dossier

Tender-(Proposal) Documentation

Tender proposal documentation shall include the following:

- Full technical literature for the equipment offered.
- A list of all accessory items together with MANUFACTURER's name and part number.
- The VENDOR shall provide a completed copy of the data sheets with all changes entered.
- Fabrication / Production schedule
- The VENDOR shall separately detail each proposed deviation from the specification, data sheets,
- Technical Requisition, and submit to the PURCHASER for approval.

APPENDIX 3: INTEGRATED CONTROL AND SAFETY SYSTEM (ICSS) SPECIFICATION FOR SUPPLIERS

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae
أدنوك البرية
ADNOC Onshore

INFORMATION TECHNOLOGY DIVISION (ITD)
IT SECURITY COMPLIANCE

ENGINEERING SPECIFICATION

Integrated Control and Safety System (ICSS) Security Specification for Suppliers

DOC. No. 30-99-39-0020

Approved:

VP(IT) & VPTC(ENG)

ENGINEERING SPECIFICATION
ICSS Security Specifications for Suppliers

Document Control

Control Document Information:

Document Owner	IT Security Compliance
Document Author	Senior IT Security Analyst
Document Custodian	IT Security Compliance & Draughting Team
Document Security Code	4 – Internal Confidential
Document Number	30-99-39-0020

This is a controlled document and being maintained on electronic media. Any hard copies made are considered uncontrolled and may not be the latest version. Any employee of ADNOC Onshore, and its authorised Third Parties, are responsible for ensuring they are referring and using the latest version of the record and conform to the Copyright information.

	Name	Signature	Position	Date
Prepared By	**Bensy Alexander**		**ITSA**	
Reviewed By	**Riju Eratta**		**ITSA**	
Reviewed By	**Mohamed Abdulla Shurafa**		**ITSA**	
Reviewed By	**Imran Abdulla Al Marzooqi**		**TL ITSC**	
Reviewed By	**Florentin Lupu**		**SEI&C**	
Reviewed By	**Bimal Thakkar**		**SEI&C**	
Reviewed By	**Amna Nawfal Abdulla**		**SEI&C**	
Reviewed By	**Hani Bakr Osman**		**CE (IC)**	
Approved By	**Arif Ahmed Al Rashedi**		**VPTC (E)**	

ENGINEERING SPECIFICATION
ICSS Security Specifications for Suppliers

For ADNOC Onshore internal permissions please refer to the Delegation of Operational Authorities.

The table below is a brief summary of the most recent revisions to this document. Details of all revisions are held on document by the issuing department.

Sr. No.	Rev. No.	Date	Description of revision
1	2	15-April-2018	Revision to incorporate additional requirements.

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي, الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

ENGINEERING SPECIFICATION
ICSS Security Specifications for Suppliers

TABLE OF CONTENT

Abu Dhabi Company for Onshore Petroleum Operations Ltd, شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

1 INTRODUCTION

1.1 Purpose

This specification defines the minimum requirements for the security of Integrated Control & Safety Systems (ICSS) and any other industrial automation and control system (IACS) to be supplied for use in Abu Dhabi Company for Onshore Petroleum Operations Ltd. (Trading as ADNOC Onshore) and is applicable to suppliers supplying such systems or services on such systems.

1.2 Scope

ADNOC Onshore and its nominated consultants, Contractors, vendors, suppliers and manufacturers responsible for the design, modification and engineering of ICSS or IACS, intend this specification for use.

The security specification shall apply but not limited to the following systems:

- Integrated Control & Safety Systems (ICSS);
- Distributed Control System (DCS);
- Supervisory Control and Data Acquisition Systems (SCADA);
- Fire & Gas system (F&G);
- Emergency Shut Down (ESD) systems;
- Third Party systems and Programmable Logic Controllers (PLC) integrated to the ICSS, DCS/SCADA;
- Supporting network infrastructure, security infrastructure, applications and software;
- Any other Industrial Automation & Control System (IACS) under the scope of the project.

For the purpose of this document, the term ***Integrated Control and Safety System (ICSS)*** would include all the Industrial Control Automation & Safety Systems including the related sub systems and third party integrations implemented within the respective Asset / Terminal of ADNOC Onshore.

The scope of implementation shall include all ICSS related infrastructure components in the scope of the project which include but not limited to controllers, PLC's, servers, PC's, workstations, laptops, switches, routers, security devices and appliances.

1.3 ADNOC Onshore Guidelines & Specifications

Document Number	Document Title
ES 30-99-52-012	Basis of Design for Concept and FEED
30-99-68-0030	Call Processing System With Unified Messaging
30-99-74-0092	Applicable Telecommunications Standards
30-99-90-0076	Field Telecom Network Engineering Guidelines
30-99-90-0077	Field Wide Transport Network Guidelines

30-99-90-0078	Fixed Voice Communication
30-99-90-0079	Mobile Voice Communication Engineering Guidelines
30-99-90-0079	Wireless Broadband Guidelines
30-99-90-0081	Industrial PAGA System
30-99-90-0082	Industrial CCTV System Engineering Guidelines
30-99-90-0083	Industrial Access Control System
30-99-90-0087	Meteorological System Engineering Guidelines

1.4 International Codes and Standards

The following codes and standards will serve as reference material for the design of security for ICSS in ADNOC Onshore projects. In case of conflict with the ADNOC Onshore guidelines and specifications, the latter shall prevail.

1.4.1 Shell DEP

DEP 32.01.23.17 Process Control Domain – Security Requirements for Suppliers

1.4.2 International Electrotechnical Commission (IEC)

IEC 62443 Industrial Automation and Control Systems (IACS) Security

1.4.3 International Organization for Standardization (ISO)

ISO 27001 Information security management systems — Requirements

1.4.4 International Society of Automation (ISA)

ISA 62443 (formerly ISA 99) Security for Industrial Automation and Control Systems

1.5 Other Standards

- UAE Information Assurance Standard (IAS)
  Relevant and applicable ADNOC Standards and Guidelines would apply.

1.6 Environmental Conditions

The following environmental data are typical on ADNOC Onshore assets. They shall be used to specify the operating conditions of electrical/electronic equipment and cables for ADNOC Onshore projects.

Item	Operating Condition
Wind	Prevailing Direction is From NW
Mean Speed	8.0 m/s
Maximum/design speed	44.7 m/s
Particulate borne	Sulphurous dust & sand

Temperature	Maximum Solar: 85°C
	Maximum Shade: 58°C
	Minimum Shade: 4°C
	Average Shade
	Summer: 36°C
	Winter: 22°C
	Yearly: 28°C
	Max. Soil at 1m depth: 38°C
	Min. Soil at 1m depth:13°C
Air Temperatures for design of various equipment under shade (or indoor)	
Air Coolers in main process	46°C
Air Coolers – others	58°C
Air Coolers – process design approach to ambient	10°C
Gas Turbines	60°C
Elec. generators/ motors	55°C
Electrical equipment	52°C
Instrumentation equipment	60°C
Control Equipment room design temperature	42°C
Passive cooled shelter's design condition	40°C
Air compressor	46°C
Diesel / gas engines	58°C
Relative Max. at 43°C	95%
Average at 53°C	60%
Solar Radiation	946 W/m2 (300 BTU/h/ft2)
Rainfall	Infrequent
Maximum	51 mm/year

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي, الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Minimum	Trace
Highest Rate	25 mm in 24 hours (January-April)
Dew	Heavy
Mists	Early morning mists causing Evaporative cooling losses
Design ambient temperatures for electrical cables	
Underground cable (buried)	40°C
In concrete trench	54°C
Soil thermal resistivity	2.5 °C m/w

Note 1: Electrical/electronic equipment and cables shall be located away from direct sunlight wherever possible. Equipment located outside shall be provided with sunshades made of non-metallic UV resistant material to protect the equipment from solar heat gain.

Note 2: Electrical/electronic equipment and cables located outdoors shall be rated for continuous operation in an ambient shaded temperature of 60°C.

1.7 Definitions

Shall	The word 'shall' indicates a mandatory requirement.
Should	The word 'should' indicates a preferred course of action.
May	The word 'may' indicates a possible course of action.
Company	Refers to ADNOC Onshore.
Contractor	The party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility.
DMZ	Demilitarized Zone is used to identify a location in the network where a computer is configured outside the inner-firewall but inside the outer-firewall.
IT Component	Unless specifically mentioned, all IT components referred to in this document are considered part of the process control domain.
Manufacturer / ICSS Vendor	The party responsible for the manufacture of equipment or material to perform the duties specified by the Contractor or the company.
Vendor / Supplier	The party responsible for the supply of equipment, material or product-related services in accordance with the purchase order issued by/for ADNOC Onshore.
System	A combination of hardware and software components, which together provides a function or service. Where 'its systems' is used, this refers

	to all systems supplied and supported by the Supplier over the systems lifecycle.
Network Device	Electronic equipment that connects or manages network traffic; e.g. Switches & routers.
Network Security Barrier	A network device that implements access controls and/or network security policy between two or more network security zones.
Remotely operated equipment	Refers to PLC's, RTU's in the remote locations such as fields, clusters, RDS's and well heads.

1.8 Abbreviations

ACL	Access Control List
AES	Advanced Encryption Standard
AV	Anti-Virus
PDB	Power Distribution Board
CDS	Central Degassing Station
CMS	Condition Monitoring System
CR	Control Room
CCS	Compressor Control System
DC	Direct Current
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
EPC	Engineering Procurement Construction
EWS	Engineering Work Station
ER	Equipment Room
ESD	Emergency Shutdown (System)
FAT	Factory Acceptance Test
F&G	Fire and Gas System
FACP	Fire Alarm Control Panel
FDIS	Field Data Integration System
FEED	Front-End Engineering and Design
GPS	Global Positioning System
HAZOP	Hazard and Operability Study
HSSD	High Sensitivity Smoke Detector

HIPPS	High Integrity Pressure Protection System
HMI	Human Machine Interface
HSE	Health, Safety & Environment
IACS	Industrial Automation & Control System
IAS	Information Assurance Standard
ICS	Industrial Control System
IAOM	Integrated Asset Operation Model
I&C	Instrument & Control
IS	Intrinsically Safe
I/O	Input / Output
ICSS	Integrated Control and Safety System
JB	Junction Box
OPC	OLE for Process Control
OLE	Object Linking and Embedding
OT	Operational Technology
LAN	Local Area Network
PAGA	Public Alarm and General Alarm
PCS	Process Control System
PCD	Process Control Domain
PCN	Process Control Network
P&ID	Piping & Instrumentation Diagram
PIES	Production, Injection and Export System
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PS	Power Supply
RDS	Remote Degassing Station
RTU	Remote Telemetry Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control And Data Acquisition
SCMS	Substation Control & Monitoring System
SDLC	System Development Life Cycle
SDV	Shutdown Valve
SIA	Signals Intelligence Agency
SIEM	Security Incident and Event Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SNMP	Simple Network Management Protocol

SSID	Service Set Identifier
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
UPS	Uninterruptible Power Supply
UA	Unified Architecture
WAN	Wide Area Network
WHCP	Well Head Control Panel
WIDA	Well Integrity Data Assessment system
WMI	Windows Management Instrumentation

2 Deviations

Where there is a discrepancy and/ or conflict between the security specifications and other codes or standards, the Contractor shall highlight the conflict to ADNOC Onshore for advice prior to finalisation of project bid. In general, the most stringent requirement may apply on conflict scenarios.

3 ICSS Cyber Security Specifications

3.1 General Conditions

This specification shall be used in conjunction with the specifications and scope of work of the project.

If security solutions and software as required in the specifications already exist within the process control environment the Contractor shall conduct a site survey, review existing solutions implemented at site and propose solutions to ensure that the proposed control systems integrate with already implemented security solutions where possible. The Contractor shall provide additional licenses where required to integrate the new nodes that are supplied as part of the project with the installed security solutions at site. The final Bill of Materials should be discussed with ADNOC Onshore IT Security Compliance team after the site survey before finalisation.

For modification to existing systems that contain cyber security solutions implemented within the network, the Contractor and ADNOC Onshore shall agree and approve the relevant and applicable security specification requirements that are required to meet the cyber security objectives of the project before proposing the Bill of Material.

Any new ICSS that requires integration or interconnection with an existing system in ADNOC Onshore, it shall be ensured that such integration / interconnection will not affect the performance and functionality of existing ICSS.

Ownership of all licenses procured as part of the project shall be transferred to ADNOC Onshore as part of commissioning and handover.

3.2 Cyber Security Project Management

3.2.1 The Contractor shall ensure that during project execution a security lead with sufficient ICSS security competency (minimum 3 years' experience in ICSS security) is assigned to the project. The security lead shall instruct the implementation team including personnel within its organization, subcontractors, and consultants about the requirement of these specifications prior to being authorized access to the ADNOC Onshore's ICSS. All official correspondence shall be through the assigned project manager. CV's of the security lead and engineers shall be provided.

3.2.2 The Contractor shall sign relevant Acceptable Usage and confidentiality agreements and shall agree to follow applicable ADNOC Onshore policies, procedures and standards.

3.2.3 The Contractor staff including subcontractor personnel shall agree to sign ADNOC Onshore ICSS Acceptable Usage Policy Undertaking during project execution phase in order to agree compliance to ICSS Security Policies and procedures.

3.2.4 The Contractor shall conduct security-related background checks on all personnel before they are assigned to ADNOC Onshore projects.

3.2.5 Requirements of the ICSS security specifications shall be verified during the FAT and SAT stages of the project by ADNOC Onshore IT Security Compliance team.

3.3 Factory Acceptance Test (FAT)

3.3.1 The Contractor shall provide a Cyber Security FAT procedure for ADNOC Onshore review and approval at least one month prior to FAT.

3.3.2 Prior to initiation of FAT, the Contractor shall install all latest, supported and compatible Operating Systems, patches, service packs and latest version of the software and applications, or other updates certified for use with the provided system.

3.3.3 Cyber Security FAT shall be conducted and verified by ADNOC Onshore.

3.3.4 The Contractor shall demonstrate during the FAT a successful backup and restoration of the ICSS.

3.3.5 The Contractor shall rectify any failures, deficiencies and faults identified during FAT without any cost and project schedule impact.

3.4 Site Acceptance Test (SAT)

3.4.1 The vendor shall provide a Cyber Security SAT procedure for ADNOC Onshore review and approval at least one month prior to SAT.

3.4.2 The Contractor shall verify and test during the SAT phase that the current operations and control system performance is not impacted with the introduction of cyber security solutions.

3.4.3 The Contractor shall ensure that the ICSS system is malware free before commissioning of the system.

3.4.4 The Contractor shall demonstrate during the SAT a successful backup and restoration of the ICSS.

3.4.5 Performance related tests on the ICSS with the introduction of cyber security solutions shall be added to the SAT procedure.

3.4.6 The Contractor shall rectify any failures, deficiencies and faults identified during FAT without any cost and project schedule impact.

3.5 System Hardening

3.5.1 The Contractor shall document the security hardening configuration settings for all IT infrastructure components, including but not limited to:

- Windows Operating System;
- Network devices such as routers and switches;
- Security devices such as firewalls;
- ICSS Application.

Hardening baseline document shall be reviewed and approved by ADNOC Onshore IT Security team.
Note 3: The Contractor shall provide AS BUILT documentation of the hardening document.

3.5.2 The CONTRACTOR hardening standards shall be based on international benchmarks such as Center for Internet Security (CIS), NSA Security Configuration Guides or DISA

STIG, which are tested and approved by the ICSS automation vendor on their system(s).

3.5.3 The Contractor shall remove and/or disable all software utilities and ports that are not required for the operation and maintenance of the ICSS prior to commissioning.

3.5.4 Contractor shall remove / uninstall software and functionality that is not required by ADNOC Onshore for the intended functional purpose of the system and business purpose; e.g. E-mail, office applications, games, messaging services, unused drivers, USB ports, Bluetooth and Wi-Fi communication etc.

3.5.5 Remote Diagnostic and configuration ports (if any) on devices shall be disabled unless requested and approved by ADNOC Onshore in writing.

3.5.6 All unused ports on switches and routers shall be disabled to prevent unauthorized access to the ICSS network infrastructure.

3.5.7 Temporary user accounts used during commissioning and testing shall be removed at the end of the activity.

3.5.8 Built in generic administrator level account shall not be used by default by the ICSS to run services (if any). A dedicated “service” account shall be created with the minimum privileges necessary for running the service.

3.6 Infrastructure Requirements

3.6.1 Infrastructure Redundancy Requirements:

- Redundant servers shall be provided for Active Directory infrastructure;
- Redundancy shall be provided for all firewalls and switches in the network;
- Servers performing the following functionality shall not be clubbed with other systems unless the technical limitation is approved by ADNOC Onshore:
  - ✓ Anti-Virus;
  - ✓ Patch Management;
  - ✓ Log Management;
  - ✓ Active Directory.

3.6.2 Operating System

- The Contractor shall ensure that the installed operating system version is not out of support or not announced by the manufacturer 5 years from of detailed engineering sign off.

3.6.3 All infrastructure components such as servers, switches and databases shall be procured as per the recommendations of the solution Manufacturer to ensure compatibility with the installed software / application and to meet capacity requirements. The latest supported version and model shall be provided.

3.6.4 The servers shall be sized to have at least 50% spare capacity of memory, CPU and hard disk space.

3.6.5 Firewalls shall be sized to have at least 50% spare capacity in bandwidth and interfaces.

3.6.6 Network devices shall be sized to have at least 30% capacity in spare ports.

3.7 Network Controls

3.7.1 The Contractor shall zone the process control network thereby partitioning the network and grouping devices with the same functionality to implement a secure zoning and conduit model.

The Contractor shall work with ADNOC Onshore to discuss and finalize the zoning model and architecture before finalization of the architecture. (**Note 4**: The Contractor shall use relevant standards and best practices such as IEC 62443, ISA 99, Shell DEP & Appendix A1 ICSS – General Architecture as the basis for the proposed architecture.

3.7.2 The Contractor shall provide ICSS protocol compatible firewalls to enforce access control between the defined zones.
Note 5: The Contractor shall communicate with ADNOC Onshore the specifications of the ICSS firewall for review and approval.

3.7.3 The proposed firewall shall not cause degradation and latency to the ICSS network outside the prescribed performance requirements as defined in the project specific specification.

3.7.4 The proposed firewalls shall be tested and approved by the ICSS manufacturer.

3.7.5 The Contractor shall segregate the ICSS Engineering workstations in a separate zone and enforce network security barrier between the engineering workstation zone and Human Machine Interface (HMI) zone (applicable to dedicated Engineering Stations). Where HMI and Engineering stations are combined in the same machine separate user accounts and authorization levels must be configured to segregate the access.

3.7.6 Maintenance Laptops must be installed with anti-virus, patch updates and other applicable controls as required and applicable to an Engineering Station.

3.7.7 The Contractor shall configure the controller such that it would accept configuration changes only from authorized engineering workstations. Controls can be implemented either in the controller or in the network security barrier to prevent configuration change commands from any unauthorized system.

3.7.8 Network devices shall provide the capability to configure AES or equivalent password encryption within the device.

3.7.9 The Contractor shall configure encryption for administration of network devices within the process control network over Ethernet.

3.7.10 The ICSS system shall be capable of collecting Historian data, using an open standard communication protocol with embedded security such as OPC, OPC UA, XI, SSL etc.

3.7.11 The Contractor shall provide time-synchronization from a secure and accurate source; e.g. via a Network Time Protocol (NTP) server, GPS Clock etc. (**Note 6**: To be considered if not already mentioned in the project scope of work / specifications).

Note 7: For remotely operated control system equipment time synchronization via Modbus / DNP3 communication protocols will be accepted if the systems cannot be integrated to the centralized time clock.

3.7.12 It is recommended that Process control network and safety network not to terminate on the same switch to ensure that two separate networks are maintained. (**Note 8**: To be considered if not already mentioned in the project scope of work / specifications)

3.7.13 Any requirement as part of the scope of work for one-way data transfer originating from the ICSS Network to Corporate IT shall be compliant with the existing ADNOC Onshore Plant Information (PI) System.

3.7.14 The Contractor shall supply and implement approved and compatible Data Diode between the ICSS Network and IT Network if the data cannot be channeled through the existing PI solution.

3.7.15 Any requirement for interconnectivity to Corporate IT Network from the ICSS Network shall be approved by the IT Security Compliance team prior to finalization of network design.

3.7.16 The Contractor shall provide the additional hardware and software licenses required for implementation of the approved ICSS zones and Demilitarized zone (DMZ).

3.7.17 Network communications across two or more zones (Level 2 and above) shall pass through a Firewall for which rules are configured such that only required communications is possible, where source and destination hosts and protocols (identified by their TCP or UDP port numbers) are specified.

3.7.18 Traffic flow from Level 3 to Level 2 shall flow through a firewall.

3.7.19 Networks used to connect Level 1 and Level 2 functions shall use physically separate network switches and routers from Level 4 networks.

3.7.20 IP routing shall be implemented using equipment explicitly designed for this purpose, i.e., router and firewall devices.

3.7.21 Any connection using office domain networks shall be tunneled and the tunnel endpoints shall implement device authentication.

3.7.22 Safety-related communications (SIL 1 and above) that share a network (or bus) with a control network SHALL be separated from the control network by a network security barrier (i.e., gateway, firewall or network device with ACLs) that only permits traffic required for the safety and control systems to inter-operate.

3.8 Malware Control

3.8.1 The Contractor shall install anti-malware solution on all applicable IT components provided as part of the project scope.

3.8.2 Anti-malware solution provided shall be approved and certified for use by the Contractor.

3.8.3 Anti-malware solution provided shall have the capability for centralized administration and centralized deployment of agents & anti-virus signatures.

3.8.4 The Contractor shall verify system performance after installation of anti-malware solution on the ICSS environment.

3.8.5 Virus definition files shall be tested and released for installation by the ICSS Vendor as soon as possible, within a maximum of 30 days after initial release from the anti-malware vendor.

3.8.6 Solution shall be designed to support offline update of anti-virus signatures.

3.8.7 The Contractor shall provide documentation describing how approved virus definition files shall be communicated to ADNOC Onshore. The channel for download or provisioning of Anti-virus signatures shall be agreed between ADNOC Onshore and the Contractor.

3.8.8 The Contractor shall provide a documented procedure for installation, configuration, offline update and uninstallation of anti-malware solution.

3.8.9 ICSS vendor shall instruct its staff that any portable media (e.g. laptops and USB storage) used for commissioning and maintenance of equipment or devices shall only be used specifically for this purpose during the project. The removable media shall be scanned by anti-malware solution implemented in ADNOC Onshore with up to date anti-virus signature (independent to the ICSS Network) before being used in ADNOC Onshore ICSS environment.

3.8.10 Where the installation of antivirus software is not technically possible, a listing of all computers where antivirus software cannot be installed shall be maintained, and other mitigating factors shall be in recommended to reduce the risk of infection.

3.8.11 Where supported and certified by the ICSS vendor the Contractor shall implement a centrally managed application whitelisting solution. The Contractor shall demonstrate that the application white listing solution does not conflict with the functionality, safety or performance of the automation system or to any of its integrated systems.

3.9 Removable Media Control

3.9.1 The Contractor shall ensure that all unneeded removable media drives are disabled. The Contractor shall provide a written list of all USB ports, CD/DVD drives and other removable media devices with their status being disabled or enabled.

3.9.2 The Contractor shall provide a solution for centralized control for management of removable media within the ICSS environment.

3.10 Technical Vulnerability Assessment

3.10.1 The Contractor shall permit ADNOC Onshore to conduct security vulnerability scans on the ICSS components in scope of the project (which include but not limited to servers, laptops, PC's, workstations, applications, network switches, routers, databases etc.) during FAT and SAT and remediate the vulnerabilities identified.

3.10.2 The Contractor shall inform ADNOC Onshore in writing or provide white papers and best practice documents of any published flaws within its supplied applications, PLC's, controllers and IT components.

3.10.3 The Contractor shall disclose the existence of any known or identified backdoor in the supplied systems.

3.10.4 The Contractor shall inform ADNOC Onshore of any hard coded credentials within the ICSS systems and subsystems.

3.10.5 The Contractor shall prove that the supplied system is robust against system scans during normal operation without affecting system performance.

3.11 Firewall Management

3.11.1 The Contractor shall implement tested and compatible process control firewalls that would not cause degradation in the expected functionality, latency and system objectives and to meet the secure zoning requirements of 3.7.1 and 3.7.2.

Note 9: The ICSS vendor shall communicate with ADNOC Onshore on the list of process control firewalls compatible with their ICSS along with their specifications.

Vendor qualified solutions should not adversely affect the published performance specifications of ICSS.

3.11.2 All firewalls implemented shall be redundant in high availability mode without any single point of failure. In case of any deviations, the ICSS Vendor shall highlight the same to ADNOC Onshore.

3.11.3 Process control firewalls that understand control system protocols such as Modbus over IP, OPC, DNP3 etc. shall be implemented at the interface points between the ICSS and any integrated third party systems.

Note 10: Positioning of process control firewall, its configuration and deviations to the above requirements (if any) should be discussed with ADNOC Onshore before finalization.

3.11.4 The Contractor shall provide detailed information on all communications (including protocols) required through the firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding firewall rule.

3.11.5 DCOM related traffic used for PI system communication shall be restricted to a single defined port using compatible OPC enforcement solutions and software.

3.11.6 All rules applied to the firewalls not required during commissioning shall be removed prior to handover.

3.12 Audit Logging

3.12.1 The process control system components shall generate audit logs for user login success/ failure, operator / administrator activities, system events/ faults, configuration changes related to the Operating System (OS), ICSS applications, security and network devices.

3.12.2 Individual audit records should include the time stamp, source, category type, event id and event result.

3.12.3 ICSS should have the ability to send audit logs to an alternate storage system for analysis and retention. The control system should be compatible to send system logs to a syslog server for integration with a SIEM (Security Incident and Event Management solution).

3.12.4 The Contractor shall provide the method statement to push the logs from the ICSS system and network nodes to the Syslog server.

3.12.5 All activities and changes made by operator accounts and accounts with engineering privileges shall be logged at the application / system level.

3.13 Account Management and Access Control

3.13.1 The ICSS shall have the capability to create unique user id for users with engineering and operator privileges at application and system level.

3.13.2 The ICSS shall support implementation of strong password authentication for all engineering functions to make configuration changes on the controller.

3.13.3 The controller should accept configuration changes only from authorized engineering workstations and nodes.

3.13.4 The ICSS application shall have the capability to create group and individual user names for different roles, e.g., monitoring, operator, engineer, administrator etc.

3.13.5 The ICSS shall support that default passwords used for system accounts (such as an administrator or root account) can be changed by ADNOC Onshore.

3.13.6 The ICSS shall support that unused default accounts can be removed or disabled; e.g. Supplier “back-door”, “super-user” and “guest” accounts.

3.13.7 The administrator account shall not be used by default by the ICSS to run services (if any). A dedicated “service” account shall be created with the minimum privileges necessary for running the service.

3.13.8 Servers and workstations located in areas that are normally unattended shall require authentication and shall have the capable of enforcing an active automatic locking.

3.13.9 The ICSS shall provide the capability to set special accounts (service, auto-login and operator accounts) so that they never expire nor be disabled automatically.

3.13.10 ICSS vendor shall integrate the servers, desktops, laptops, printers and workstations in to a domain based environment using a dedicated redundant domain controller such as Active Directory to facilitate central enforcement of policies.

3.13.11 ICSS Application logins with engineering level privileges should be logged out after a defined period of inactivity.

3.13.12 Changes to operating condition from remote or advisory set points shall be logged on a system where operations can review them.

3.13.13 Windows administrator level privileges shall not be provided to operators.

3.13.14 All system passwords shall be provided to ADNOC Onshore in a sealed envelope after commissioning.

3.14 Password Management

3.14.1 The Contractor shall disable or remove all default ICSS vendor and guest accounts prior to the SAT.

3.14.2 Passwords shall not be transmitted in clear text.

3.14.3 Network devices shall have passwords encrypted within the device.

3.14.4 The channel for management access to network devices shall be through an encrypted channel such as SSH from designated hosts within the ICSS Network.

3.14.5 The ICSS should not allow applications to provide any auto-fill functionality during login, or allow anonymous logins.

3.14.6 For ICSS systems utilizing password based authentication, ICSS should provide the capability to enforce:
a) configurable password strength of at least 8 characters length and consisting of a combination of lowercase, uppercase, numeric digits and special character;

b) Password history of 3 passwords;

c) Password minimum and maximum lifetime restrictions for users.

3.14.7 The Contractor shall configure ADNOC Onshore password policy on ICSS unless there is a technical constraint in configuration.

3.15 Privilege Management

3.15.1 The ICSS vendor shall configure access privileges on the control systems and applications based on roles as recommended and documented by ADNOC Onshore to ensure that only the privileges required for the role is configured.

3.15.2 The ICSS vendor shall verify that a user cannot escalate privileges without logging into a higher-privileged role first.

3.16 Patch Management

3.16.1 The Contractor shall provide a solution for centralized deployment of Microsoft patches (Ex: WSUS). The solution shall have the capability to deploy Microsoft patches in an offline mode without connectivity to the internet. The patches shall be loaded from a removable media (CD, DVD, USB Hard Disk etc.) to the centralized patch management server and then deployed to all the ICSS end point nodes.

Note: Solution architecture needs to be developed with the understanding that the patch download and installation shall be performed in an offline mode.

3.16.2 The Contractor shall provide the patch management server with sufficient capacity and storage space as recommended by the system OEM.

3.16.3 The Contractor shall provide documentation on the offline patch deployment and roll back procedure.

3.16.4 The Contractor shall ensure that the operating system and applications are patched to current recommended status before commissioning.

3.16.5 The Contractor shall inform ADNOC Onshore about approved, not approved and not relevant security patches within 90 days after release by the manufacturer of the OS and software during the maintenance phase under the provision of the maintenance agreement. This shall also include a warning if the application of a patch requires or causes a re-start of the system, if not already documented in the patch release notes.

3.16.6 The ICSS vendor shall test all relevant security patches that are released by the manufacturer of the operating system and software provided by the vendor before informing ADNOC Onshore to install the patch.

3.16.7 The ICSS vendor shall establish a communication channel to inform ADNOC Onshore on the list of patches recommended for installation.

3.16.8 Groups shall be created such that the approved patches can be deployed on a set of designated nodes prior to deployment of patches to all nodes.

3.16.9 The Contractor shall provide a patch management solution as supported and certified, which can deploy patches of common software such as Oracle, Java, Adobe Flash, Adobe Reader etc. in addition to patch management of Microsoft related Operating System and products.

3.16.10 The Contractor shall supply and implement a software deployment solution for remote deployment of software and patches of third party software.

3.17 Monitoring and Capacity Management

3.17.1 The Contractor shall provide centralized monitoring tools to continuously monitor ICSS assets, manage configurations and detect availability, communication errors, capacity and performance of all servers, desktops, firewalls and network devices and shall support syslog, SNMP, syslog and WMI.

3.17.2 The proposed solution must have the following minimum capabilities:

- Ability to monitor wired and wireless networks, physical and virtual servers;
- Discover & map the network including desktops, workstations, servers, firewalls, switches and routers.
- Ability to visualize the complete network map;
- Monitor the availability and performance of routers, switches, and firewalls.
- Identify root causes of failure;
- Alert system and network failures;
- Provide capacity monitoring reports;
- Intuitive web based dashboards;
- supports scripting languages like VBScript and PowerShell and supports SQL queries to create database monitors;
- Assign device roles to the identified devices;

- Supports multiple monitors such as active monitors that proactively poll to monitor device states, performance monitors that capture actual performance metrics like CPU and memory utilization, and passive monitors that collect SNMP traps, Syslog info, and Windows event logs.

3.18 Wireless Security

3.18.1 Wireless instruments shall support authentication and cryptography for enhanced security mechanisms (at least 128 bits) to prevent unauthorized wireless access into the ICSS. For wireless connections, the highest feasible level of WPA, WPA2 or AES security / encryption shall be used.

3.18.2 Industrial wireless field devices shall be based on ISA 100 or WirelessHART (IEC 62591). Other techniques used shall be approved by ADNOC Onshore.

3.18.3 Wireless bridges providing point-to-point backbone connectivity shall support strong encryption (e.g., WPA, WPA2, AES-256 etc.). The highest possible encryption shall be provided by the vendor and shall be discussed and agreed with ADNOC Onshore.

Note 11: A wireless bridge is a hardware component used to connect two or more network segments, which are physically and logically (by protocol) separated.

3.18.4 Pre-shared encryption keys shall support at least 128 bit encryption.

3.18.5 The SSID shall only be broadcasted if services require its visibility.

3.18.6 Access Control Lists (ACLs) and authentication methods shall be implemented to secure the wireless network and access points.

3.18.7 Wireless devices connected to a TCP/IP port shall use static IP addresses.

3.18.8 The point of connection to a wired Ethernet network shall be firewalled with documented firewall rules from the wireless network.

3.18.9 Unused ports provided on wireless instruments shall be disabled.

3.18.10 The Contractor shall change manufacturers' default user names and passwords.

3.18.11 The Contractor shall provide architecture documentation describing how wireless systems will provide data exchange, authentication and connectivity between the wireless instruments and to other process control domain devices / systems.

3.19 Backup and Recovery

3.19.1 The Contractor shall provide a centralized backup and recovery system to conduct centralized automated backup of user-level and system-level information without affecting normal operations.

3.19.2 Three Tier Central Backup Topology shall be implemented:

- Each device individually utilizing a dedicated partition;
- The Central Backup Server with centralized reporting capabilities;
- Tape Library for offsite storage.

3.19.3 The backup solution should support the capability to verify the reliability of the backup mechanism.

3.19.4 The backup and recovery system shall provide the functionality to allow the system to be recovered and reconstituted to previously saved backup after a disruption or failure.

3.19.5 The Contractor shall provide a detailed procedure for taking backup and for restoration of ICS system components, which includes but is not limited to:

- Operating system files;
- Applications (including middleware);
- Configuration data;
- Database files;
- Network Configurations and system state backups;
- Log files;
- Active Directory;
- Field instrumentation and controller parameters;
- Unconventional file types; e.g. network equipment settings, Process Automation System (PAS) controller settings (tuning parameters, set points, alarm levels, etc.) and field instrumentation parameters;
- Other files, identified by the ICSS vendor, required to create a complete backup of the ICS system;
- System Image Backup.

3.19.6 For virtual machines the backup solution shall have the capability to:

- Take file-level and image-level virtual machine backups;
- Support replication and recovery of virtual machines to alternate locations;
- Support file level recovery for database VMs;
- Monitor Backup of virtual machines.
- The backup and restore system shall maintain an audit trail of all backup and restore activities.

3.19.7 The backup and recovery system shall function normally without significant changes of CPU load whilst a backup is in progress. It is recommended that the backup system can be adjusted for bandwidth usage and CPU load. The Contractor shall demonstrate as a minimum that its system functions normally during the back-up.

3.19.8 The CONTRACTOR shall provide minimum of 10 backup tapes in total for onsite and offsite backup storage.

3.19.9 Dedicated backup and recovery server shall be provided for each plant in scope.

3.19.10 Backup solution shall have the capability to take whole disk image and data backup along with bare metal remote restore capability.

3.19.11 The solution shall be integrated with Active Directory with role based access control.

3.19.12 The backup solution shall have centralized software to monitor the status of the backup and restoration activity and to make policy configurations centrally.

3.19.13 The backup solution shall support AES 128 / 256-bit encryption for backup images and files.

3.19.14 The solution shall support agents for Windows, Linux, applicable applications and database.

3.20 Documentation

3.20.1 Detailed Vendor Document register shall be submitted by the CONTRACTOR.

3.20.2 The Contractor shall submit the following minimum documentation as part of the project for ADNOC Onshore review and approval:

- Vendor Document register
- Bill of Material
- Functional Design Specification (FDS)
- Detailed Design Specification (DDS)
- FAT Procedure
- SAT Procedure
- Control Architecture Diagram based on ISA Zoning and Conduit model
- Cabinet Detailed Design Drawings
- System Interconnection Diagram
- Control Room Layout Diagram
- Specification and Datasheets
- Hardening Standard for Windows Desktop, Server, Firewall, Switch, Router and ICSS application.

3.20.3 System manuals must be provided by the CONTRACTOR in both hard and soft copy in English.

3.20.4 All training documents must be provided by the CONTRACTOR both hard and soft copy in English.

3.20.5 The Contractor shall provide documentation defining access and security permissions configured for user accounts at the operating system and application level.

3.20.6 The Contractor shall provide a listing of ports, and services required for any system running control system applications or required to interface with third party systems.

3.20.7 The Contractor in coordination with ADNOC Onshore (as applicable) shall document all external connections and third party system interfaces in their control architecture documentation.

3.20.8 The Contractor shall supply and maintain an inventory register of the ICSS components supplied by them.

3.20.9 The Contractor shall provide documentation related to installation, configuration, backup and restoration for all security technologies and software implemented as part of the scope of the project.

3.20.10 The Contractor shall update the existing ICSS control architecture diagram.

3.21 Monitoring Console

3.21.1 A dedicated console for monitoring of all the security technologies shall be supplied and implemented as part of the project scope in the engineering room.

3.21.2 The monitoring console shall be installed with the software required to enable ADNOC Onshore to troubleshoot, monitor and view diagnostics information of the security solutions that are implemented as part of the project.

3.22 Secure Coding and Design

3.22.1 The Contractor shall provide to ADNOC Onshore controllers and PLC's that are tested and certified for cyber security from reputed certification agencies such as Wurldtech Security Technologies' Achilles certification, ISA Security Compliance Institute (ISCI) or any equivalent certification agency which shall be reviewed and approved by ADNOC Onshore. The test certificates shall be provided to ADNOC Onshore.

3.22.2 The Contractor shall provide assurance that the source code of the control system is reviewed for security vulnerabilities and adequately certified during the SDLC cycle. The ICSS vendor shall provide secure code review and testing certificates where available.

3.22.3 The Contractor shall provide assurance for the following application level controls related to ICSS:

- Data input to the application systems are validated;
- Validation checks are incorporated into the system to detect any corruption of data while processing;
- Ensure authenticity and integrity in processing of messages/commands within the application;
- Data output from the application system shall be validated to ensure that the processing of stored information is correct;
- Error messages generated by the ICSS shall provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the system.

3.23 Incident Management

3.23.1 The Contractor shall provide a communication channel to ADNOC Onshore to report security incidents, problems and remediation requests to the ICSS manufacturer / vendor. This shall include contact details of any existing technical call center for reporting cyber security incidents.

3.24 Training

3.24.1 The ICSS vendor shall provide cyber security training for 10 ADNOC Onshore nominated staff. The training and knowledge transfer shall cover administration training for all the security technologies and software covered in the scope of the project.

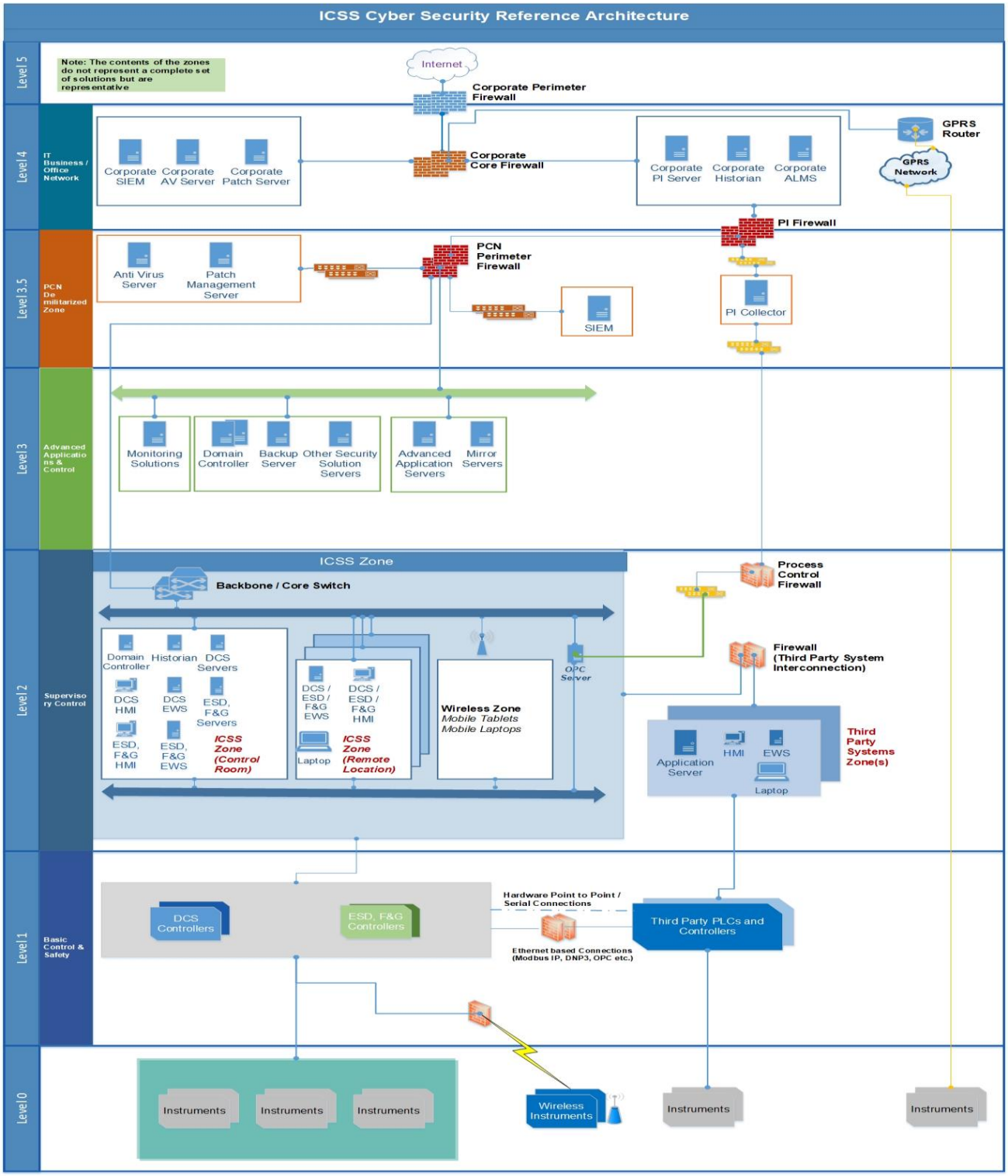
3.24.2 Training materials shall be provided and shall be customized for ADNOC Onshore and as applicable for the training focus group (Maintenance engineers, Telecom engineers, IT Security engineers etc.)

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي, الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

ENGINEERING SPECIFICATION
ICSS Security Specifications for Suppliers

APPENDIX A1: ICSS – General Reference Architecture



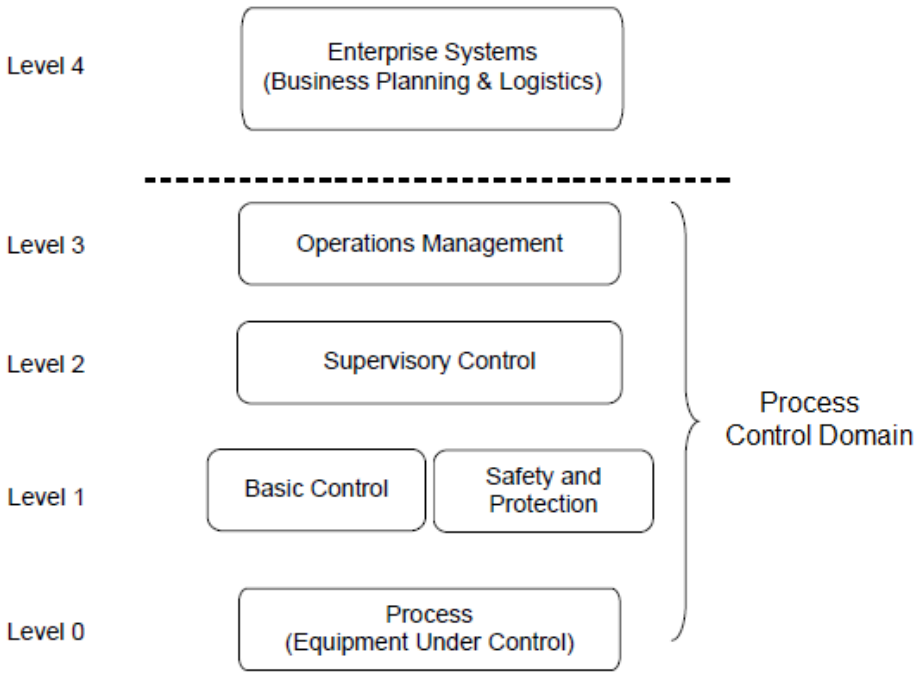
Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي, الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Note:

- The above diagram is representative typical architecture. All deviations and Contractor approved secure architecture shall be discussed with IT Security Compliance team prior to finalisation.
- Network Devices (Router, Switch or Firewall) interconnecting the different levels and zones must have access control list configured to restrict access between the zones.
- The firewalls tagged as Corporate and the PI Firewall will **not** be in the scope of supply of the Contractor unless specifically mentioned in the scope of work of the project.
- Positioning of the servers can vary based on the approved architecture design of the Automation Vendor.

APPENDIX A2: ICSS – Reference Model for ISA99 Standard



APPENDIX 4: DESIGN GUIDELINES – ALARM MANAGEMENT

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae
أدنوك البرية
ADNOC Onshore

أدنـوك
ADNOC

TECHNICAL CENTER & PROJECTS (TC&P)
TECHNICAL CENTER (Engineering)

Design Guidelines

Alarm Management

DOC. No. 30-99-39-0002

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

Document Control

Control Document Information:

Document Owner	Technical Center - Engineering
Document Author	Vinod Pal Singh, Senior Engineer Control
Document Custodian	In-house Engineering
Document Security Code	3 – Confidential
Document Number	30-99-39-0002

This is a controlled document and being maintained on electronic media. Any hard copies made are considered uncontrolled and may not be the latest version. Any employee of ADNOC Onshore, and its authorised 3rd Parties, are responsible for ensuring they are referring and using the latest version of the record and conform to the Copyright information.

	Name	Signature	Position	Date
Prepared By	Vinod Pal Singh		Senior Engineer Control	April 2019
	Sherif Abdelmoteleb		Senior Engineer Process Safety	April 2019
	Ahmed Al Zaabi		Specialist Reliability (IC)	April 2019
Reviewed By	Hani Bakr Osman		Chief Engineer (IC)	April 2019
	Sami Al Ankar		Manager Engineering Support	April 2019
Endorsed By	Khalil Abdel Aziz Mansour		A/ Manager In-House Engineering	April 2019
Approved By	Abbas Ahmed Yousef		VP- TC (I&OE)	April 2019
	Arif Al Rashedi		VP- TC (Eng.)	April 2019

Sr. No.	Rev. No.	Date	Description of revision
1	1	28-12-2017	Issued for Implementation
2	2	09-05-2018	Revised & Issued for Assets Feedback (Included TC-IOED comments)
3	3	April 2019	Revised & Reissued for Implementation (Incorporated/ addressed Asset (NEB, BUH),TC-IOED comments)

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Contents

General

The design guideline provides technical requirements for alarm management systems for use in ADNOC Onshore process facilities.

1.1 Introduction

This document has been developed with the following intentions:

a) To promote and ensure standardisation in the terms applied and in the approach used in describing alarm systems across ADNOC Onshore fields,

b) To describe alarm management lifecycle stages and briefly describe the stages requirements,

c) To provide guidance on alarms identification, rationalization (including prioritization) and detailed design,

d) To define key performance indicators (KPIs) and the respective target values for alarm systems,

e) To ensure that the alarm systems improve operator's situational awareness thereby contributing in improving safety, quality and efficiency of the processes,

f) To ensure that the latest developments, as outlined in the basic standards related to the alarm management are taken into consideration in describing/ specifying alarm systems,

This document only provides minimum guidelines for the alarm system lifecycle stages and supplements the requirements on the subject covered by the references mentioned in this document.

1.1.1 The Objective of this Guideline

The objective of this guideline is to provide guidelines for specifying (inclusive of performance matrices), engineering, designing, manufacturing, supplying, inspection & testing, installing, validating, operations, maintenance, monitoring & assessment, management of change, audit and management of the alarm systems in ADNOC Onshore facilities. This guideline is intended for use by the following:

a) ADNOC Onshore FEED/ EPC/ PC Project Engineers,

b) Contractors, Consultants & Alarm System Suppliers,

c) ADNOC Onshore Operation & Maintenance Engineers.

1.2 Scope

The alarm management guidelines covered in this document defines the philosophy for the alarm management and the general requirements to be followed for the Alarm systems in ADNOC Onshore new facilities.

These guidelines can also be applied to the Alarm systems in ADNOC Onshore existing facilities, however, the extent of application should be determined based on the considerations given in clause no. 3.3 of this document.

This document covers the minimum requirements for alarm management for use in ADNOC Onshore existing and new facilities. Specifically, this alarm management guidelines cover alarm system description, applicable terms and guidance on the specific stages of the alarm (system) management lifecycle inclusive of the stages, philosophy, identification, rationalisation (together with prioritisation), engineering/ design, implementation, operations, maintenance, monitoring & assessment, management of change and audit. Alarm system KPIs are also covered.

The alarm systems are considered part of the facility basic process control system (BPCS) using programmable electronics based systems with workstation(s). BPCS in a given facility includes all the systems in the given facility, which allows facility processes/ equipment to operate in the desired manner and therefore include system like DCS, SCADA, etc.

1.3 Exclusion

The scope of this guideline excludes the topics identified as exclusions in ANSI/ ISA 18.2-2016: Management of Alarms Systems for the Process Industries. Further, the scope of application of this guideline is elaborated in clauses 3.2 and 3.3 of this document.

1.4 Definitions and Glossary

For the purpose of this guidelines document, the following definitions shall apply:

COMPANY	ADNOC Onshore
CONTRACTOR	The party that carries out all or part of the design, Engineering, Procurement, Construction, Commissioning and Management of a project.
Manufacturer	The owner of the brand name of the equipment / who manufactures the equipment.
SUPPLIER/ VENDOR	Any and all persons, firms, partnerships, companies, bodies, entities or a combination thereof including Sub-Suppliers, who are providing Equipment, Material or Services to perform duties specified by COMPANY / CONTRACTOR with provisions of prior ADNOC Onshore approval and limited to ADNOC Onshore approved vendor list.
May / Can	Used where alternatives/actions are equally acceptable.
Should	Used where provision is preferred.
Shall / Must	Used where a provision is mandatory/vital.

Further, definitions and glossary applicable to this guideline are given in Appendix-A.

1.5 Abbreviations

For the purpose of this document, following abbreviations apply:

A&E	Alarms & Events
AIL	Asset Integrity Level
ALARP	As Low As Reasonably Practicable
AMLC	Alarm management lifecycle
ANSI	American National Standards Institute
API	American Petroleum Institute
ASM	Abnormal Situation Management (Consortium)
ASRS	Alarm system requirements specification
BPCS	Basic process control system
CDS	Central Degassing Station
COP	Code of Practice
CPP	Central Processing Plant
CRR	Contract Research Report
DCS	Distributed Control System
DA	Data Access
DEP	Design and Engineering Practice
EEMUA	Electrical Equipment and Materials Users Association
EIL	Environment Integrity Level
EPC	Engineering Procurement Construction
ESD	Emergency Shutdown
FEED	Front End Engineering Design
FF	Foundation Fieldbus
F&G	Fire & Gas
HAZID	Hazard Identification
HAZOP	Hazard and operability study
HMA	Highly managed alarms
HMI	Human machine interface
HSE	Health Safety Environment
HSE-UK	Health and Safety Executive of United Kingdom
I/O	Input / output
ICSS	Integrated Control & Safety System
IEC	International Electro-technical Commission
IM	Integrity Management
IOM	Installation Operation Maintenance
IPF	Instrumented Protective Function
ISA	International Society of Automation
KPI	Key Performance Indicator
LOPA	Layer of protection analysis

MADB	Master Alarm Data-base
MAH	Major Accident Hazards
MOC	Management of change
OEM	Original Equipment Manufacturer
OWS	Operator Workstation
OPC	Objection Linking & Embedding for Process Control
P&ID	Piping and instrumentation diagram
PC	Procurement Construction
PHA	Process hazards analysis
PV	Process Variable/ Value
QRA	Quantitative Risk Analysis
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition (System)
SCE	Safety Critical Equipment
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
TR	Technical Report

1.6 References, Codes and Standards

The following documents are indispensable for the application this engineering specification. For dated references, typically the edition cited apply, however, the updated/ latest edition shall also be taken into consideration for application. For undated references, the latest edition of the referenced document (including any amendments) applies:

ADNOC Standards/ Procedures	
ADNOC Corporate Risk Matrix- Version1 June 2018	
ADNOC-COP IM 1.4	ADNOC Code of Practice & Guidance on Operating Integrity
ADNOC Onshore Standards/ Procedures	
	Manage MoC Business Process (Management of Change)
International/ National/ Industry Standards/ Reports	
ANSI/ISA-18.2-2016	Management of Alarms System for the Process Industries
API RP 554 (Part 1, 2, 3)	Process Control Systems
ASM Consortium Guidelines, 2nd Edition, 2015	Effective Console Operator HMI Design.
EEMUA-191, 3rd Edition, 2013	Alarm Systems.

HSE-UK, CRR-166/1998	The Management of Alarm Systems
IEC-61511-2016(All Parts), 2nd edition	Functional Safety- Safety Instrumented Systems for the Process Industry Sector.
IEC 62682	Management of alarm systems for the process industries
ISA-TR18.2.2-2016	Alarm Identification and Rationalization
ISA-TR18.2.3-2015	Basic Alarm Design
SHELL DEP 30.00.60.16, February 2017	Human Factors Engineering- Human Machine Interface Design for Situation Awareness
SHELL DEP 32.80.10.14, February 2017	Alarm Management
SHELL DEP 62.10.08.11	"Inspection and Functional Testing of Instruments"
	The High Performance HMI Handbook, first edition, 2008. By Hollifield, Oliver, Nimmo, Habibi. Published- PAS, USA.

1.7 Roles & Responsibilities

The roles and responsibilities associated with the application of alarm management are dependent of given alarm management lifecycle. Refer clause 3.2 of this document for the roles & responsibilities related to each stage in alarm management lifecycle.

Alarm Systems Purpose & Description

1.8 ADNOC Code Of Practice

Alarm management is the integral part of operations integrity management of the facility. The ADNOC Code of Practice, i.e., ADNOC COP IM 1.4, on operations integrity management covers alarm management requirements which shall be complied in the applicable stages of alarm management lifecycle as described in this document. Following are the excerpts on alarm management from ADNOC COP IM 1.4:

Quote:

"11.6 Alarm Management
ADNOC Group Companies shall ensure that process alarms are enunciated in the Control Room as required to warn the Control Room Operator of an excursion beyond an operating envelope, in order for the operator to initiate appropriate proactive action.

All process alarms shall be documented, reviewed, prioritized and rationalized in order to prevent Alarm Flood, such that the operator is able to respond to an alarm in the prescribed way without being overwhelmed.

Guideline:

Alarm management is concerned with classifying, prioritizing and rationalizing process alarms. It involves the application of a consistent methodology to eliminate alarms which are deemed unnecessary and prioritize those that remain, such that the correct action can be taken, and the number of alarms is manageable.

A master alarm database should exist as a controlled document, accessible in the Control Room, covering all assets, plant and equipment that require be monitoring and controlling from the Control Room. The alarm master database should contain as a minimum:

- The process value range (operating set point)
- The alarm set point
- The priority of the alarm
- The reason for the alarm limit
- The consequence of exceeding the limit
- The estimated time for the consequence to be realized
- The required actions to be taken, including any required escalations.

The master alarm database should be kept up-to-date and accessible for Control Room Operators. Changes to the master alarm database should be managed through a defined MOC process. The alarm set points should be periodically verified against the design limits and trip set points.

There should be an alarm management process in place which reviews alarm rate, standing alarms, and disabled alarms and analyzes and resolves any issues impeding the ability of the control room operator to act on an alarm in the prescribed way.

There should be a defined target for the average alarm rate per console operator per hour in steady state conditions. There should be an alarm and event analysis capability to allow measurement and trending of alarm rates and the review of repeat alarms, standing alarms, bad actor alarms and nuisance alarms.

Industry best practice for average alarm rate in steady state is < 6 alarms per operator console per hour. An initial minimum standard upon which to build improvement is <12 alarms per operator console per hour. Anything more than this should be addressed by an improvement process.

Operators should complete training on how to respond to alarms, and such training should be recorded in a competency assurance record.

Roles and responsibilities for managing alarms should be defined and documented."

Unquote:

This alarm management guidelines document address the requirements of the ADNOC COP IM 1.4 related to alarm management.
As the starting point, the ADNOC COP IM 1.4 suggested KPI of <12 alarms per operator console per hour, is considered in this document.

1.9 Alarm System Principal Purpose

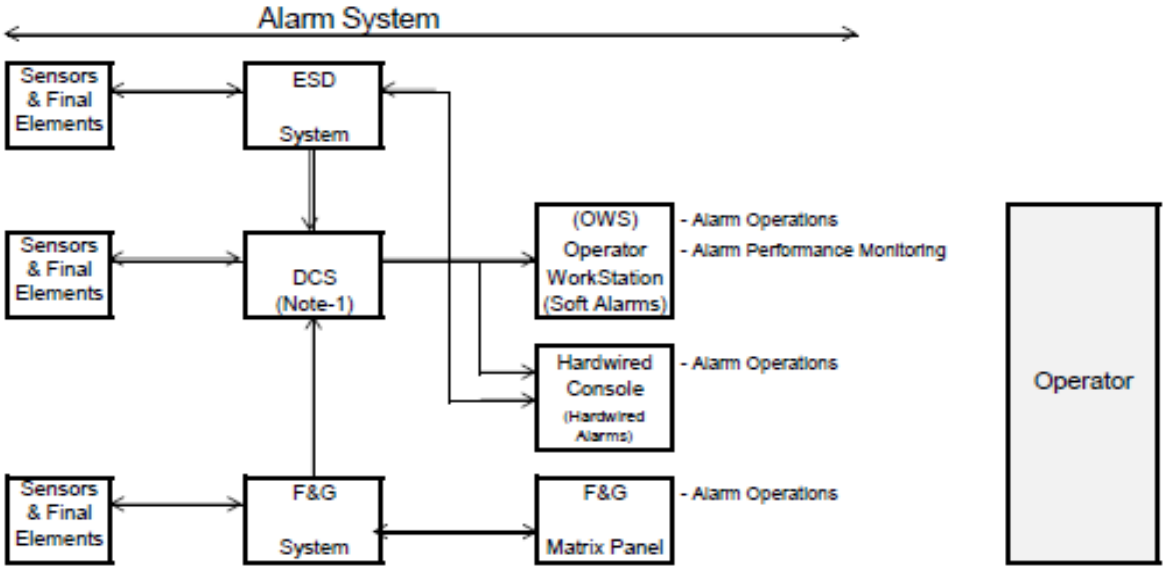
The main purpose of the alarm system is to notify the operators of abnormal process conditions or equipment malfunctions and support the corresponding operator response.

1.10 Alarm Systems in ADNOC Onshore facilities

ADNOC Onshore facilities are spread over geographically segregated fields. Each field is essentially operated/ maintained quasi-independently from the other fields by its dedicated team. Each field has the centralised location, i.e., main/ central control room at central degassing station (CDS) or central processing plant (CPP), from where the entire given field facilities are primarily monitored/ controlled by the operations team continuously.

In general, ADNOC Onshore facilities are monitored/ controlled by the Operations team through programmable electronics based basic process control systems (BPCS), like distributed control systems (DCS). The alarms functions are handled by the operators through DCS Operator Workstations (OWS). Further, Hardwired alarm annunciators on auxiliary consoles located beside the DCS OWS are generally provided for few critical/ main parameters for the given facility.

Typically, ADNOC Onshore facility DCS is interfaced with the respective safety systems, i.e., ESD System and F&G System, utilizing Ethernet/ Serial/ etc interfaces forming an integrated system referred to as integrated control & safety system (ICSS). In addition, the facility DCS may also interface with the facility process/ equipment packages control system (wherever provided) to allow monitoring/ control of the packages from the DCS.
Further, in some of the ADNOC ONSHORE fields, sometimes parallel systems are provided, like SCADA, in addition to the DCS, to allow monitoring/ control of the part process facilities.
Given below figure is the generic outline of the alarm systems used in ADNOC Onshore facilities.



NOTES-
1. Above figure is not for the purpose of identifying all the interfaces required between the systems.
2. Above figure is only for the purpose of identifying interfaces among systems from alarming view point.
3. Packages Control Systems and their interfaces with DCS are applicable however these are not shown for simplicity.
4. In some of the ADNOC Onshore fields SCADA system is also provided for monitoring/ control of part facilities.

Figure-1: Typical Alarm System in ADNOC Onshore Process Facilities

(Above figure is the simplified version of ANSI/ISA 18.2-2016, Figure-1 and is modified to describe alarm systems in ADNOC Onshore facilities)

The Alarm system design/ implementation in the ADNOC Onshore new facilities shall generally follow the outline given in this section, however, requirements of all the relevant sections of this document shall be applied.

Alarm System Basic Requirements

The alarm systems shall be designed/ engineered/ implemented and further managed meeting the requirements of these guidelines together with the requirements stated in the documents mentioned in the “References” section.

1.11 Alarm System Basic Functional Requirements

Alarm systems shall implement the following basic functional requirements:

a) To enhance operational effectiveness by implementing the following:

i. Detects alarm state in the facility representing equipment malfunction, process deviation, or abnormal condition requiring a timely operator response,

ii. Communicates, using audible and/or visible means, the indication of the alarm state to the operator, and records changes in the alarm state,

iii. Allow enforcement of the master alarm database,

iv. Generates alarms reporting, logs and implement alarm historian function,

v. Provide functionality to the operator to implement alarm suppression techniques, to handle nuisance alarms, out-of-service alarms, state-based alarms with appropriate access control methods

vi. Provide functionality to the operator to implement advanced/ enhanced alarm techniques (if required),

b) To realize alarm system performance monitoring and assessment: by collecting the alarms & events data, summarizing the data and deriving the figures for the KPIs identified in this guideline document. The system shall compare the calculated KPIs figures with the corresponding target values defined in this guideline and broadcasting the results on the HMI graphic dashboard format in real-time.

1.12 Alarm Management Lifecycle

The framework for managing the alarm system is managing and executing the Alarm Management Lifecycle stages logically. Alarm management lifecycle defines all the stages, from initial conception stage, i.e., defining philosophy, to operations & maintenance stage inclusive of decommissioning of the alarm system.

The alarm management lifecycle shall follow the requirements of ANSI/ ISA 18.2-2016 Section 5.2, SHELL DEP 32.80.10.14 Feb 2017 Section 2. The figure given below, which is based on above mentioned standards, shall be followed for ADNOC Onshore facilities alarm systems.

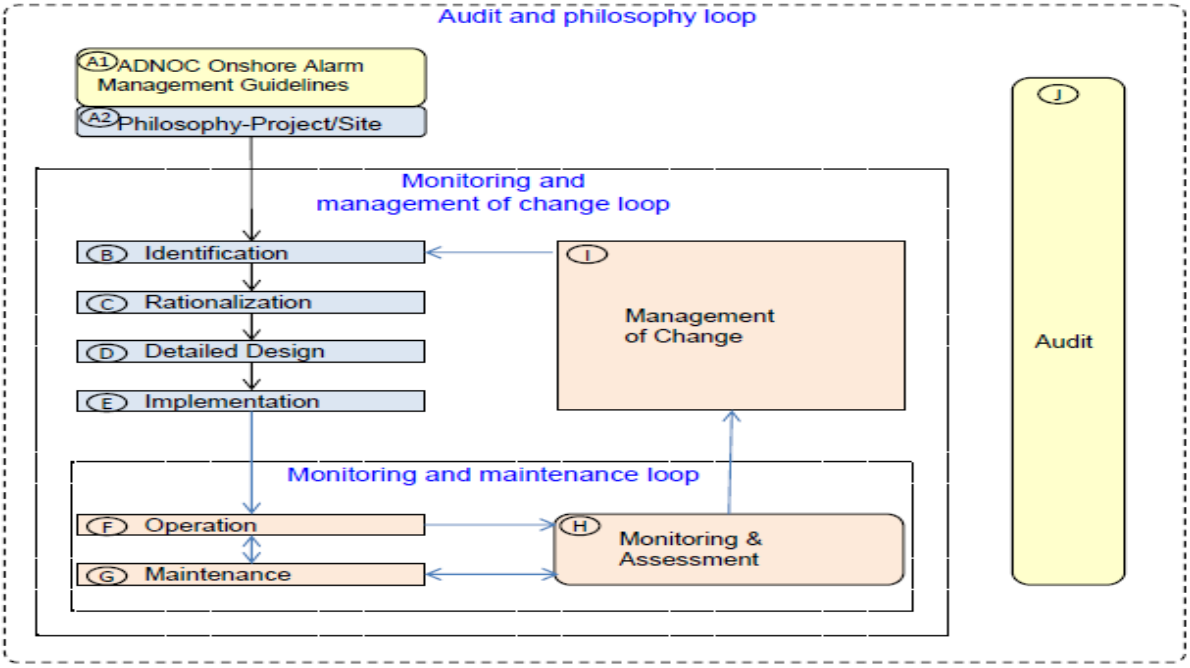


Figure-2: Alarm Management Lifecycle

(Above figure is based on SHELL DEP 32.80.10.14., February-2017, Figure 2.1 and ANSI/ ISA-18.2-2016, Figure 2.)

This section also captures the AMLC table based on ANSI/ ISA-18.2-2016, Table-1 with modifications to reflect the requirements of ADNOC Onshore. The table captures all the AMLC stages together with respective stage requirements detailing the activities involved, inputs required, outputs generated, and the responsible entities for the given stage.

Table-1: Alarm Management Lifecycle Stages requirements
(Below table is based on ANSI/ ISA-18.2-2016, Table-1)

Alarm management lifecycle stage		Alarm management lifecycle stage requirements			
Stage	Stage Title	Stage Activities	Stage Input Requirements	Stage Outputs	Responsibility
A1	ADNOC Onshore Alarm Management Guidelines (Note-a)	Develop Alarm Management Guidelines- Purpose, Terms, Key Requirements including KPIs	Objectives, Standards, Audit recommendations (if any)	Alarm Management Guidelines	ADNOC Onshore-TC-Engineering
A2	Philosophy-Project/Site (Note-b)	Develop Project/ Site specific philosophy (Supplementing ADNOC ONSHORE Alarm Management Guidelines)	Objectives (Specific), Site Alarm Management Operational Procedures	Project/ Site Alarm Management Philosophy	FEED Consultant/ Contractor and ADNOC Onshore Project Engineering Team (feedback from Site Operations Team shall be taken)
B	Identification (Notes-c, d)	Identify Potential Alarms	Alarm Management Guidelines, Project Alarm Management Philosophy, P&IDs & PHA reports, Standards, Operating Procedures	Potential Alarms List	FEED Consultant (Note-c) / Contractor and ADNOC Onshore Project Engineering Team
C	Rationalization (Note-d)	Alarms Rationalization, Prioritization	Alarm Management Guidelines,	Master Alarm Database (MADB)	Contractor and ADNOC Onshore Project

Alarm management lifecycle stage		Alarm management lifecycle stage requirements			
Stage	Stage Title	Stage Activities	Stage Input Requirements	Stage Outputs	Responsibility
		Classification,	Project Alarm Management Philosophy, P&IDs & PHA reports, Standards, Operating Procedures		Engineering Team, Qualified Facilitator, ADNOC ONSHORE Site Operations Team
D	Detailed Design (Note-d)	Develop ASRS covering functional requirements and HMI requirements	Alarm Management Guidelines, Project Alarm Management Philosophy, MADB	ASRS	Contractor/ Alarm System Vendor and ADNOC Onshore Project Engineering Team
E	Implementation (Note-d)	Install, test alarm systems and training	Alarm Management Guidelines, Project Alarm Management Philosophy, ASRS, MADB	Alarm System with Operational Alarms, IOM Manuals	Contractor/ Alarm System Vendor and ADNOC Onshore Project Engineering Team, ADNOC Onshore Site Operation/ Maintenance Team (Note f)
F	Operation (Note-e)	Operator responds to alarms	Alarm Management Guidelines, Project Alarm Management Philosophy, MADB, IOM Manuals	Alarms data	ADNOC Onshore Site Operations Team
G	Maintenance (Note-e)	Periodic Testing, Out-of-Service, Equipment repair/ replacement	Alarm Management Guidelines, Project Alarm Management Philosophy,	Alarm records, Alarm System Maintenance Logs	ADNOC Onshore Maintenance/ Operations Team

Alarm management lifecycle stage		Alarm management lifecycle stage requirements			
Stage	Stage Title	Stage Activities	Stage Input Requirements	Stage Outputs	Responsibility
			MADB, IOM Manuals, Diagnostics Alarms	(including Lessons Learned)	
H	Monitoring & Assessment (Note-e)	Monitoring alarm data and report performance	Alarm Management Guidelines, Project Alarm Management Philosophy, Alarm records, Alarm System Maintenance Logs (including Lessons Learned)	Alarm Assessment Reports (Note g)	ADNOC Onshore Operations Team
I	Management of Change (Note-e)	Process to authorize changes in the alarm systems	Audit/ Survey Report, Gap Analysis Report, Management of Change Procedure	MOC Implementation Records/ Reports	As per ADNOC Onshore MOC Procedure
J	Audit (Note-e)	Audit of alarm management processes	Alarm Management Guidelines, Project Alarm Management Philosophy, Standards	Audit Reports, Gap Analysis Reports, (with Recommendations)	ADNOC Onshore

Following notes shall be applied to the above table: Table-1:

a) Stage responsibility is with ADNOC Onshore, TC-Engineering.

b) Project/ Site specific Alarm Management Philosophy is recommended to be developed during FEED by the Consultant. This stage shall primarily capture the project/ site specific requirements pertaining to the Alarm System/ Management. As a norm FEED documents shall be revisited during EPC/ PC stage of the project.

c) “Potential Alarms List” is not required to the developed as a separate document during FEED stage. Alarms should however be reflected in the FEED deliverables like P&ID, Specifications, etc. Alarms should also be reflected in the system I/O list. During EPC/ PC stage “Potential Alarms List” shall be developed by the Contractor. As a norm FEED documents shall be revisited and modified during EPC/ PC stage of the project.

d) Stage(s) primary responsibility is with Consultant/ EPC Contractor/ PC Contractor.

e) Stage(s) primary responsibility is with ADNOC Onshore.

f) Formal handover of the Alarm Systems to ADNOC Onshore Operations team shall only be undertaken after successful execution of works in "AMLC Stage-E: Implementation". Primary deliverables that are required to be provided to ADNOC Onshore Operations during handover included updated MADB, ASRS, IOM Manuals. Refer clause no. 8 for more details.

g) Alarm Assessment Reports should include the following: Tabulation of Alarm System Target KPIs Vs Achieved Performance (averaged over 30 days period), Alarm Lists (depicting specific instances of nuisance, shelving/ suppression, etc if required), Alarm & Trip Set Point List, Maintenance Logs & Lessons Learnt, Graphic Print-out, P&IDs, etc. Requirements of ISA TR 18.2.5-2012 Section 5.11- Report design, should be used as guidance for generating alarm assessment reports.

1.13 Conformance to the Guidelines

The extent of application of these guidelines shall depend on the applicable alarm management lifecycle stage for the given alarm system in a project/ facility. Following considerations shall be complied with based on the given project/ facility stage:

a) New Projects with new BPCS/ Alarm System

For the new projects involving completely new BPCS inclusive of the Alarm System these guidelines shall be applied right from the starting point of the alarm management lifecycle, i.e., Philosophy- Project/Site, and shall be applied thereafter to all the subsequent stages of the alarm (system) management lifecycle covered in this document.
It shall ensure that all the applicable requirements of these guidelines document are complied with.

b) New Projects with modifications to the existing BPCS/ Alarm System

For the new projects involving modifications/ expansion/ addition to the old BPCS (inclusive of alarm systems) these guidelines shall be applied right from the starting point of the alarm management lifecycle, Philosophy- Project/Site, and should be applied thereafter to all the subsequent stages of the alarm (system) management lifecycle with due considerations noted in the below paragraphs.
The extent of application of this guideline shall be assessed by the Consultant/ Contractor involving ADNOC Project Engineering/ Operations & Maintenance Team to ensure that the modified system is as close as possible to these guidelines in terms of conformance taking into consideration the following:

i. Consideration shall be given to impact on the production operations due to the modifications/ expansions/ additions scope on existing alarm system.

ii. The requirements of alarm management lifecycle stages: Philosophy, Identification, Rationalization shall be fully implemented.

iii. The extent of conformance to the requirements of the alarm management lifecycle stage, Detailed Design, shall be assessed for the existing BPCS. It is not advisable to have BPCS systems in the same Control Room with differing alarm philosophies/ specifications.

iv. The existing alarm system shall be subjected to survey. OEMs may be involved to identify the gaps. Once gaps are identified that ADNOC Field Operations Team/ TC- Engineering shall decide to cascade the matter through Management of Change route.

v. The requirements of alarm management lifecycle, Implementation, shall be fully applied.

vi. The requirements of alarm management lifecycle stage Monitoring & Assessment shall be applied as allowed by the already installed BPCS/Alarm system.

c) Existing BPCS/ Alarm System

In order for the alarm systems to be effective it is desirable that the target KPIs requirements are met. Alarm systems target KPIs are covered later in this document. The trigger for the application of this guidelines document should be from Asset/ field operations & maintenance team and/ or Integrity & Operations team when it is prima-facie concluded with the requisite records (e.g., daily alarm logs) that there are significant gaps of the installed alarm system performance with respect to the target KPIs. It is however recommended that the Asset/ field organise existing alarms systems audit to identify gaps with respect to this guidelines document. OEMs may be involved for identifying gaps.

Once the alarms system audit findings are available then the extent of application of this guideline shall be assessed by the ADNOC Onshore Operations & Maintenance/ TC-Engineering Team to ensure that the modified system is as close as possible to these guidelines in terms of conformance taking into consideration the following:

i. Consideration shall be given to impact on the production operations due to the modifications/ expansions/ additions scope on existing alarm system.

ii. The requirements of alarm management lifecycle stages: Philosophy, Identification, Rationalization shall be implemented as described below.

iii. Philosophy- Site/ project specific alarm management philosophy is recommended to be prepared taking into consideration this guideline document and design/ limitations of existing alarm systems. The goal should be to as close as possible to this guideline document and render the modified alarm system to facilitate performance monitoring with due considerations to incremental improvement to meet target KPIs.

iv. Identification/ Rationalization: The goal of alarms identification/ rationalization shall be to develop MADB to capture all the required alarms with necessary information for ensuring safe operation & maintenance.

v. The extent of conformance to the requirements of the alarm management lifecycle stage, Detail Engineering, shall be assessed for the existing BPCS.

vi. The existing alarm system shall be subjected to survey. OEMs may be involved to identify the gaps. Once gaps are identified that ADNOC Field Operations Team/ TC- Engineering shall decide to cascade the matter through Management of Change route.

vii. The requirements of alarm management lifecycle, Implementation, shall be fully applied.

viii. The requirements of alarm management lifecycle stage Monitoring & Assessment shall be applied as allowed by the already installed BPCS/Alarm system.

Alarm Identification (AMLC Stage-B)

Alarm identification stage of alarm management lifecycle involves generating the initial list of potential alarms in a given project which shall be made based on the following projects associated documents:

a) P&IDs

b) PHA reports inclusive of HAZOP, HAZID, SIL Assessment, etc reports

c) Project applicable Standards/ References requirements,

d) Specific facility/ site requirements/ practice,

e) Facility/ Site investigation/ study reports,

The initial list of potential alarms should contain the following information for each potential alarm which is required for the next stage of the alarm management lifecycle, i.e., alarm rationalization:

a) Consequence threshold

b) Operator response

c) Consequence of inaction

d) Probable cause

e) Basis for the consequence threshold

For the existing alarm systems associated works refer to the requirements in clause no. 3.3.

Alarm Rationalisation (AMLC Stage-C)

The purpose of alarm rationalization stage of alarm management lifecycle is to justify, prioritize and classify the alarms from the list of potential alarms generated during the Alarm Identification stage.

For the existing alarm systems associated works refer to the requirements in clause no. 3.3.

1.14 Alarm System Priority Levels

Existing Alarm Systems

Site/ project specific alarm management philosophy is recommended to be prepared taking into consideration this guideline document and design/ limitations of existing alarm systems. The goal should be to as close as possible to this guideline document and render the modified alarm system to facilitate performance monitoring with due considerations to incremental improvement to meet target KPIs.

New Alarm Systems

Alarm systems shall be designed to have the levels of priority in-line with the requirements given in “Method 4- General Alarm Assessment” in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013 and the same are tabulated below:

Table-2: Alarm System Priority Levels

(Alarm Priorities designation in below table are based on the flowchart given in EEMUA-191, 3rd Edition, 2013, Appendix-3: Prioritisation methods, Section A3.5.3 Method 4- General Alarm Assessment.)

Criticality	Criticality-Least ----------> Criticality-Highest		
Priority Level	3	2	1
Priority Designation	Low	High	Critical

Effectively, there are three levels of priority for the alarms, i.e., Priority 1 designated as “Critical”, Priority 2 designated as “High” and Priority 3 designated as “Low”.

Alarm System Priority Levels Definitions

Given below definitions of the alarms priority levels are based on EEMUA-191, 3rd Edition, 2013.

a) Low Priority Alarm: A low priority alarm notification is usually associated with the condition involving low level consequence severity.

b) High Priority Alarm: A high priority alarm notification is usually associated with the condition involving consequence severity level of 2 or 3 as defined in ADNOC Corporate Risk Matrix Version 1 June 2018.

c) Critical Priority Alarm: A critical priority alarm notification is usually associated with the condition involving consequence severity levels of 4, 5 or 6 as defined in ADNOC Corporate Risk Matrix Version 1 June 2018, Appendix-2 & 3.

EEMUA-191, 3rd Edition, 2013 also define another class of notification referred to as Alerts. An alert is a notification used for indicating equipment/ process condition to the operator, but, do not qualify to meet the criteria of an alarm. An alert associated operation action is not time-critical. Therefore, an alert is a notification that is used to attract the attention of the operator to changes that may require assessment or action when time allows.

1.15 Alarm Prioritization- Specific Requirements

Alarm justification/ prioritization shall be carried out for each alarm based on the requirements given in SHELL DEP 32.80.10.14, February 2017 and EEMUA-191, 3rd Edition, 2013.

The above mentioned SHELL DEP identify various alarm types to be considered in the alarm systems. For few of the alarm categories, the above mentioned SHELL DEP already assigns the priority level and thus indirectly justifying the given alarm. For few other alarm categories, besides identification and narration on the requirement, the assignment of the priority is recommended to be carried out through the use of Alarm Prioritisation Flowchart (referred in SHELL DEP as Notification Analysis Flowchart). Refer to Appendix-B which describes Alarm Prioritisation Flowchart to be used for ADNOC Onshore projects.
Given below table is the synopsis of the requirements given in SHELL DEP 32.80.10.14, February 2017.

Table-3: Alarm Justification/Prioritization- Specific Requirements
(Below table is based on SHELL DEP 32.80.10.14, February-2017, clause 5.1)

S.No.	Alarm/ Alarm Description	Alarm priority assignment as per SHELL DEP 32.80.10.14-2017 (Specification)/ (Informative)		Remarks
		Clause Ref.	Recommended Priority	
Process Alarms				
1.	Process Alarms (generally implemented in BPCS) *Note- As per SHELL DEP* 32.80.10.14-2017 (Specification) clause 5.2, *"alarms and alarm parameters needed for FF devices shall be designed and configured in BPCS, note in the FF device itself.*	5.1, 5.2 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
SIF Pre-Alarms				
2.	SIF pre-alarms (generally, SIF pre-alarms are avoided in the design and instead "Process Alarms" are implemented in BPCS. SIF pre-alarms implementation should be based on exceptions as noted in SHELL DEP 32.80.10.14-2017 (Specification), cl. 5.3.Approval of	5.3 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart

S.No.	Alarm/ Alarm Description	Alarm priority assignment as per SHELL DEP 32.80.10.14-2017 (Specification)/ (Informative)		Remarks
		Clause Ref.	Recommended Priority	
	the Company shall be taken).			
SIF Alarms/ Notifications				
3.	SIF trip status	5.4.1, 1 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
4.	SIF trip failure alarms	5.4.1, 1 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
5.	First-Out Indicator alarm	5.4.1, 1 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
6.	SIF mismatch alarms- actual final element status differs from commanded status	5.4.1, 3 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
7.	Device Fault/ Failure signals of non-voted (1oo1) SIF Transmitters/ Sensors	5.4.1, 4 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
8.	Voted Trip Signals- Single notification for only voted trip signal	5.4.2, 1 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
9.	Voted Trip Signals- Deviation Diagnostic Signal	5.4.2, 2 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
10.	SIF final elements- trip status signals	5.4 (Informative)	Alert	
F&G Alarms/ Notifications				
11.	Unconfirmed Gas or Fire Alarm	5.5, 3 (Specification)	Critical	
12.	Confirmed Gas or Fire Alarm	5.5, 3 (Specification)	Critical	
13.	Detector Diagnostic Alarm	5.5, 4 (Specification)	High	
Diagnostics Alarms/ Notifications				
14.	Bad PV Signals with at least one Standard Limit	5.6 (Informative)	High	
15.	Bad PV Signals with at least one Critical Limit	5.6 (Informative)	Critical	
16.	System Diagnostics Alarms	5.6 (Informative)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
Operator Switches & Controls				

S.No.	Alarm/ Alarm Description	Alarm priority assignment as per SHELL DEP 32.80.10.14-2017 (Specification)/ (Informative)		Remarks
		Clause Ref.	Recommended Priority	
17.	Control Room located Switches associated notifications	5.7, 1 (Specification)	Alert	
18.	Outside Control Room located Emergency Trip Switches	5.7, 2 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
19.	Initiation of Maintenance Override Switch or Bypass Switch for SIF sensor located outside Control Room	5.7, 3 (Specification)	*(Refer remarks)*	Apply Appendix-II, Alarm Prioritisation Flowchart
Intermittently Operated and Spared Equipment Notifications				
20.	Start/ Stop Signals- intermittently operated units	5.10, 1 (Specification)	Alert	
Common Notifications Facility Notifications *Generic requirements given.*				

SHELL DEP 32.80.10.14, February-2017 uses alarm priority designations: “Critical”, “Standard” whereas this document describes the alarm priority designations: “Critical”, “High”, “Low”. The alarm priority designations “Critical”, “Standard” used in SHELL DEP 32.80.10.14, February-2017 are described respectively as “Critical”, “High” alarm priority designations in this document.

1.16 Alarm Prioritization Flowchart

The potential alarms cases for which there are no specific requirements of priority assignments are given in SHELL DEP 32.80.10.14, Feb 2017 then such cases shall be subjected to assessment as per the Alarm Prioritisation Flowchart described in Appendix-II of this document.

The Alarm Prioritisation Flowchart given in Appendix-B is based on “Method 4- General Alarm Assessment” in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013. Further, Appendix-B also captures the equivalence/ mapping of the consequence categories described in ADNOC Corporate Risk Matrix Version 1 June 2018 with the categories used in “Method 4- General Alarm Assessment” in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013.

Appendix-C captures the relevant extracts from ADNOC Corporate Risk Matrix Version 1 June 2018 that describe ADNOC Potential Risk Matrix and the consequence categories used therein.

1.17 Alarm Set-Point Determination Considerations

The alarms set-point determination is carried out by process engineering discipline of the project engineering consultant. Given below considerations, based on ANSI/ISA 18.2-2016, section 9.4 should be considered in determining the set-points:

a) The allowable response time

b) The complexity of the operator action

c) The time necessary to complete the operator action

d) The normal operating range

e) Other operating or design boundaries

f) Knowledge of the process operation and history

1.18 Highly Managed Alarms

Highly Managed Alarms are the class of alarms with additional requirements (e.g., regulatory requirements) involving more administration and documentation than the other general alarms.

Alarm Rationalization stage shall identify the alarms to be classified as Highly Managed Alarms. Following alarms should be considered for classification as Highly Managed Alarms:

a) Safety Alarms.

b) Alarms required by standards/ regulations/ codes (e.g., alarms required by NFPA codes concerning fire suppression, Fire detection systems).

c) Alarms as decided by the Alarms Rationalization team.

1.19 Master Alarm Database

A given field typically has hundreds of alarms. Therefore, in order to facilitate tracking of alarms, including their documentation, their justification, and current status the master alarm database shall be developed during Alarm Rationalization stage of the alarm management lifecycle. The master alarm database shall be maintained throughout the remaining alarm management lifecycle stages.

The Master alarm database shall have the following information as required by ISA TR18.2.2-2016, section 9.3:

a) Alarm tag

b) Alarm type

c) Alarm set-point or logical condition

d) Potential cause of alarm

e) Nature and severity of the consequences associated with failing to respond to the alarm

f) Potential corrective actions or responses to the alarm or reference to an available response procedure

g) Time available for the operator to respond to the alarm

h) Alarm priority

i) Alarm message, if applicable

j) Alarm classification

k) Values or settings of alarm attributes

l) Any special considerations for the alarm (e.g., design factors, HMI depiction, special or applicable handling techniques or advanced methods being applied to the alarm)

m) If the process or equipment has different states that should utilize different alarm settings

Alarm System Detailed Design (AMLC Stage-D)

The purpose of the detailed design stage of AMLC is to primarily develop the alarm system requirements specification (ASRS) to capture in detail the functional and technical requirements of the alarm system.

This section of the document only captures the generic requirements for designing alarm systems which shall be incorporated in the project specific ASRS. In addition to this document, the Project/ Site Alarm Management Philosophy, MADB (Master Alarm Database), shall also be referred in developing ASRS.

1.20 Alarm System Description & General Requirements

1.20.1 Alarm System Description

All the required system hardware and software packages shall be provided to meet the requirements of the alarm system & management as narrated in this guidelines document.
The alarm system shall be part of the BPCS of the given field. The BPCS in the given field typically comprises of:

a) DCS for control monitoring of the main/ common processes/ equipment in the field. DCS is also interfaced with ESD and F&G systems and this integrated system typically referred to as ICSS.

b) Package control systems for specific processes/ equipment. Typically package control systems are also interfaced with the DCS to allow packages processes/ equipment monitoring/ control from the facility DCS.

c) SCADA: A given field may also comprise SCADA for the monitoring/ control of the part process facilities.

The main alarm sub-system operator interfaces shall be OWSs of the field DCS which are located in the control rooms. The main alarm sub-system shall implement all the functions noted in this section inclusive of basic functions (including suppression/ etc), advanced/ enhanced functions, reporting functions, performance monitoring/ assessment functions, historian functions.

In addition to the main alarm sub-system following items also have alarming features and form the part of alarm system in the facility:

a) Hardwired consoles: Typically, in the field, for the few main alarms, hardwired alarm indications are provided. Generally, these alarm indicators are provided together with push-buttons, etc for initiating manual ESD and other functions.

b) F&G System and Packages Control Systems are also provided with OWS/ HMI with alarming features. Note- The main ESD Systems located in de-gassing stations/ processing plants, generally, are not provided with the Alarming functions.

c) For the packages it is desirable that the alarms are handled from the DCS together with the package monitoring/ control. In order to facilitate this, package control systems shall be interfaced, using hardwired interfaces and soft links based on open protocols with the DCS. These Open interfaces shall typically consider OPC-A&E-OPC-DA for communicating alarms/ events/ etc information with time-stamping and MODBUS-RTU/RS-485 interface for implementing operator initiated alarm functions (like acknowledge, reset, etc.).

d) SCADA, when provided in the facility, may have their own OWSs/ HMIs with alarming features.

1.20.2 Alarm System General Requirements

The alarm system shall meet the following general/ principal requirements:

a) Implement basic alarm system functions- This include interfacing with the sensors, implement associated signal conditioning, implement alarms configuration & attributes programming, implement alarming associated logics, provide the required man-machine interfaces for operator to manage alarms including HMI/ indicators/ switches/ push-buttons.

b) Implement alarm suppression functions- This include implementing alarm shelving, suppression by design and out of service functionality by an operator to manage alarms/ alarm system whenever required/ demanded by an operator.

c) Implement advanced and enhanced alarm functions.

d) Implement alarm reporting functions- This include generation of the alarm reports shift wise, priority-wise, alarm history reports and any custom reports. The reporting shall include separate report generation for maintenance alarms.

e) Implement alarm system performance monitoring and assessment- This shall include collecting and generating statistics related to alarms KPIs defined in this guideline and reflect the real time KPI estimation in comparison with the respective targets on a dashboard graphics on HMI whenever demanded.

f) Implement Alarm Historian- This include storing the alarms history together with storing standard reports and alarm system performance monitoring and assessment data. The duration for which the historical records will be stored shall be detailed in the respective project/ site documents.

1.21 Alarm Attributes Configuration

Alarm attributes are the settings for an alarm within the alarm system. Attributes are applicable to each alarm and these are required to be configured in the alarm system. The alarm system shall allow enabling of the individual alarm conditions for a tag, such as high or low, while not enabling other conditions such as high-high or low-low. As a minimum following alarm attributes shall be addressed while designing the alarm system:

Table-4: List of principal alarm attributes
(Below table is based on ANSI/ISA 18.2-2016, clauses 6.2.13, 10.5)

Alarm Attribute	Remarks
Alarm Setpoint	Refer to elsewhere in this guidelines for the considerations to addressed while deriving alarm setpoint
Alarm deadband	Requirements are given in this section
Alarm on-delay and off-delay	Requirements are given in this section
Process value filtering	Requirements are given in this section
Default configuration of alarms	Requirements are given in this section
Alarm priority	As defined during the Alarm Rationalization stage and considerations covered elsewhere in this guideline
Alarm message composition	Requirements are given in this section

1.21.1 Alarm Deadband Requirements

Alarms design shall include deadband configuration to prevent repeat alarms caused by signal noise. Given below table shall be applied as the starting point for common processes which shall be reviewed/ verified/ evaluated for each alarm tag during given project alarm system design, implementation stages.

Table-5: Alarm deadband requirements- Initial considerations

(Below table is based on HSE-UK CRR 166/1998, The Management of Alarm Systems, Table-14 and SHELL DEP 32.80.10.14, Table 5.3)

Signal Type	Suggested Initial Setting for Deadband Equivalent To
Flow	˜ 5 % of Span
Level	˜ 5 % of Span
Liquid Pressure	˜ 5 % of Span
Gas Pressure	˜ 2 % of Span
Temperature	˜ 1 % of Span

1.21.2 Alarm On-Delay and Off-Delay Requirements

Alarms design shall include alarm on-delays and off-delays to prevent chattering and alarming of the fast transient signals. Given below table shall be applied as the starting point for common processes which shall be reviewed/ verified/ evaluated for each alarm tag during given project alarm system design, implementation stages.

Table-6: Alarm delay-off timer/ de-bouncer timer requirements- Initial considerations

(Below table is based on HSE-UK CRR 166/1998, The Management of Alarm Systems, Table-15 *and SHELL DEP 32.80.10.14, Table 5.2)*

Signal Type	Suggested Initial Setting for Delay-off/ De-bounce Timer
Flow	˜15 seconds
Level	˜60 seconds
Liquid Pressure	˜15 seconds
Gas Pressure	˜15 seconds
Temperature	˜60 seconds

1.21.3 Process Value Filtering

Process value filtering is used sometimes in addition to deadband for the process input signals that are noisy. Excessive process value filtering can potentially obscure true process variations. Based on the recommendations in ISA TR18.2.3-2015, section 8.4, it should be assessed if the process value filtering should also be applied for alarming.

1.21.4 Default Configuration of Alarms

The default alarm states for all loops in the BPCS are recommended to be set as “Not Enabled”. This is as per ISA TR18.2.3-2015, section 8.5. Once the default setting for the

alarms is done globally then activation of the individual alarm states should be carried out as needed to match the Master Alarm DataBase requirements.

1.21.5 Alarm Message Composition

For the ensuring the effectiveness of alarm messaging it is highly recommended that the message structure, terminology, abbreviations, wordings, etc be consistent and be based on the library being followed in a given facility. In case such library is not available then it is recommended to the developed while preparing project/ site specific alarm philosophy.

Following recommendations for alarm message composition, as enumerated in ISA TR18.2.3-2015, section 8.7 shall be followed:

a) Clearly identify the condition that has occurred (e.g., Separator-ABC High Temperature).

b) Do not duplicate information provided by other displayed fields such as alarm priority, tag name or alarm type.

c) Use terms that the operator is familiar with.

d) Use consistent abbreviations from a standard site dictionary of abbreviations. In case such information is not available then the alarm system currently being operated shall be used for generating such library.

e) Define a consistent message structure. Recommended to structure the message as equipment/ parameter/ condition/ alarm setpoint/ current value of PV/etc. For example, Separator-ABC Pressure High.

f) Do not rely on the learning of tag names or numbers by the operator- Identification of the alarm should use the text description of the device or equipment and its location.

g) Indicate the cause of the trip or shut-down for first out alarm messages. For example, Separator Trip on High Liquid Level.

h) Check the usability during plant operations.

1.22 Alarm System HMI Design

HMI design for alarm systems shall meet following references requirements as a minimum:

a) ANSI/ ISA 18.2-2016, section 11 (describes functional, informational, reporting, display requirements related to alarm system),

b) SHELL DEP 30.00.60.16- Feb 2017, Human Factors Engineering- Human Machine Interface Design for Situation Awareness.

c) ASM Consortium Guidelines- Effective Console Operator HMI Design.

d) "The High Performance HMI Handbook", 1st Edition by Hollifield, Oliver, Nimmo & Habibi, Published- PAS, USA.

The subsequent below sub-sections sometimes refer to specific sections of ANSI/ ISA 18.2-2016. These sections of ANSI/ ISA 18.2-2016 should not be read in isolation as the complete standard is applicable for meeting the requirements of this document. Also, standards other than ANSI/ ISA have multiple of sections applicable to every single sub-sequent below sub-sections and therefore specific sections have not been identified for these standards.

1.22.1 Alarm System HMI Functions

For the purpose of alarm system HMI functions the requirements and recommendations given in ANSI/ ISA 18.2-2016, clause no. 11.2 shall be followed.

1.22.2 Alarm State Indications

For the purpose of alarm state indications given below requirements narrated in the table shall be followed in line with the requirements given in ANSI/ ISA 18.2-2016, clause no. 11.3:

Table-7: Alarm States and Audio-Visual notification requirements

(Below table is based on ANSI/ ISA 18.2-2016, Table-4 with the customization highlighted using shaded cells of the table.)

Alarm State	Audible Presentation	Visual Indications		
		Colour	Symbol	Blinking
Normal	No	No	No	No
Unacknowledged alarm	Yes	Yes	Yes	Yes
Acknowledged alarm	No	Yes	Yes	No
Return-to-normal unacknowledged alarm	No	Combination		No
Shelved alarm	No	Yes		N/A
Suppressed-by-design alarm	No	Yes		N/A
Out-of-service alarm	No	Yes		N/A

Note 1- "Yes" signifies the indication type should be used to indicate the alarm state.
Note 2- "No" signifies the indication type should not be used to indicate the alarm state.
Note 3- "N/A" signifies not applicable or that the condition is not relevant to the alarm state.
Note 4- "Combination" signifies the indication is combination of visual colour and symbol indications.

1.22.3 Alarm Priority Indications

The alarm priority is recommended to be indicated using the combination of colour coding & symbols in line with the recommendations of "ASM Consortium Guidelines- Effective Console Operator HMI Design". Following table depict the indications to be used for showing alarm priority in the various HMI displays.

Table-8: Alarm priority indication shape/colour/text coding for HMI Displays
(Below table is based on ASM Consortium Guidelines- Effective Console Operator HMI Design- 2015, 2nd edition, Section D-4.2.)

Alarm Priority Level	Alarm Priority Designation	Recommended Visual Indication- Colour & Symbol	Remarks
Priority 1	Critical	1	Symbol- Square Symbol Colour (border & fill)- **RED** Symbol text to indicate priority level
Priority 2	High	2	Symbol- Circle Symbol Colour (border & fill)- **ORANGE** Symbol text to indicate priority level
Priority 3	Low	3	Symbol- Triangle Symbol Colour (border & fill)- **CYAN** Symbol text to indicate priority level

Designs of HMI displays are critical for operations management. For the HMI displays to be effective not only the alarms indications, but, the general philosophy of showing normal and abnormal conditions in the process in the HMI displays are important.
Below figure is taken from "ASM Consortium Guidelines- Effective Console Operator HMI Design" showing the recommended process graphics with alarm indications.

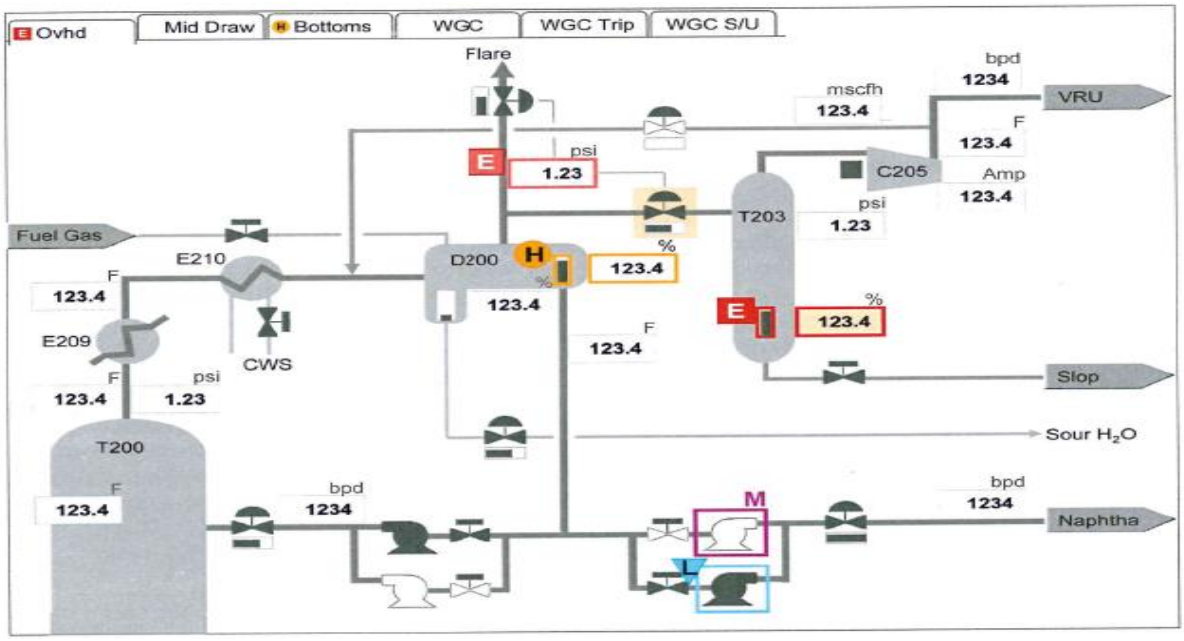


Figure-3: Alarms indication on HMI Displays- Process Graphics
(Above figure is based on ASM Consortium Guidelines- Effective Console Operator HMI Design- 2015, 2nd edition, Figure-AP-3.5)

Note that the above mentioned ASM Consortium Guidelines, in order show alarm priority indication in the graphics, uses the abbreviation, E (for “Emergency” Priority), H (for “High” Priority), L (for “Low” Priority) indications within the respective symbols.

1.23 Alarm Message Indications

For the purpose of alarm messages indications the requirements and recommendations given in ANSI/ ISA 18.2-2016, clause no. 11.4 shall be followed. Further, it is suggested to use only the visual alarm message indications in the alarm systems. Vocalized alarm messages are generally not used in the alarm system and their use shall be critically reviewed and justified.

1.24 Alarm Displays

For the purpose of alarm messages indications the requirements and recommendations given in ANSI/ ISA 18.2-2016, clause no. 11.6 shall be followed. This referred standard capture the requirements pertaining to generic issues, alarm summary displays, alarm summary status, alarm log displays, process displays, tag detail displays and other display elements, etc.

1.25 Alarm Shelving

The alarm system shall allow operator initiated controlled access shelving, i.e., temporary suppression, of the alarms. Alarm shelving is the temporary suppression of alarm by the operator which is generally used to keep nuisance alarm from interfering with the effectiveness of the alarm system. Shelving function, when implemented, shall ensure that the integrity of the alarm system is maintained.

1.25.1 Applications of Alarm Shelving

As a general rule the suppression of an alarm or group of alarms shall be avoided unless the suppression becomes necessary to temporarily suppress the nuisance alarm(s) in order to maintain the alarm system effectiveness.

Following conditions should exist for the alarm or group of alarms to allow alarm shelving:

a) The condition of nuisance alarm(s) is present,

b) Temporary suppression of the given alarm will not lead to the situations that would impact safety and/ or production effectiveness. In the cases this condition is not met then there shall be another way of monitoring the same event with the required.

c) Alarm shelving of the alarms which are associated with safety and/ or production effectiveness shall be through access controlled methods,

d) Alarm shelving of the group of alarms shall be always through access controlled methods.

1.25.2 Alarm Shelving Requirements

Alarm shelving functional and displays requirements shall be as per ANSI/ISA 18.2-2016, section 11.7 and SHELL DEP 32.80.10.14, Feb 2017, section 6.2. Further, the functional recommendations in these standards shall also be implemented.

1.26 Our-Of-Service Alarms

The alarm system shall allow operator initiated controlled access for placing an alarm out of service using suppression to remove alarms from service and to allow maintenance.

1.26.1 Applications of Out-Of-Service Alarms

Out-of-service alarms shall be applied to the given process/ equipment wherein it is technically acceptable and required from maintenance view point to place, via access control, the process/ equipment under out-of-service condition. Once the process/ equipment is placed in out-of-service condition then it is recommended to remove the service of the related alarms by suppression till the process/ equipment is again put back in the service condition.

Out-of-service alarms shall always be through access controlled methods.

1.26.2 Out-Of-Service Requirements

Out-of-service alarm displays requirements and functional requirements shall be as per ANSI/ISA 18.2-2016, section 11.8 and SHELL DEP 32.80.10.14, Feb 2017, section 6. Further, the recommendations in this standard pertaining to out-of-service alarm displays shall also be implemented.

1.27 Alarms Suppression by Design

The alarm system shall have/ allow the alarms suppression by design functionality. Alarms suppression by design shall be implemented wherein alarm are not needed due to intended or actual operating conditions (e.g., stand-by condition) of the associated process/ equipment. This functionality shall support the testing, maintenance and operator understanding of designed suppression.

1.27.1 Application of Alarms Suppression by Design

Alarms suppression by design should be applied to the cases involving the part of the process/ equipment with non-working condition/ stand-by condition as one of the operation state. The scheme shall be critically reviewed and it shall be qualified, alarm tag wise, that the alarm suppression shall not inhibit the notification of impending safety/ critical situation which could happen even when the associated process part/ equipment is not working.

1.27.2 Alarms Suppression by Design Requirements

Alarms suppression by design displays requirements and functional requirements shall be as per ANSI/ISA 18.2-2016, section 11.9 and SHELL DEP 32.80.10.14, Feb 2017, section 6. Further, the recommendations in this standard pertaining to alarms suppression by design alarm displays and functions shall also be implemented.

1.28 Highly Managed Alarms

Highly managed alarms are the class of alarms with additional requirements above the general alarms. The additional requirements may be required in order to comply with the regulations/ standards (like API/ NFPA/ etc) or on account of specific application (like Safety related alarms). Safety related alarms typically are associated with the operator initiated risk reduction measures for a specific risk scenario. Technically, Safety alarms are required to be periodically proof-tested to ensure that the associated risk reduction factor remain valid during Operation & Maintenance stage.

For the purpose of designing highly managed alarms following shall be considered:

a) Highly managed alarms may be provided with separate HMI considering risk reduction factors and/ or associated standard/ regulation/ code requirements. This shall be assessed on case to case basis during engineering stage of the given project.

b) Highly managed alarms implementation on account of compliance requirements to the standards/ regulation/ code shall generally follow the respective reference document requirements.

1.29 Alarm Annunciation

It is common practice to provide hardwired alarm annunciation on the auxiliary panel/ console for the few critical alarms in the facility. The requirement of such hardwired alarm annunciation panel/ console shall follow the requirements given in ANSI/ISA 18.2-2016.

1.30 F&G HMI/ MIMIC Panel

For the purpose of facility F&G system HMI design and MIMIC panel involving notification of alarms, etc the requirements given in the SHELL DEP 32.30.20.11 shall be followed.

1.31 Access Control Methods

The design of HMI/ OWS used for alarm operations/ maintenance shall ensure that appropriate entities/ personnel have accounts that allow access and that these accounts provide appropriate access privileges. Access control is the method of controlling who or what entities/ personnel can access the alarm systems and what type of access is permitted.

Wherever this guideline specifies implementation through access control methods, at-least additional access control of the subject features/ functions/ operations by Supervisory level is required to be considered in the design.

Alarm System Implementation (AMLC Stage-E)

Alarm system Implementation stage is the transition stage from design to operation. Specifically, this stage includes the following:

a) Installation

b) Testing/ Validation

c) Documentation Verification

d) Training

Alarm system implementation shall generally follow the requirements given for this stage in ANSI/ ISA 18.2-2016.

1.32 Installation, Testing & Validation

The installation of the alarm system shall follow the guidelines for installation of BPCS and shall generally be in-line with the standards API RP 554-1, -2 & -3 and the procedure specific to system as recommended by the vendor.

Testing & validation requirements and recommendations as described in ANSI/ ISA 18.2-2016 shall be followed. Further, as alarm system generally is the part of BPCS the requirements given in SHELL DEP 62.10.08.11 “Inspection and Functional Testing of Instruments” and API RP 554-1, -2, -3 shall also be followed.

1.33 Documentation Verification

Implementation stage is a stage before operation and therefore it is essential that the necessary documentation for the alarms system is available to the operator reflecting complete and correct information. The documentation shall be available and verified for correctness and completeness during Implementation stage for the coverage of the following areas:

a) Project Specific Alarm Philosophy

b) Alarm Rationalization Report

c) Master Alarm DataBase

d) Alarm System Requirement Specifications

e) Alarm Response Procedures

f) Suppression Alarming documentation

g) Alarm system testing procedures.

h) IOM Manual.

i) System design (including, I/O Assignment, System Configuration, FDS, SDS, HMI Specification, Data-Sheets)

1.34 Training

Operator & Maintenance training shall be provided to the respective site personnel during the implementation stage as the same is essential before handing over the system to the ADNOC ONSHORE site/ facility team.

Operator training shall include familiarization on the complete HMI design features for handling alarms. Specifically, the following topics shall be given thorough coverage:

a) Alarm Philosophy

b) Alarm Rationalization results

c) Master Alarm DataBase

d) Alarm displays, logs & reports

e) HMI functional features

f) Alarm Suppression (Shelving, Suppression, Suppression by design)

g) Highly managed alarms

h) Alarm response procedure references

i) Alarm system performance monitoring & assessment

Maintenance training shall include familiarization of the alarm system architecture together with HMI features. Specifically, the following topics shall be given due coverage:

a) Alarm Philosophy

b) Master Alarm DataBase

c) ASRS

d) Alarm system testing procedures.

e) IOM Manual.

f) System documents (including, I/O Assignment, System Configuration, FDS, SDS, HMI Specification, Data-Sheets)

Alarm System Operation (AMLC Stage-F)

Alarm System Operation is the alarm management lifecycle following implementation and when returning from maintenance.

Formal handover of the Alarm Systems to ADNOC Onshore Operations team shall only be undertaken after successful execution of works in “AMLC Stage-E: Implementation”. As the Alarm Systems in ADNOC Onshore facilities is the part of BPCS the handover is dependent on the works completion & readiness of BPCS, DCS, F&G Systems and other required systems/ equipment needed for ensuring safe operations. As the part of formal handover following essential documentation, finalized to reflect the as-is and agreed status, shall be provided to Operations:

a) Alarm Philosophy

b) Alarms & Trips set-points list

c) MADB: Master Alarm DataBase

d) ASRS: Alarm System Requirements Specification

e) Alarm system testing procedures.

f) IOM Manual.

g) System documents (including, I/O Assignment, System Configuration, FDS, SDS, HMI Specification, Data-Sheets)

For the purpose of operations related to alarms systems, MADB shall be used as the primary reference. Consequently, MADB shall be developed with all the requisite information about the alarm and the associated operator actions required & the related consequences. The alarms systems related HMIs/ OWSs should be designed to include targeted & quick reference to MADB to facilitate quick & correct operator actions.

1.35 Purpose

This section covers requirements for alarms to remain in and return to the operational state. The operational state is when an alarm is on-line and able to indicate an abnormal condition to the operator. This section also describes appropriate use of tools for alarm handling within the operational state.

Note: Out-of-service alarms are discussed as the part of AMLC Stage-G: Alarm System Maintenance (clause no. 9).

1.36 Alarm Response Procedures

The operator response procedures to the alarms shall be detailed/ referenced in Master alarm database and shall be readily accessible to the operator for executing the associated tasks.

1.36.1 Alarms Response Procedure Requirements

The Master alarm database shall be used as reference for operator response procedures and related alarm information. Refer section 5.6 of this guidelines document which addresses Master alarm database requirements.
During AMLC-D stage, i.e., Alarm System Detailed Design stage, the requirement of other forms of developing & maintaining the alarm response procedures, if required, shall be addressed taking into account ADNOC Onshore Operations & Maintenance requirements.

1.37 Alarm Shelving

Alarm shelving requirements shall be addressed in the project/ site alarm philosophy taking into consideration the requirements of section 8.6 of this guideline document.

1.37.1 Alarms Shelving Operations Requirements

Following are the alarm shelving operations requirements:

a) Shelved alarms shall be reviewed at the beginning of each shift.

b) The operator should be permitted to shelve alarms after necessary approvals to prevent unnecessary distraction due to unforeseen alarm system malfunctioning alarms. Shelved alarms extending beyond a single operating shift should be reauthorized.

1.37.2 Alarms Shelving Operations Requirements for Highly Managed Alarm

If a highly managed alarm class is used then shelving highly managed alarms shall follow authorization and reauthorization requirements as detailed in the alarm philosophy.
An audit trail shall be maintained recording approval, interim alarms and procedures, and reauthorization details.

1.37.3 Alarms Shelving Records

The following information shall be recorded for each shelved alarm extending beyond a single operating shift:

a) Alarm name,

b) The reason for shelving

Alarm System Maintenance (AMLC Stage-G)

Alarm System Maintenance stage of AMLC involves alarm or alarm system in non-operational state but is being tested or repaired.

1.38 Purpose

This section covers the activities, inclusive of testing, replacement (in-kind) & repair, necessary to maintain the alarm system. Specific elements that are covered in this section include:

a) Alarm maintenance history archiving,

b) The requirement around out-of-service alarms,

c) The policy on the use of interim alarms

Further, requirements for maintenance refresher training for personnel maintaining the alarm system are addressed

1.39 Periodic Testing

Periodic testing requirements for alarms shall be determined as detailed during the AMLC State-D, i.e., Alarm System Detailed Design stage, and as detailed below.

1.39.1 Periodic Testing Requirements

The requirements of periodic testing of the alarm/ alarm systems shall be determined during AMLC State-D, i.e., Alarm System Detailed Design stage.
Highly managed alarms should be tested at least once a year; preventive maintenance program should be prepared accordingly.
Any deficiencies found during functional testing of highly managed alarms shall be repaired or else an interim alarm or procedure shall be put in a timely manner.

1.39.2 Periodic Testing Procedure Requirement

Test procedure should be provided for alarm requiring testing. Procedures should contain:

a) Steps for taking the alarm out-of-service prior to the test and returning the alarm to service after the test,

b) Appropriate warnings regarding control loops or final elements that might be affected by the test,

c) Steps to address advanced alarming techniques if applicable

1.39.3 Periodic Testing Records

When tests are performed, a record shall be kept for and shall contain the following as minimum:

a) Date(s) of testing,

b) Name(s) of person(s) who performed the test or inspection,

c) Unique identifier of equipment (e.g., loop number, tag number, equipment number)

d) Method of testing,

e) Planned interval before next test

1.40 Out-of-Service Alarms

Out-of-service requirements for alarms shall be addressed in the project/ site alarm philosophy taking into consideration the requirements of section 8.7 of this guideline document.

1.40.1 Out-Of-Service Alarms Authorization Process

Approval requirements for taking alarm(s) out-of-service are as follows:

a) Operation Team Leader or designee shall authorize out-of-service alarm within one shift.

b) Operation Manager or designee shall authorize out-of-service alarm if extending more than one shift. He should also seek the requirement of any alternative.

1.40.2 Out-Of-Service Process Requirements

Alarms that will be compromised for extended durations (e.g., days, weeks, or months) shall be examined to determine whether an alternative alarm is necessary. If an interim is necessary then it shall adhere to management of change requirements.

An authorization and documentation process (e.g., permit process) shall be used to take an alarm out-of-service. A list/register of out-of-service alarms shall be available for review on-demand with their corresponding replacement where applicable.

The following information shall be recorded for each out-of-service alarm:

a) The name of the tag in alarm,

b) The alarm type,

c) Approval details,

d) Details concerning interim alarms of procedures if required,

e) The reason for taking the alarm out-of-service

1.40.3 Out-Of-Service Process Requirements for Highly Managed Alarms

If a highly managed alarm is taken out-of-service for longer than one shift, appropriate interim alarms or procedures shall be identified unless the process is in a state where the consequence has been eliminated.

1.41 Alarm System Equipment Repair

Information related to an alarm malfunction should be available to the operator. Alarms affected by non-functioning equipment (e.g., equipment that is taken out-of-service for repair or preventative maintenance) should be placed out-of-service if the condition will not resolved within a reasonable time as determined during AMLC State-D, i.e., Alarm System Detailed Design stage.

1.42 Alarm System Equipment Replacement

If replacement equipment (e.g., measurement devices, valves, process equipment) will change operating conditions or alarm attributes, then management of change procedures should be followed. Replacements that do not result in such changes do not require management of change. If a replacement is made then alarm validation shall be performed as the part of standard procedure.

1.43 Returning Alarms to Service State

Prior to returning out-of-service alarms to the operational state, operators shall be notified to ensure they are aware of the returning alarm and the removal of the interim methods.

1.43.1 Recommendations for Returning Alarm to Service

Interim alarms and procedures should be removed, where applicable, when the original alarms are returned to service.

1.44 Refresher Training for Maintenance

The refresher training requirements for the maintenance of alarms shall be assessed during the Alarm System Maintenance stage and whenever there is a change in the alarm/ alarm system.

1.44.1 Refresher Training Requirements for Highly Managed Alarms

If a highly managed alarm class is used then the appropriate personnel shall be periodically trained on the maintenance requirement for all highly managed alarms. Documentation of the training shall include the persons trained, the method of training, and the date of the training.

1.44.2 Refresher Training Recommendation for Alarms

Maintenance personnel should receive periodic training on the maintenance requirements of alarms.

1.45 Alarm System Maintenance Records

As the part of alarm system maintenance following records should be generated and maintained periodically:

a) Alarm records (as required),

b) Alarm System Maintenance Logs (including proof-testing, repairs, lessons learned, etc)

c) Out-of-Service alarms list and associated records

d) Training records

e) etc

Alarm System Monitoring & Assessment (AMLC Stage-H)

1.46 Alarm System Performance Requirements

The main purpose of the alarm system is to aid the operator by informing him/ her the impending & evolving process situations which have potential to exceed the normal operating conditions and allow sufficient time to initiate operator action(s) to contain the situation within the normal/ safe conditions. In some situations the alarms/ alerts are activated when the process has already exceeded/ passed the design limit, for example, Gas detection & Fire Detection Alarms, during which the purpose of the alarm system is to limit the consequence and aid in the facility emergency procedures.

In order to ensure the effectiveness of the alarm system the design is required to take into consideration the Operator as a trained human being. Human reliability is significantly & negatively impacted by the increase in the complexity in the required operations, less time available for completing the required operations and operational stresses associated with the impending & developing abnormal situation in the process and various other factors. It is therefore necessary to define performance requirements for the alarm systems with an "Operator" as the key consideration. Following table prescribes the KPIs for the alarms system for a given facility and:

Table-9: Alarm System Performance KPI Target Values

(Below table is based on is based on ANSI/ ISA 18.2-2016, Table-7)

S.No.	KPI Definition	KPI Target Value (Maximum Value)
1.	Average annunciated alarms per hour per operator console	12
2.	Average annunciated alarms per 10 minutes per operator console	2
3.	Percentage of 10-minute periods containing more than 10 alarms	1%
4.	Maximum number of alarms in a 10-min period	10
5.	Percentage of time the alarm system is in a flood condition	1%
6.	Percentage contribution of the top 10 most frequent alarm to the overall alarm load	5%
7.	Quantity of chattering and fleeting alarms	Zero

		(Note-2)
8.	Stale alarms	Less than 5 on any day (Note-2)
9.	Annunciated priority distribution (The alarm priority distribution should also be used for Alarm Prioritisation Assessment/ Workshop.	Critical- 5% High- 15% Low- 80%

Notes:

1. The actual performance indicators of the alarms/ alarm system shall be generated by evaluating/ considering related statistics for the period of 30 days and compared against the target value for the respective KPIs.
2. Action plan shall be developed to address deficiencies as and when discovered.

1.47 Alarm System Monitoring & Assessment Requirements

Alarm system periodic monitoring and assessment is essential to ensure operations effectiveness with respect to handling alarms and related probable exigencies.
Alarm system periodic monitoring shall be carried out after every 30 days. This is primarily required as alarm KPIs target values suggested elsewhere in this guideline are averaged over 30 days.

As suggested in ISA TR 18.2-2016, clause 16.7, at various phases of an improvement effort, different analyses should be performed at different reporting periods (e.g., providing weekly reports at the start of an effort and monthly reports later on). Weekly analysis shall cover the prior 30 days of data to produce meaningful trends.
Typical requirements for the topics to be addressed in the Alarm System Monitoring & Assessment reports are covered in clause 3.2, Table-1, Note g.

Alarm System Management Of Change (AMLC Stage-I)

Management of change stage of the lifecycle is applied for an operational alarm system and when any of the following change or in combination are required:

a) Addition of new alarms
b) Removal of existing alarms
c) Alarm attribute modification
d) Changes to alarm system functions

The principal aspect of MOC stage shall be to keep MADB and other associated documents updated and be maintained for every relevant MOC activity. This ensures that the operations and maintenance functions consider updated/ latest MADB.

An important aspect of the MOC is technical review and associated authorization for the change before implementation.

For the management of change the existing MOC procedure shall be followed. Refer ADNOC Onshore standard procedure, “Manage MoC Business Process (Management of Change)”, Rev-1.

Alarm System Management Audit (AMLC Stage-J)

1.48 Purpose

Audit shall be conducted periodically to maintain the integrity of the alarm system and alarm management processes. The primary purpose of the Audit of the Alarm System and the associated Alarm Management Processes is to reveal gaps not apparent from monitoring.

During the Audit the actual Alarm System and the associated Alarm Management Processes are assessed against this guidelines document together with the project/ site alarm philosophy document to identify any requirements for system improvements, such as modifications to the alarm philosophy or the work process defined therein. The Audit determines whether the current alarm management practices are sufficient to adequately administer the system by reviewing practices vs. procedures and procedures vs. policy or requirements. Audit also includes comparison of the alarm management practices against the newly developed industry guidelines not addressed in this guidelines document and/ or project/ site alarm philosophy document. The frequency of the audit process is lower than monitoring and assessment.

1.49 Audit Interviews

Personnel interviews or questionnaires should be conducted as part of the audit to identify performance and usability issues. Interview topics may include:

a) Alarms occur only on events that require operator action,

b) Alarm priority is consistently applied and meaningful,

c) Alarms occur in time for effective action to be taken,

d) Roles and responsibilities for the alarm system users and support personnel are clear, and

e) Training regarding the proper use and functioning of the alarm system is effective.

It is the responsibility of Audit Committee to schedule, conduct, and document the annual audit.

1.50 Audit Requirements

The alarm philosophy should be audited against these guidelines document together with the project/ site alarm philosophy document taking into considerations the newly developed industry guidelines. The work processes and procedures that ensure compliance with the alarm philosophy should be evaluated for effectiveness on a periodic basis. The audit should review work practice documentation, including:

a) Verification that alarms are used only to represent situations that require operator action to avoid defined consequences,

b) Documentation of alarm settings and rationalization,

c) Alarm documentation in the Master Alarm Database is current and sufficient to provide for proper operator guidance

d) Modification of alarms is properly controlled by MOC

e) Alarm performance monitoring reports,

f) Documentation of repairs to malfunctioning alarms, and

g) Documentation for out-of-service alarms.

h) Roles and responsibilities for the alarm system users and support personnel are clear, documented, and known by appropriate personnel.

1.51 Action Plan

Action plan must be developed for problems identified during the audit process. When defining an action plan, timelines, accountabilities, and review of results obtained shall be assigned to each item.

Appendices

Appendix-A: Alarm Management Related Definitions

Appendix-B: Alarm Prioritization Flowchart

Appendix-C: ADNOC Risk Matrix

Abu Dhabi Company for Onshore Petroleum Operations Ltd.شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

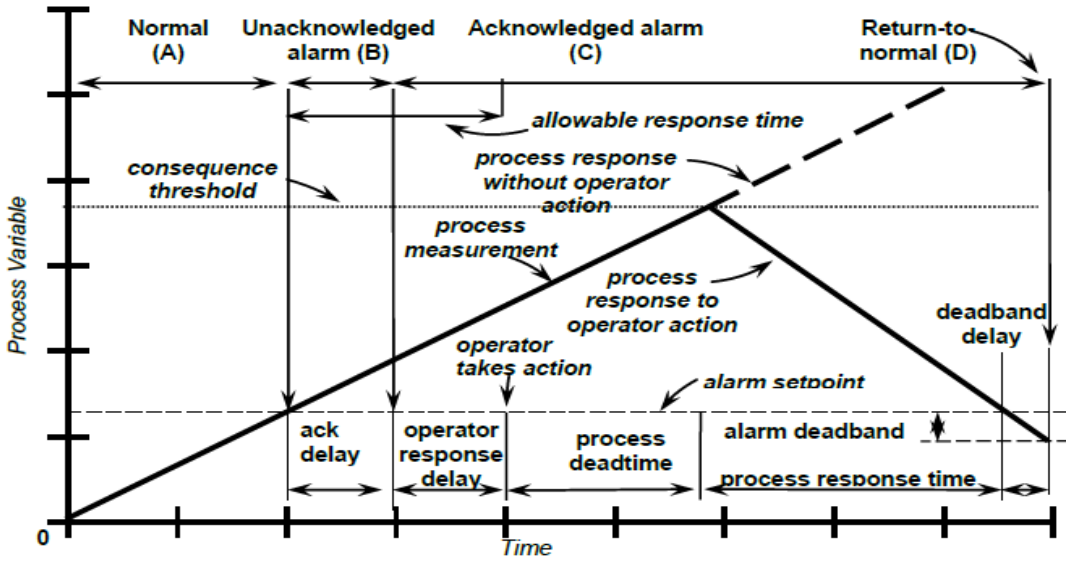
Appendix-A : Alarm Management Related Definitions

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Given below figure from ISA 18.2-2016 (clause no. 5.4.1) depicts the process measurement and various conditions/ terms related to alarm & associated operator actions.

Figure-4: Alarm Response Time
(From ISA 18.2-2016, clause 5.4.1, Figure 4)



For the purpose of this document the terms given in the documents mentioned in the "References" section apply. However, some of the terms from the documents mentioned in the "References" section, have been reproduced below for ready reference.

Basic Terms	
Alarm	Audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response
Alarm class	Group of alarms with common set of alarm management requirements (e.g., testing, training, monitoring, and audit requirements)
Alarm flood	Condition during which the alarm rate is greater than the operator can effectively manage (e.g., more than 10 alarms per 10 minutes)
Alarm group	Set of alarms with common association (e.g., process unit, process area, equipment set, or service)
Alarm historian	Long term repository for alarm records
Alarm log	Short term repository for alarm records

Alarm management/ Alarm system management	Collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems
Alarm priority	Relative importance assigned to an alarm within the alarm system to indicate the urgency of response (e.g., seriousness of consequences and allowable response time)
Alarm summary alarm list	Display that lists annunciated alarms with selected information (e.g., date, time, priority, and alarm type).
Alarm system	Collection of hardware and software that detects an alarm state, communicates the indication of that state to the operator, and records changes in the alarm state
Alarm system requirements specification	Document which describes the functionality of the alarm system
Alert	Audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness and which does not meet the criteria for an alarm
Allowable response time	Maximum time between the annunciation of the alarm and when the operator must take corrective action to avoid the consequence
Classification	Process of separating alarms into alarm classes based on common requirements (e.g., testing, training, monitoring, and auditing requirements)
Consequence threshold	The consequence threshold is the value of the process measurement at which the consequence begins to occur. The consequence results when no operator action is taken, incorrect or insufficient action is taken or the action is not completed within the allowable response time.
Enforcement	Enhanced alarming technique that can verify and restore alarm attributes in the control system to the values in the master alarm database
Event	Representation of a solicited or unsolicited fact indicating a state change
Interim alarm	Alarm used on a temporary basis to replace an out -of-service alarm
Master alarm database	Authorized list of rationalized alarms and associated attributes
Remote alarm	Alarm from a remotely operated facility or directed to a remote interface

Alarm Attributes Related Terms	
Alarm attribute	Setting for an alarm within the process control system
Alarm deadband	Change in signal from the alarm setpoint necessary for the alarm to return to normal
Alarm description	Informative text provided as a tag description, or alarm description, or both
Alarm group	Set of alarms with common association (e.g., process unit, process area, equipment set, or service)
Alarm message	Text string displayed with the alarm indication that provides additional information to the operator (e.g., operator action)
Alarm off-delay Debounce	Time an alarm remains active after the process measurement has returned within the alarm setpoint
Alarm on-delay	Time before an alarm becomes active after the process measurement has exceeded the alarm setpoint
Alarm priority	Relative importance assigned to an alarm within the alarm system to indicate the urgency of response (e.g., seriousness of consequences and allowable response time)
Alarm setpoint Alarm limit Alarm trip point	Threshold value of a process variable or discrete state that is used to determine if the alarm is active
Alarm Lifecycle Related Terms	
Alarm philosophy	Document that establishes the basic definitions, principles, and processes to design, implement, and maintain an alarm system
Alarm Identification	General term for the different methods that can be used to determine the possible need for an alarm or a change to an alarm
Alarm Rationalization	Process to review potential alarms using the principles of the alarm philosophy, to select alarms for design, and to document the rationale for each alarm
Alarm prioritization	Process of assigning a level of operational importance to an alarm
Detailed design	Phase wherein additional alarm attributes are specified and designed based on the requirements determined by rationalization. There are three areas of design: basic alarm design, HMI design, and design of advanced alarming techniques
Alarm Implementation	Transition stage between design and operation during which the

	alarm is put into service
Alarm (System) Operation	The operational state is when an alarm is able to indicate an abnormal condition to the operator. Operation is the lifecycle stage following implementation and when returning from maintenance.
Alarm (System) Maintenance	Phase wherein the transition of alarms to the out-of-service state and then return to service.
Alarm (System) Assessment	Comparison of information from monitoring and additional qualitative (subjective) measurements, against stated goals and defined performance metrics
Alarm (System) Monitoring	The measurement and reporting of quantitative (objective) aspects of alarm system performance
Management of change (Alarm (System))	Phase wherein modifications to the alarm system are proposed and approved. The change process should follow each of the alarm management lifecycle stages from identification to implementation
Alarm (System) Audit	Comprehensive assessment that includes the evaluation of alarm system performance and of the work practices used to administer the alarm system
Alarm Operations Related Terms	
Acknowledge	Operator action that confirms recognition of an alarm
Active	An alarm in a state in which the alarm condition is true
Advanced alarming	Collection of techniques that can help manage annunciations during specific situations
(Alarm) filtering	Function which selects alarm records to be displayed according to a given element or elements of the alarm record
Alarm response procedure	Guidance for response to an alarm (e.g., operator action, probable cause)
(Alarm) sorting	Function which orders alarm records to be displayed according to a given element of alarm record
Chattering alarm	Alarm that repeatedly transitions between active state and not active state in a short period of time
Fleeting alarm	Alarm that transitions between an active alarm state and a not active alarm state in a short period of time without rapidly repeating
Highly Managed Alarm (HMA)	Alarm belonging to a class with additional requirements (e.g., regulatory requirements) above general alarms
Latching alarm	Alarm that remains in alarm state after the process condition has returned to normal and requires an operator reset before the

	alarm returns to normal
Nuisance alarm	Alarm that annunciates excessively, unnecessarily, or does not return to normal after the operator action is taken
Out-of-service	State of an alarm during which the alarm indication is indefinitely suppressed, typically manually, for reasons such as maintenance
Reset	Operator action that unlatches a latched alarm
eturn to normal/ Clear	Alarm transition from an active alarm state to a not active alarm state
Shelve	Temporarily suppress an alarm, initiated by the operator, with engineering controls (e.g., timelimited) that unsuppress the alarm
Silence	Operator action that terminates the audible alarm indication
Stale alarm	Alarm that remains annunciated for an extended period of time (e.g., 24 hours)
Suppress	Prevent the annunciation of the alarm to the operator when the alarm is active
Unacknowledged	Alarm state in which the operator has not yet confirmed recognition of an alarm indication
Terms Related to Alarm Types	
Alarm type	Alarm attribute which gives a distinction of the alarm condition
Absolute alarm	Alarm generated when the alarm setpoint is exceeded (e.g., high-high, high, low, low-low)
Adaptive alarm	Alarm for which the setpoint is changed by an algorithm (e.g., calculated based on production rate)
Adjustable alarm operator-set alarm	Alarm for which the setpoint can be changed manually by the operator
Bad-measurement alarm	Alarm generated when the signal for a process measurement is outside the expected range (e.g., 3.8mA for a 4 to 20mA signal)
Bit-pattern alarm	Alarm that is generated when a pattern of digital signals matches a predetermined pattern
Calculated alarm	Alarm generated from a calculated value instead of a direct process measurement
Controller-output alarm	Alarm generated from the output signal of a control algorithm (e.g., PID controller) instead of a direct process measurement
Deviation alarm	Alarm generated when the difference between two values exceeds an alarm setpoint (e.g., deviation between primary and

	redundant instruments or a deviation between process variable and controller setpoint)
Discrepancy alarm mismatch alarm	Alarm generated by the difference between the expected plant or device state to its actual state (e.g., when a motor fails to start after it is commanded to the on state)
First-out alarm First-up alarm	Alarm determined (i.e., by first-out logic) to be the first, in a multiple-alarm scenario
Instrument diagnostic alarm	Alarm to indicate a field device or signal fault
Rate-of-change alarm	Alarm generated when the change in process variable per unit time (dPV/dt) exceeds a defined setpoint
Re-alarming alarm Re-triggering alarm	Alarm that is automatically re-annunciated to the operator under certain conditions
recipe-driven alarm	Alarm with setpoints that depend on the recipe that is currently being executed
Safety alarm Safety related alarm	An alarm that is classified as critical to process safety for the protection of human life or the environment
Statistical alarm	Alarm generated based on statistical processing of a process variable or variables
System diagnostic alarm	Alarm generated by the control system to indicate a fault within the system hardware, software or components

Appendix-B : Alarm Prioritisation Flowchart

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Basis of Alarm Prioritisation Methodology

The potential alarms cases for which there are no specific requirements of priority assignments are given in SHELL DEP 32.80.10.14, Feb 2017 then such cases shall be subjected to assessment as per the Alarm Prioritisation Flowchart described in Appendix-II of this document.

The Alarm Prioritisation Flowchart given in Appendix-II is based on "Method 4- General Alarm Assessment" in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013. Further, Appendix-II also captures the equivalence/ mapping of the consequence categories described in ADNOC Corporate Risk Matrix Version 1 June 2018 (Refer Appendix-C of this document) with the categories used in "Method 4- General Alarm Assessment" in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013.

General Considerations for Alarm Prioritisation Process

a) Alarm prioritisation shall be carried out as multi-discipline workshops. Following personnel should participate in alarm prioritisation workshops:

   i. Facilitator: Facilitator shall lead the workshop. The Facilitator shall be technically qualified with the requisite experience in the field of Alarm Management (and associated areas) in general and in AMLC stages A2, B, C & D in particular. The Facilitator shall have proven experience in facilitating & leading the Alarm Prioritisation workshops for the process facilities similar to ADNOC Onshore. It is desirable that the Facilitator carry formal training in Alarm Management and is knowledgeable in the standards referred in this guidelines document. Facilitator shall be arranged by CONTRACTOR/ CONSULTANT and prior approval from ADNOC Onshore shall be taken.

   ii. Project Manager (CONTRACTOR/ CONSULTANT/ COMPANY) (Optional)

   iii. Engineering Manager (CONTRACTOR/ CONSULTANT/ COMPANY) (Optional)

   iv. Process Engineers (CONTRACTOR/ CONSULTANT/ COMPANY)

   v. Instrumentation Engineers (CONTRACTOR/ CONSULTANT/ COMPANY)

   vi. Other Discipline Eng(CONTRACTOR/CONSULTANT/COMPANY)(As required)

   vii. Operation & Maintenance (Instrumentation) Engineers (COMPANY)

b) Following table captures the equivalence in the consequence categories described in ADNOC Corporate Risk Matrix Version 1 June 2018 with the categories noted in "Method 4- General Alarm Assessment" in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013:

Table-10: Consequence severity levels equivalence

Below table maps consequence severity levels described in ADNOC Corporate Risk Matrix Version 1 June 2018 with the levels used EEMUA-191, 3rd Edition, 2013, Appendix-3 Method-4 Flowchart.

Consequence Severity Levels (ADNOC Corporate Risk Matrix Version 1 June 2018)		Corresponding Consequence Severity Levels used in EEMUA-191, 3rd Edition, 2013, Appendix-3, Method-4
Level	Consequence Severity Description	Consequence Severity Description
Personnel		
6	Multiple public (more than 1)/ workers (more than 10) fatalities or permanent total disabilities	(Level 4) One of more deaths
5	Multiple worker fatalities (up-to 10)/ permanent total disabilities, or single public fatality	
4	Single worker fatality or Permanent total disability or serious injury to public	
3	Serious injuries or health effects	(Level 3) (Not used in EEMUA-191, App-3, Method-4) Team may escalate level-3 to level-4 in assessment)
2	Minor injuries or health effects (reversible effects- weeks to months)	(Level 2) Minor injury
1	Slight injuries or health effects (short term effects)	(Level 1) No personnel safety issues
Environment		
6	Disastrous effect	(Level 4) Serious catastrophic damage
5	Catastrophic effect	
4	Major effect	
3	Local effect	(Level 3) Release with in boundary fence with serious reportable consequence
2	Minor effect	(Level 2) Release with in boundary fence with minor implications but reportable
1	Slight effect	(Level 1) No serious environment issues
Financial		
6	Disastrous Impact (Direct Financial Impact >= USD 1B in a year) (Production Loss >= USD 1B in a year)	(Level 4) Damage … in excess of USD 1.5M

Consequence Severity Levels (ADNOC Corporate Risk Matrix Version 1 June 2018)		Corresponding Consequence Severity Levels used in EEMUA-191, 3rd Edition, 2013, Appendix-3, Method-4
5	Catastrophic Impact (Direct Financial Impact >= USD 100M, < 1B in a year) (Production Loss >= USD 100M, < 1B in a year)	
4	Major Impact (Direct Financial Impact >= USD 10M , < 100M in a year) (Production Loss >= USD 10M , < 100M in a year)	(Level 3) Damage … up to USD 1.5M
3	Serious Impact (Direct Financial Impact >= USD 1M, < 10M in a year) (Production Loss >= USD 1M, < 10M in a year)	(Level 2) Damage … up to USD 150K
2	Minor Impact (Direct Financial Impact >= USD 100K, < 1M in a year) (Production Loss >= USD 100K, < 1M in a year)	(Level 1) Damage … up to USD 15K
1	Notable Impact (Direct Financial Impact < USD 100K in a year) (Production Loss < USD 100K in a year)	(Level 0) Damage … less than USD 5K

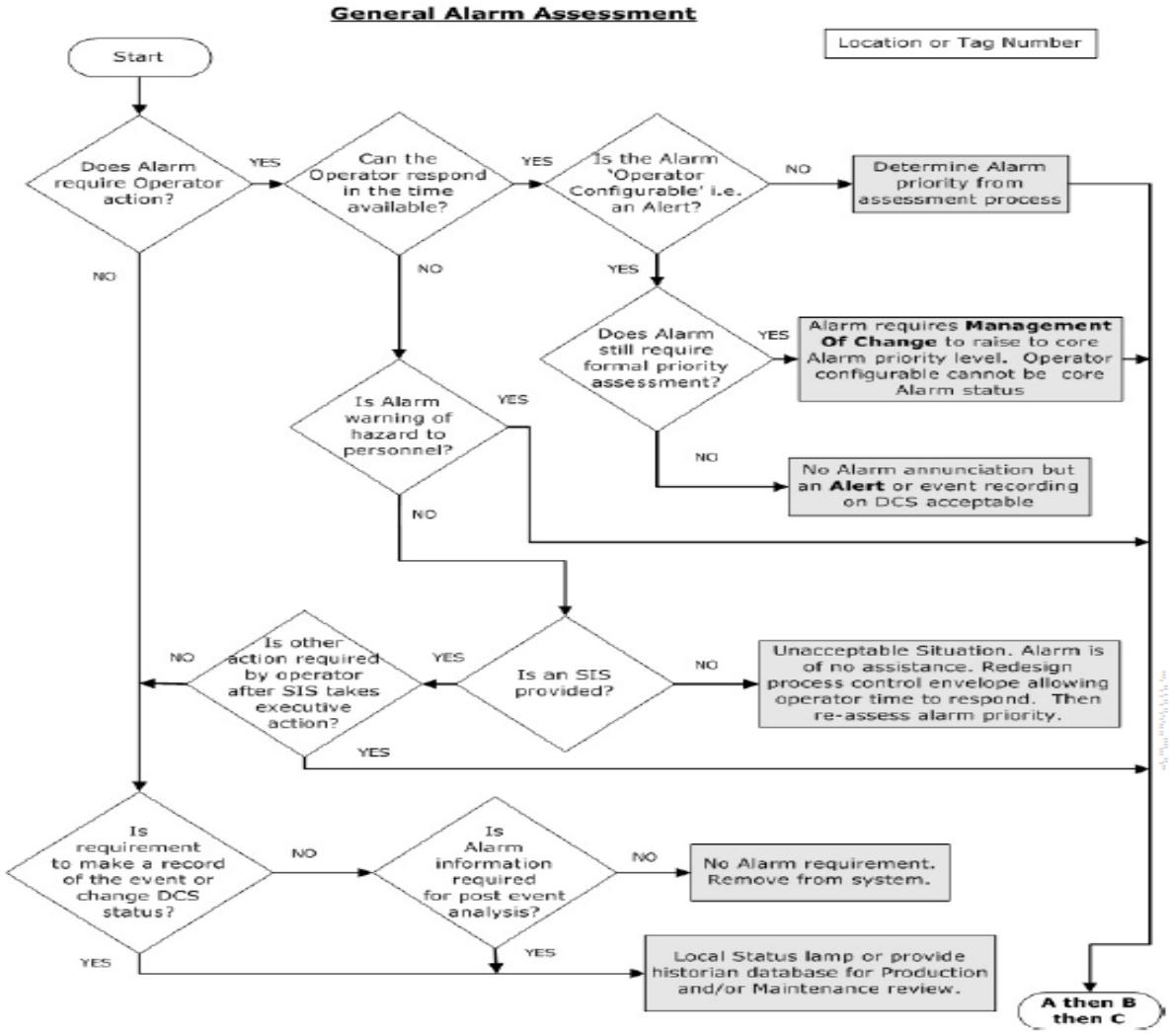
i. The outcome of the Alarm Prioritisation workshops shall be captured in a report which shall be prepared by the workshop Facilitator together with the CONTRACTOR/ CONSULTANT. The report shall capture all the relevant details inclusive of alarm tag-wise details covering the associated tag details from P&IDs, etc, associated consequence severities, alarm prioritisation flowchart assessment process results, etc.

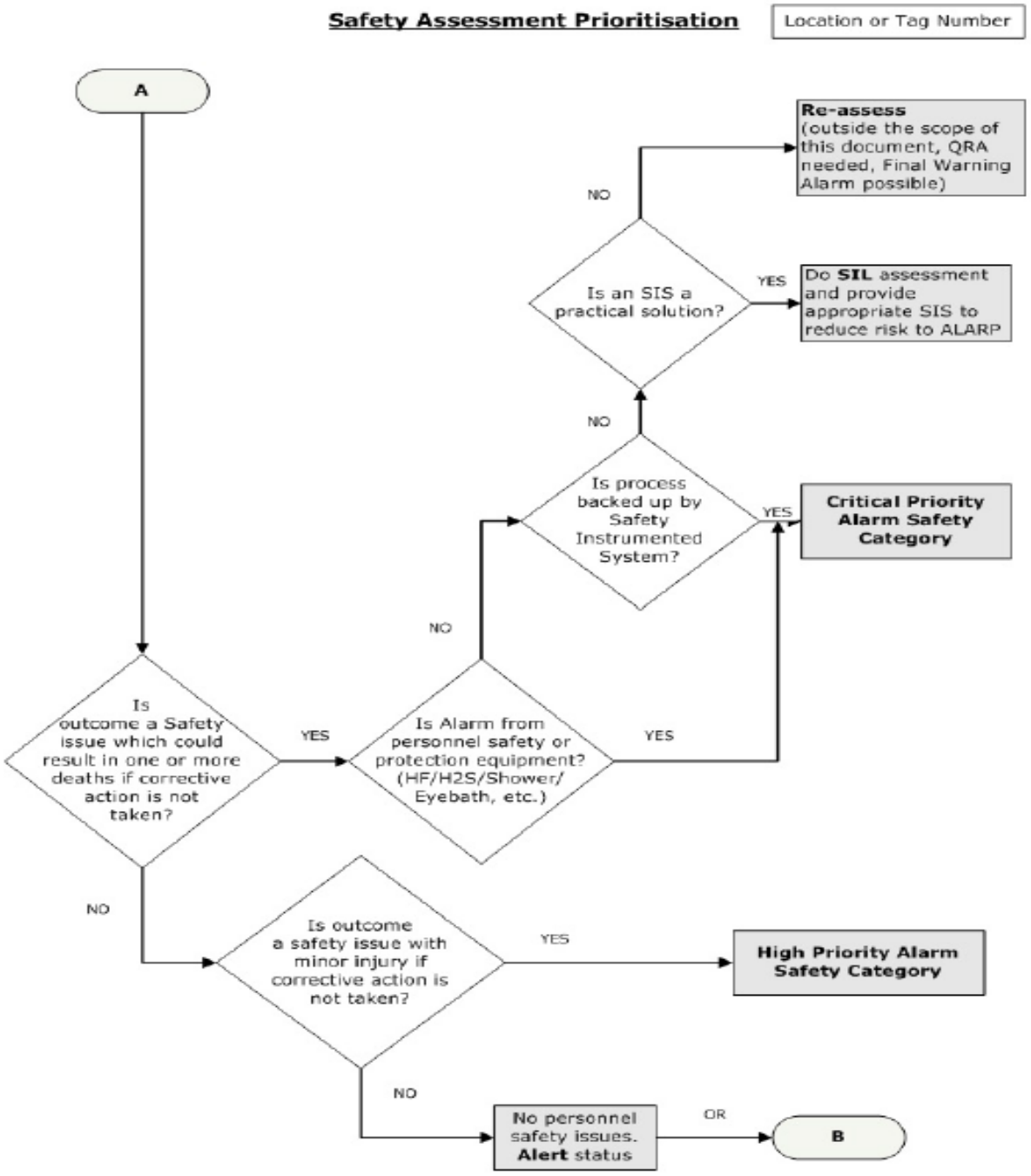
ii. For the cases involving Alarm Prioritisation Flowchart decision boxes “Is the process backed up by a Safety Instrumented System?” with the subsequent assessment as “Yes”, the workshop team shall analytically assess the required alarm priority. In these cases the assignment of Critical Priority to the alarm should take into consideration if the credit of risk reduction is taken in SIL/ EIL/ AIL assessment.

iii. Alarm Prioritization Flowchart given below is from “Method 4- General Alarm Assessment” in Sec. A3.5.3 of Appendix-3 in EEMUA-191, 3rd Edition, 2013

Figure-5: Alarm Prioritization Flowchart

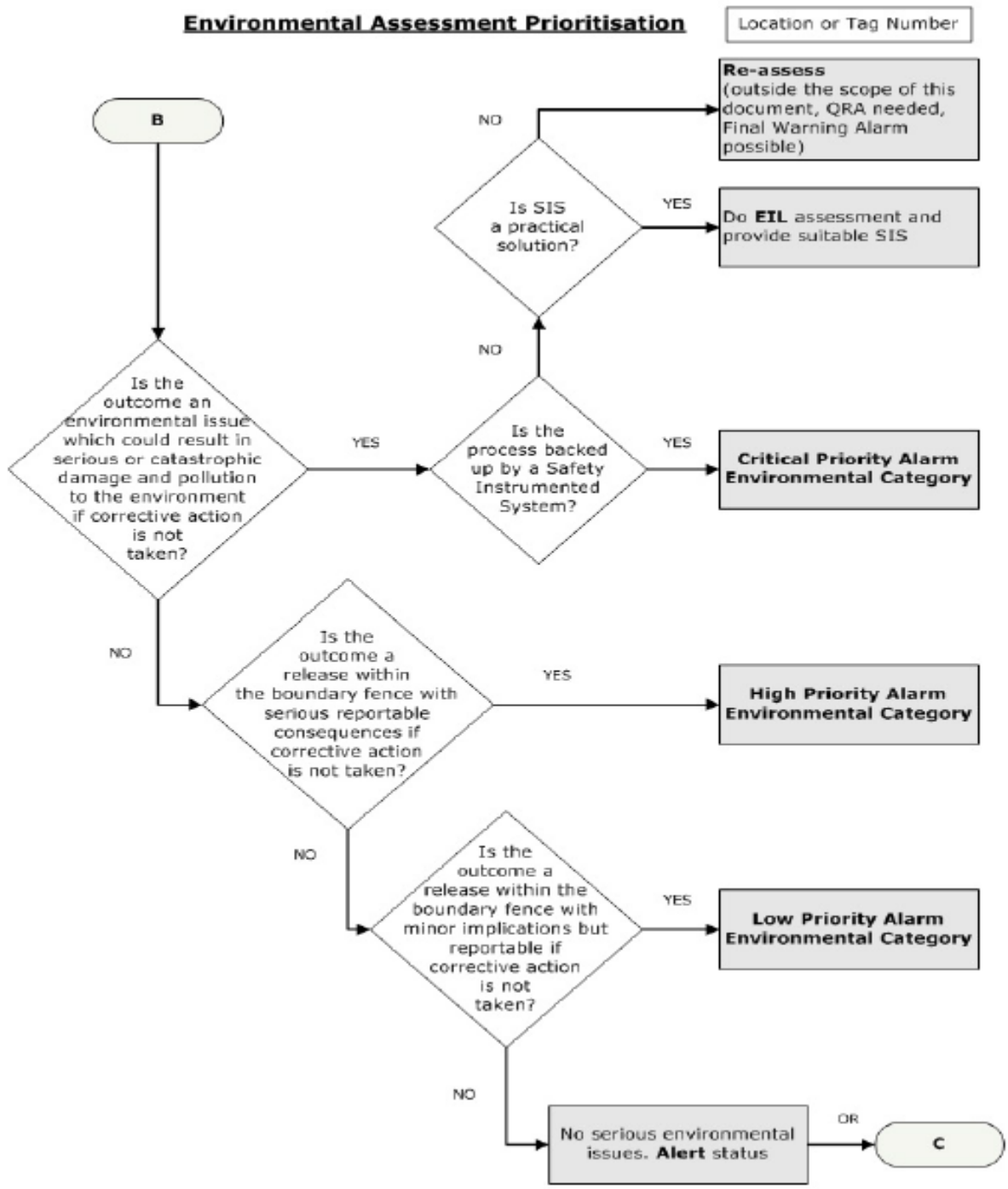
Alarm rationalization flowchart is from EEMUA-191, 3rd Edition, 2013, Appendix-3: Prioritisation methods, Section A3.5.3 Method 4- General Alarm Assessment.





Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

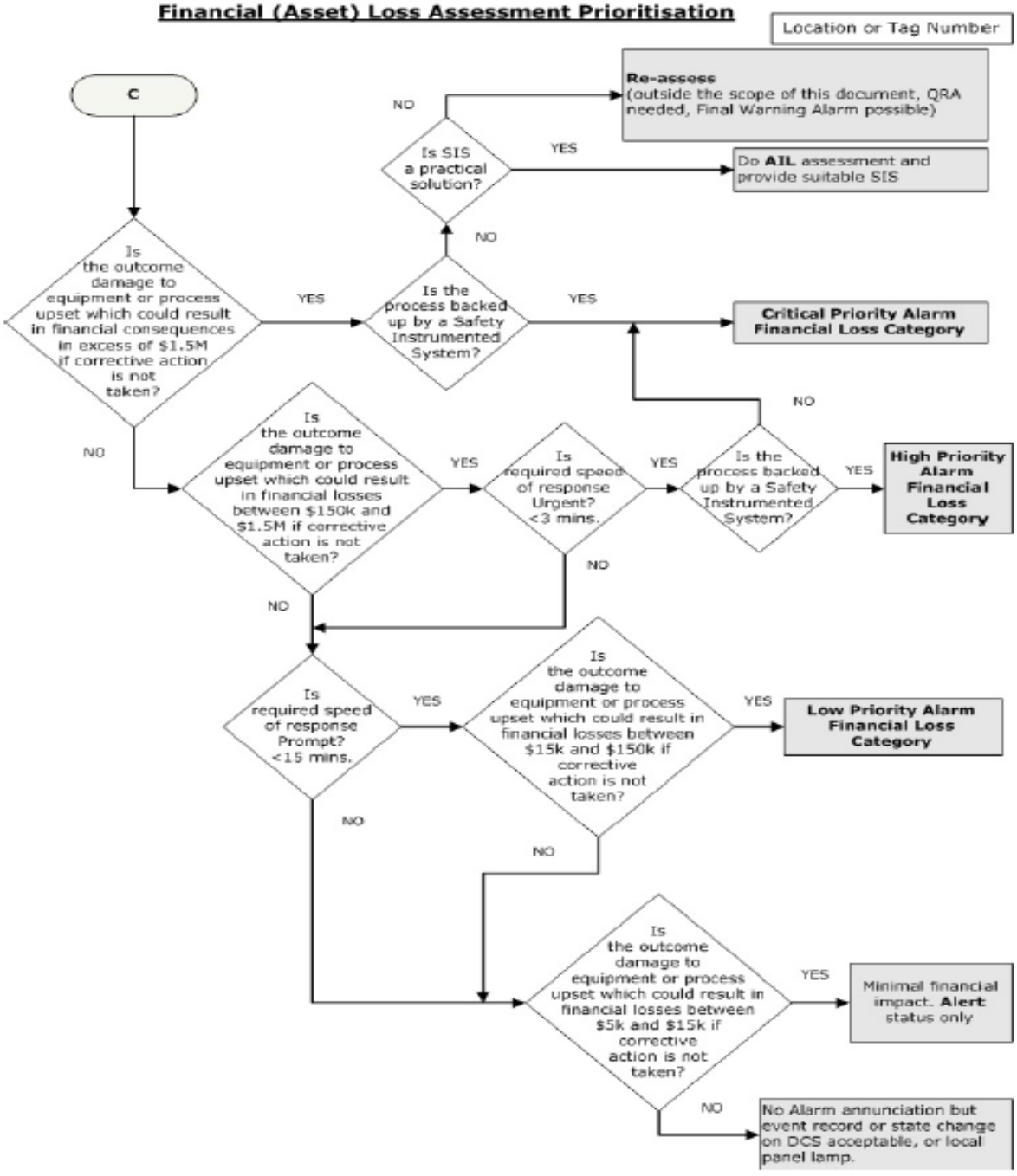
أدنوك البرية
ADNOC Onshore



Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Financial (Asset) Loss Assessment Prioritisation



Appendix-C : ADNOC Corporate Risk Matrix

Abu Dhabi Company for Onshore Petroleum Operations Ltd,شركة ابوظبي للعمليات البترولية البرية المحدودة
PO Box 270, Abu Dhabi, UAE ص ب 270 أبوظبي، الامارات العربية المتحدة
adnoc.ae

أدنوك البرية
ADNOC Onshore

Following is the ADNOC Corporate Risk Matrix Version 1 June 2018. Consequence severity levels as defined in ADNOC Corporate Risk Matrix Version 1 June 2018 are correlated with the levels used in Alarm Prioritisation flowchart in Appendix-II.

ADNOC Corporate Risk Matrix

ADNOC 25/06/18

Term	Rare	Unlikely	Possible	Likely	Very Likely	Almost Certain
ERM Criteria	Hasn't happened in the industry in the last 50 years	Could be incurred in the next 20-30 years	Could be incurred within a 5 -10 year time frame	Could be incurred within the 5 year Strategic Planning period	Could be incurred over the next 1-2 year budget period	Could be incurred once or more during the next year
HSE Frequency	$10^{-6} \leq - < 10^{-5}$	$10^{-5} \leq - < 10^{-4}$	$10^{-4} \leq - < 10^{-3}$	$10^{-3} \leq - < 10^{-2}$	$10^{-2} \leq - < 10^{-1}$	$10^{-1} \leq - < 1$
HSE Likelihood	Has not occurred in world-wide industry	Has occurred in world-wide industry but not in ADNOC	Has occurred at least once in the Group Company	Has occurred at least once in Group Company but not on the site	Has occurred more than once in Group Company or once on the site	Has occurred more than once on the site

Severity	Health & Safety	Environment	Reputation	*/**/***Financial: Direct Financial Impact (DFI)	*/**/***Financial: Production Loss (PL)	Legal	#	A	B	C	D	E	F
Disastrous	Multiple public (more than 1) / workers (more than 10) fatalities or permanent total disabilities	Disastrous effect (severe and permanent impacts, consistently exceeding limits)	Prolonged international impact and public attention. Effect will last for years and can spread internationally and affect other industry players	>=$1Billion in a year	>=$1Billion in a year	Inability to comply with laws, regulations or contracts resulting in substantially material losses. Disastrous regulatory sanction, prosecution or prolonged multiple litigations. Potential jail terms for executives	6	6A	6B	6C	6D	6E	6F
Catastrophic	Multiple worker fatalities (upto 10) / permanent total disabilities, or single public fatality	Catastrophic effect (serious impacts on many attributes of environment in larger area)	Serious international impact and public attention - extensive adverse coverage in the international media with potentially severe impact on licenses	>=$100 million - <$1 Billion in a year	>=$100 million - <$1 Billion in a year	Significantly constrained ability to comply with laws, regulations or contracts resulting in material financial losses. Very serious litigation, including class actions	5	5A	5B	5C	5D	5E	5F
Major	Single worker fatality / permanent total disability or serious injury to public	Major effect (negative impacts on surrounding environment and repeated non compliances)	Significant national impact and public concern - extensive adverse attention in the national media. Effect could last a few months and likely to spread to close industry partners	>=$10M - <$100M in a year	>=$10M - <$100M in a year	Major breach of law, contract or regulation. External investigation(s), significant regulatory sanction or major litigation	4	4A	4B	4C	4D	4E	4F
Serious	Serious injuries or health effects (permanent partial disability)	Local effect (reversible impacts but frequent non compliances)	Considerable impact - adverse attention in local media / local government / action groups	>=$1M - <$10M in a year	>=$1M - <$10M in a year	Serious breach of law, contract or regulation - moderate fines / litigation and / or requires reporting to regulator(s)	3	3A	3B	3C	3D	3E	3F
Minor	Minor injuries or health effects (reversible effects - weeks to months)	Minor effect (impacts limited organizational surroundings)	Limited impact - some local media / political attention. Effect will last a few days only	>=$100K - <$1M in a year	>=$100K - <$1M in a year	Minor breach of law, contract or regulation where mild regulatory sanction or minor litigation	2	2A	2B	2C	2D	2E	2F
Notable	Slight injuries or health effects (short term effects)	Slight effect (impacts within fence area)	Slight impact - no public concern	<$100K in a year	<$100K in a year	Low-level legal or business ethics issue; litigation or regulatory sanction unlikely	1	1A	1B	1C	1D	1E	1F

Risk Level	Minimum Required Action	Management Signoff Authority
HIGH / CATAGORY 1	Report immediately upon identification. Must be reduced as soon as possible to As Low As Reasonably Practicable (ALARP) / Management satisfied the costs to reduce the risk exceed the benefits of doing so. Include in Risk Register for tracking. Consider advanced risk methodologies for further investigation. Quantification of **Financial impact, Maximum Foreseeable Loss (MFL) and Risk Control Effectiveness (RCE) shall be calculated.	Signoff by Director or GC CEO
HIGH-MEDIUM / CATAGORY 2	Should be reduced as soon as possible to ALARP / Management satisfied the costs to reduce the risk exceed the benefits of doing so. Include in Risk Register for tracking. Consider advanced risk methodologies for further investigation. Quantification of **Financial impact, Maximum Foreseeable Loss (MFL) and Risk Control Effectiveness (RCE) shall be calculated.	Signoff by Unit Manager / SVP
MEDIUM / CATAGORY 3	Medium priority, monitor and improve effectiveness of current controls. Include in Risk Register for tracking. Quantification of **Financial impact, Maximum Foreseeable Loss (MFL) and Risk Control Effectiveness (RCE) should be calculated.	Signoff by Dept. Manager / VP
LOW / CATAGORY 4	Low priority, monitor and improve effectiveness of current controls.	Signoff by Line Manager

*Financial criteria for Operating Companies shall be specified by ADNOC Corporate / for upward reporting Operating Companies shall report against the ADNOC Corporate & Operating Company Financial Consequence levels.
**Financial Impact is the combination of Direct and Indirect costs.
*** For Investments, "Financial" refers to NPV impact.

Version 1. June 2018