ervia

European Commission

ERVIA CCS PRE-FEED STUDY

Communications & Control Philosophy - Cork

MDE1234-RPS-01-CX-RP-Z-00013
S3 P02
08-April 2022

rpsgroup.com

rps BECHTEL

Document status

Status	Revision	Purpose of document	Authored by	Reviewed by	Approved by	Review date
S3	P01	Issued for Ervia Review	SPJ	MJC	PD/CB	01/02/2022
S3	P01.1	Interim HAZOP Issue for Ervia review	SPJ	MJC	PD/CB	04/02/2022
S3	P02	Issued for Pre-FEED	NK	SPJ	PD/CB	08/04/2022

Approval for issue

CB	8 April 2022

© Copyright RPS Group Limited. All rights reserved.

The report has been prepared for the exclusive use of our client and unless otherwise agreed in writing by RPS Group Limited no other party may use, make use of, or rely on the contents of this report.

The report has been compiled using the resources agreed with the client and in accordance with the scope of work agreed with the client. No liability is accepted by RPS Group Limited for any use of this report, other than the purpose for which it was prepared.

RPS Group Limited accepts no responsibility for any documents or information supplied to RPS Group Limited by others and no legal liability arising from the use by others of opinions or data contained in this report. It is expressly stated that no independent verification of any documents or information supplied by others has been made.

RPS Group Limited has used reasonable skill, care, and diligence in compiling this report and no warranty is provided as to the report's accuracy.

No part of this report may be copied or reproduced, by any means, without the written permission of RPS Group Limited.

Prepared by:

RPS / Bechtel

Prepared for:

Ervia

Dublin | Cork | Galway | Sligo
rpsgroup.com

RPS Group Limited, registered in Ireland No. 91911
RPS Consulting Engineers Limited, registered in Ireland No. 161581
RPS Planning & Environment Limited, registered in Ireland No. 160191
RPS Engineering Services Limited, registered in Ireland No. 99795
The Registered office of each of the above companies is West Pier Business Campus, Dun Laoghaire, Co. Dublin, A96 N6T7

Contents

Holds v
Glossary vi
References ix

1 INTRODUCTION 1
1.1 Project Background 1
1.2 Scope 1
1.3 Control System Implementation 1

2 APPLICABLE CODES, STANDARDS, REGULATIONS 2
2.1 General 2
2.2 International Codes and Standards 2

3 GENERAL DESIGN CRITERIA 3
3.1 Environmental Data 3
3.2 Units of Measurement 3
3.3 EMC 3
3.4 ICSS and Process Control Domain Networks Levels 3
3.4.1 Level 0 – Field Instrumentation 3
3.4.2 Level 1 – Control Local Area Network 3
3.4.3 Level 2 – Process Control Network 4
3.4.4 Level 3 – Plant Information Management System 4
3.4.5 Level 3.5 – De-militarised Zone (DMZ) 4
3.4.6 Level 4 - Management Information System (MIS) / Business LAN 4
3.5 Quality Assurance 5

4 CONTROL SYSTEM REQUIREMENTS 6
4.1 Introduction 6
4.2 Operational Aspects 7
4.3 Plant Safety 8
4.4 Interface & Package Controls Philosophy 8
4.5 Electrical Interfaces 9
4.6 Communication Protocols 10
4.7 Vibration Monitoring 10
4.8 Custody Metering Systems 10
4.9 Pipeline Leak Detection System 11
4.10 In Field RTUs 11
4.11 Berth, Mooring, Loading/Unloading and Ship to Shore Systems 12

5 COMMON REQUIREMENTS FOR SYSTEMS 13
5.1 Power Supply Systems 13
5.2 Fibre Optic Network 13
5.3 Availability 13
5.4 System Segregation 14
5.5 Sparing and Performance Requirements 14
5.6 Central Control Room (CCR) and Jetty Control Room (JCR) 14
5.7 Analyser House 15
5.8 Systems Hardware, Cabinets and Network Cabling 15
5.9 Heating, Ventilation and Air Conditioning (HVAC) Requirements 15

6 DISTRIBUTED CONTROL SYSTEM (DCS) 17
6.1 General 17
6.2 Human Machine Interface 17
6.3 DCS Hardware 18
6.4 HART DATA 18

6.5 Software 18
6.6 Instrument Asset Management System (IAMS) 18
6.7 Time Synchronisation 19
6.8 DCS Communications 19
6.9 Central Processing Facility (CPF) Networks Architecture 19
6.10 Alarm Management and Sequence of Event (SOE) 19
6.11 DCS Anywhere 20
6.12 DCS Large Screen Displays 20

7 SAFETY INSTRUMENTED SYSTEM (SIS) 21
7.1 General 21
7.2 Measurement Devices 22
7.3 Final Elements 22
7.4 Partial Stroke Testing (PST) 22
7.5 Reset 22
7.6 Sequence of Event (SOE) and First Out 23
7.7 Maintenance Override Switch (MOS) 23
7.8 Matrix Panel, Emergency Shut Down 23

8 FIRE AND GAS DETECTION SYSTEMS (FGS) 24
8.1 General 24
8.2 Fire and Gas Detectors 24
8.3 Fire and Gas Detection in Buildings / RTU 24
8.4 Fire Fighting Actions 24

9 SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) 25

10 ICSS INTERFACE AND COMMUNICATION SYSTEMS 27
10.1 General 27
10.2 Cyber Security 27

Holds

HOLDS	Description	Responsibility
N/A		

Glossary

Term	Definition
ANSI	American National Standard Institute
CCR	Central Control Room
CCS	Carbon Capture and Storage
CCTV	Closed Circuit Television
CPF	Central Processing Facility
CPU	Central Processing Unit
EDG	Emergency Diesel Generator
EMC	Electromagnetic Compatibility
EPC	Engineering Procurement Construction
EWS	Engineering Workstation
FEED	Front End Engineering Design
GPS	Global Positioning System
HVAC	Heating Ventilation and Air Conditioning
JCR	Jetty Control Room
C&E	Cause & Effect
DCS	Distributed Control System
DMZ	De militarised Zone
EWS	Engineering Workstation
FGS	Fire and Gas Detection System
FAT	Factory Acceptance Test
FO	Fibre Optic Cable
GPS	Global Positioning System
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
HSSD	High Sensitivity Smoke Detection

Term	Definition
IAMS	Instrument Asset Management System
ICSS	Integrated Control and Safety System
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMCS	Intelligent Motor Control System
I/O	Inputs/Outputs
ISA	International Society of Automation
ISO	International Organisation for Standards
IT	Information Technology
KVM	Keyboard Video Monitor
LAN	Local Area Network
MAC	Main Automation Contractor
MCMS	Machine Conditioning Monitoring System
MIS	Management Information System
MOS	Maintenance Override Switch
NC	Normally Closed
NTP	Network Time Protocol
OLE	Object Link Embedded
OPC	OLE for Process Control
OWS	Operator Workstation
PAGA	Public Address and General Alarm
PC	Personal Computer
PCN	Process Control Network
PST	Partial Stroke Testing
PLC	Programmable Logic Controller

Term	Definition
RIO	Remote Inputs/Outputs
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIF	Safety Instrumented Function
SIGTTO	Society of International Gas Tanker and Terminal Operators
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SOE	Sequence of Event
SRS	Safety Requirement Specifications
TCP/IP	Transmission Control Protocol / Internet Protocol
UCP	Unit Control Panel
UPS	Uninterrupted Power Supply
VDU	Visual Display Unit
VSAT	Very Small Aperture Terminal

References

1. Study Basis, MDE1234-RPS-01-CX-RP-Z-0001.
2. Process Safety Design Basis, Cork MDE1234-RPS-01-CX-RP-Z-0011
3. Control System Architecture Drawings, MDE1234-BEC-03-CX-DR-E-0001
4. Operations and Maintenance, MDE1234-RPS-01-CX-RP-Z-0010

International Codes and Standard:

Unless specified otherwise, the latest editions of the following Codes, Standards and References shall be used.

5. IEC 61000 - Electromagnetic Compatibility – All Parts
6. IEC 61131 - Programmable Controllers-General Information – All Parts
7. IEC 61508 - Functional Safety of Electrical / Electronic /Programmable Electronic Safety-Related Systems-All Parts
8. IEC 61511 - Functional Safety – Safety Instrumented Systems for the Process Industry Sector – All parts
9. IEC 62443 - Industrial communication networks - Network and system security-All Parts
10. IEC 62439 - Industrial communication networks - High availability automation networks
11. IEC 62264 - Enterprise Control System Integration
12. ANSI/ISA Standard- 18.2 - Management of Alarm Systems for The Process Industries
13. ISO 11064 - Ergonomic Design of Control Centers-All Parts
14. ISO 9001 - Quality Management Systems
15. EEMUA 191 - Alarm Systems - A Guide to Design, Management and Procurement (Edition 3)
16. EEMUA 138 - Design and Installation of On-Line Analyzer Systems
17. NFPA 72 - National Fire Alarm and Signaling Code

1 INTRODUCTION

1.1 Project Background

Ervia is assessing how Carbon Capture and Storage (CCS), located close to large-scale CO_2 emitters can play a role in reducing Ireland's CO_2 emissions. A technical feasibility study on the potential for large-scale CCS in Ireland was completed by Ervia in 2020.

The general location of Aghada Power Station in County Cork was selected as a potential site for a Central Processing Facility (CPF) for liquefaction, storage, and export of CO_2 overseas via a new marine jetty. The CPF will cater for CO_2 captured at 3 emitter locations (Whitegate Power Station, Irving Oil Whitegate Refinery and Aghada CCGT). A new CO_2 gas pipeline gathering network will transport CO_2 from the emitters to the CPF.

Ervia has appointed RPS / Bechtel to carry out a Pre-FEED study that involves a detailed assessment of the key CPF, pipeline and storage infrastructure necessary to condition, compress, transport and store liquid CO_2 at Cork harbour for subsequent loading onto ships for export. (Note: The scope of this project does not include the carbon capture facilities at each emitter).

Additionally, the new marine jetty in Cork will also be used for import of liquid CO_2. This scenario considers the regasification of liquid CO_2 at Cork for transport via pipeline to the Inch terminal which is the link to indigenous offshore permanent storage at the depleted Kinsale Head Gas Field.

1.2 Scope

This philosophy defines the basic requirements for ICSS and SCADA of the project, including all of the CO_2 gas gathering network from the Whitegate Power Station, Irving Oil Whitegate Refinery and Aghada CCGT site.

This Philosophy is developed as a Pre-FEED standard document and shall be the basis of the Front-End Engineering Design (FEED). This shall be further developed in detailed design in compliance with this philosophy.

This philosophy defines the basic requirements for automation levels 1, 2 and 3 as per IEC 62443, being the field instrumentation layer, the production control system layer and plant information management (Manufacturing Execution Systems) layer. IEC 62443 layer 4, enterprise resource planning, is outside the scope of this document.

Field instrumentation shall be described in a separate "General Instrumentation Specification" which should be prepared during FEED/EPC phase.

All locations shall be interconnected by means of Fibre Optic (FO) cabling. Control equipment to which this philosophy is applicable shall be installed at the locations listed below.

- Central Processing Facilities (CPF);
- Jetty Control Room (JCR);
- Valve Installation;
- Pigging Installations at Whitegate, Aghada and Inch terminal; and
- Any new locations as required per the applicable project(s).

1.3 Control System Implementation

The Main Automation Contractor (MAC) will be responsible for the supply and installation supervision of the DCS, SIS, and FGS system (Part of ICSS) cabinets and system cables. Furthermore, the MAC is responsible for the integration of sub systems connected to the DCS e.g., IMCS, MCMS, etc.

Control configuration of the systems will be based on automation deliverables for DCS, SIS and FGS. These documents shall be prepared during detailed design based on conceptual documents developed during FEED.

2 APPLICABLE CODES, STANDARDS, REGULATIONS

2.1 General

The design of the Automation System and associated facilities shall comply with all national and local laws and international codes, standards, and regulations.

In the event of conflict or deviation from requirements stipulated in this design basis and other applicable documents, the order of precedence shall be as defined in Study Basis, MDE1234-RPS-01-CX-RP-Z-0001

Notwithstanding the order of precedence, the owner's interpretation shall be final. The manufacturer/supplier shall be responsible for informing the owner of any conflicts, deviations from or exceptions to the referenced specifications, codes, and standards.

2.2 International Codes and Standards

Unless specified otherwise, the latest editions of the Codes, Standards and References shall be used. Referenced standards may be replaced by equivalent standards that are internationally or otherwise recognised provided they meet or exceed the requirements of the reference standard.

Standard	Description
IEC 61000	Electromagnetic Compatibility – All Parts
IEC 61131	Programmable Controllers-General Information – All Parts
IEC 61508	Functional Safety of Electrical / Electronic /Programmable Electronic Safety-Related Systems-All Parts
IEC 61511	Functional Safety – Safety Instrumented Systems for the Process Industry Sector – All parts
IEC 62443	Industrial communication networks - Network and system security-All Parts
IEC 62439	Industrial communication networks - High availability automation networks
IEC 62264	Enterprise Control System Integration
ANSI/ISA Standard-18.2	Management of Alarm Systems for The Process Industries
ISO 11064	Ergonomic Design of Control Centers-All Parts
ISO 9001	Quality Management Systems
EEMUA 191	Alarm Systems - A Guide to Design, Management and Procurement
EEMUA 138	Design and Installation of On-Line Analyzer Systems
NFPA 72	National Fire Alarm and Signaling Code

3 GENERAL DESIGN CRITERIA

3.1 Environmental Data

Service conditions for all automation systems, indoor and outdoor, shall be as described in Study Basis.

Telecommunication cabinets shall be specified for in indoor and outdoor environment and shall provide appropriate ingress protection.

Telecommunication cabinet IP requirements shall be described in the Telecommunication Design Philosophy which will developed during FEED.

All suppliers shall specify the max/min tolerance limits for temperature, humidity, and other environmental parameters for normal as well as extreme conditions that can occur due to prolonged failure of heating, ventilation and air conditioning.

3.2 Units of Measurement

Units of measurement are defined in Pre-FEED Study Basis MDE1234-RPS-01-CX-RP-Z-0001.

3.3 EMC

All systems, components, installations, cabinets, cabling and earthing shall comply with IEC 61000, Electromagnetic Compatibility (EMC).

3.4 ICSS and Process Control Domain Networks Levels

The ICSS Control and automation systems shall be designed to integrate multiple layers of hierarchy as per IEC 62264 - international standard for enterprise-control system integration.

3.4.1 Level 0 – Field Instrumentation

Level 0 is for measurement and control device/ instrumentation. The base layer consists of a wide variety of field I/O including sensors and actuators involved in the basic process measurement as well as safety devices.

3.4.2 Level 1 – Control Local Area Network

Level 1 is for ICSS basic control/ safety functions, process measurement and device diagnostic data. The level contains the controller systems that perform DCS, SIS, monitoring and data acquisition required to maintain steady, efficient, and safe operation. The Controller Network segment is comprised of a Distributed Controller Network segment and Safety Controller Network segment.

- The Distributed Controller Network connects process measurement and control devices/ equipment to the process controllers and allows interaction between them so that process control functions can be distributed.
- The Safety Controller Network connects safety related devices/ equipment to the safety controllers (e.g., SIS, FGS) and allows interaction, e.g., inter-trips, between safety related systems so that safety functions can be distributed. Safety Bus (SIL 3 rated bus for safety critical signals) shall be implemented for safety function related communications between SIS controller/ nodes.

Vendor supplied third party package unit PLCs shall also connect to the Controller Systems at this level through appropriate firewalls and network switches.

3.4.3 Level 2 – Process Control Network

Level 2 is identified as Process Control Network (PCN) and contains the supervisory control and includes the functions involved in monitoring and controlling the physical process. Typical functions include:

- Operator Workstations (OWS);
- Engineering Workstations (EWS);
- Process History collection;
- Advanced Process Control; and
- Secure connectivity to Level 3 through Firewall.

3.4.4 Level 3 – Plant Information Management System

A fault tolerant Plant Information Management System Server comprises a Real Time Database and long-term data archive, with which other software packages can readily exchange data using standard techniques such as Open Database Connectivity, Object Link Embedding (OLE) or Software Development Kit.

The Plant Information Management System uses a dedicated OPC interface to collect real time ICSS data that can be made available on the business Local Area Network (LAN). Firewalls shall ensure the security of data flowing between these domains.

The Plant Information Management System may also combine with a web server, supporting XML and allow wider dissemination of secure read-only plant data, without the need for dedicated workstations or client software.

The applications and functions that exist at this level typically include the following: -

- Instrument Asset Management System;
- Alarm Management System;
- Machine Condition and Monitoring System;
- Domain controller, Anti-Virus Server, Patch server, backup server, and remote access server;
- GPS Time Server (NTP); and
- Tank Gauging System.

3.4.5 Level 3.5 – De-militarised Zone (DMZ)

The DMZ provides a buffer zone where services and data can be shared securely between the Process Control Environment (i.e., Level 0, 1, 2, 3) and the Enterprise Network, Level 4. Firewalls are implemented to manage the traffic flow between the Process Control Environment networks and the Enterprise Networks to establish the DMZ's.

Cyber security strategies will be implemented in the project which includes uplink to Client provided firewall for application and functions described above. IP addressing and switch configuration is done by the owner. Cyber security requirements to be agreed during FEED/EPC phase with the owner.

3.4.6 Level 4 - Management Information System (MIS) / Business LAN

The fourth layer is the Enterprise Network for site business planning and logistics, owner services, remote access services, corporate application and users and is where the functions and systems that need standard access to services provided by the business network reside. The basic business administration tasks are performed here and rely on standard IT services.

The MIS will be supplied with all of the necessary software packages including any project specific configuration to perform the following functions:

- Emergency guidance checklist and messages;
- Decision making capabilities for unit / plant shutdowns;

- Shift oriented reporting system;
- Production accounting system;
- Unit yield auditing;
- Heat and mass balance reconciliation application at unit and area levels;
- Production/dispatch scheduling;
- Performance monitoring and analysis; and
- Process diagnostics.

Reporting should include daily, weekly, monthly and long period historical reports of production / consumption of feed stocks as per requirement.

The services, systems, and applications at this level are also directly managed and operated by the owner IT organisation. The Level 4 Enterprise Network shall be provided by the owner's IT organisation.

3.5 Quality Assurance

All suppliers of equipment shall operate a Quality Assurance system. This system shall be based on the principles of ISO 9001 or equivalent and may be subject to periodic auditing and monitoring.

4 CONTROL SYSTEM REQUIREMENTS

4.1 Introduction

An Integrated Control and Safety System (ICSS) shall be provided for the facilities. The ICSS shall consist of:

- Distributed Control System (DCS);
- Safety Instrumented System (SIS); and
- Fire and Gas Detection System (FGS).

It will also include the necessary interfaces to other systems and information management systems.

For interfacing with the operators, a continuously manned Central Control Room (CCR) shall be used at CPF, containing the operator consoles. The CCR will have an adjacent equipment room which will contain all back-bone related equipment of the ICSS, as well as all system and maintenance engineering related equipment.

Facilities for monitoring and control of the plant shall be based on the single operator window concept and shall as much as possible be implemented in the DCS. The DCS shall be employed to its full functional capability.

ICSS screens and panels pertinent to jetty operations (e.g., berthing, mooring and loading /unloading) will be provided in the Jetty Control Room (JCR), however control of loading/unloading can be transferred to the CCR in case of a failure of control from JCR or an emergency situation at the jetty.

The various systems that interface to the field instrumentation and other equipment of the plant will be installed in the CCR, strategically located within the plant. Other locations where equipment may be installed should be defined during detail engineering for value optimisation in the project.

The requirements of field instrumentation, i.e., General Instrument Specifications shall be developed in FEED.

Field instruments shall be loop powered from the automation systems as much as possible. Hazardous area for this project is Unclassified. However, Ex-d or Ex-e will be the preferred solution in order to standardise wiring and cabling methodologies in the project.

All analogue signal-loops located in a different lightning zone to the control panels shall be equipped with voltage surge protection utilising rail mounted, pluggable surge protection terminals which comply with IEC 61643-21.

The ERVIA field installations are controlled, monitored, and protected by the following major systems:

- Distributed Control System (DCS, part of ICSS);
- Safety Instrumented System (SIS, part of ICSS);
- Fire and Gas Detection System (FGS, part of ICSS);
- Machine Conditioning Monitoring System (MCMS);
- Intelligent Motor Control System (IMCS);
- Programmable Logic Controller (PLC) based control systems for Package Units;
- Anti-Surge Control System part of package;
- Remote Telemetry Units (RTU);
- Automatic Tank Gauging;
- Custody Metering Systems; and
- Berth, Mooring, Loading/unloading and Ship to Shore Communication Systems.

The ICSS will be an integrated system where the DCS provides the primary control and monitoring of the plant. SIL-3 certified Safety Instrumented Systems (SIS) will be integrated into the control system architecture using direct communication over the control bus. Safety systems that require serial link communication to a specific DCS controller are not acceptable.

The FGS in design will be identical to the SIS and hence the FGS hardware shall be SIL-3 compliant. However, the overall FGS (from sensing detector to final element) will not require SIL determination (and hence will also not be SIL verified).

The control bus or data highway of the ICSS shall be a redundant Ethernet based deterministic and fault tolerant network with fibre-optic (FO) network infrastructure between CCR, JCR and various control buildings i,e Valve Installation / Pigging Installations. Various network parts shall be connected by means of L2 network switches.

As part of the network configuration, a dedicated network (or network function) that allows for distribution of non-process control related information, such as system configurations, asset management information, system backups, etc., shall be provided. Failure of such network or network function shall not interrupt operation of the redundant control bus.

Remote Input / Output units (RIO), for DCS, SIS and FGS, should be used where this is economically advantageous.

The Valve Installation and each pigging installation will have an RTU with a local panel display and a combined FGS.

Each sub-system of the DCS will be a standalone, redundant programmable system with independent I/O modules. All I/O is expected to be wired into the CCR equipment room at CPF, JCR equipment room at Jetty, valve installation and pigging installations. These equipment rooms shall be connected via redundant fibre optic network. The platform will be easily expandable to allow for future expansion. To accommodate future expansion 20% spare I/O capacity shall be allowed for. Controller processing and memory capacity shall also be installed to allow for this possible future expansion.

ICSS consists of the following components:

- A highly scalable, field proven, state of the art and SIL certified PLC system;
- Redundant power supplies;
- Redundant controllers (CPU);
- I/O cards (redundant I/O for critical signals such as SIS Trip and DCS Closed Control Loops etc.);
- Redundant interfaces to SCADA, unit control systems, gas measurement system, gas quality; systems, sub systems and remote I/O;
- Process interface with overvoltage protection and interposing relays were necessary; and
- HMI hardware, including redundant servers, operator workstations and engineering Workstation.

All control cabinets and server racks shall be in the equipment rooms of the CCR and JCR control buildings, only HMI's will be installed in the CCR and JCR control rooms. KVM extenders shall be used to connect screens, keyboard and mouse to the workstations and servers located in server racks.

4.2 Operational Aspects

All field wide process and utility units and related facilities shall be monitored and controlled from the CCR and jetty equipment from the JCR respectively. The CCR comprises operator consoles with related equipment, Closed Circuit Television (CCTV) monitors, printers, telecommunications equipment, Personal Computers (PC), F&G detection overview screens, and large screen displays.

The panel operators shall have access to all relevant process variables via the ICSS. The operators carry out all actions at OWS via the ICSS Human Machine Interface (HMI) [Visual Display Units (VDU's) and keyboards]. It shall be possible from each OWS, to retrieve any process information of the applicable part of the plant. The ICSS provides all control and computing functions needed for operation of the plant in a stable, efficient, and reliable manner.

All displays shall be made available to all operational staff controlling process units to observe plant conditions. The panel operator responsible for operating a certain process unit will be able to manipulate process variables

in that unit. Graphical displays not within the panel operator's responsibility will be available as view only. FGS information and graphics shall be accessible from OWS.

The ICSS shall include facilities for trending and deviation indications, to keep the operator aware of non-steady process conditions and to give him a possibility to observe the development of imminent disturbances.

Start-up, operation, and safe Start / Stop shall be from the CCR to reduce operator presence in the field. The anticipated fully manned or fully unmanned requirements for some of the plant operations are as follows: -

- Jetty Control Operation from JCR for berthing, mooring and loading/unloading are manned.
- Local Control Operation from local skid control panels are unmanned.
- Pipeline Control Operation of RTU, SIS, FGS and UCP are intermittently manned at Valve installation and pigging installations.
- CCR Control Operation of ICSS, leak detection, compressor control is manned.
- Operation Management Center in CCR for CPF and associated pipelines. This has ICSS supervisory consoles and are fully manned for complete facilities monitoring; and
- Incident Response Management Centre in Ervia Administration building. This has secure telecommunication systems and can be used in case of an emergency.

4.3 Plant Safety

A separate, dedicated Safety Instrumented System (SIS), independent from the DCS, shall be provided to mitigate the following consequences:

- Hazards to people;
- Economic loss (financial impact, asset damage, production loss);
- Impact on the environment;
- Loss of reputation; and
- Regulatory impact.

During FEED /detailed design, critical SIL assessment shall be made as per IEC 61511 whether the severity of the consequences of a failure requires a SIF to be implemented in SIS or that needs to be facilitated in the DCS. Process safety time assessment shall be part of the SIL assessment. The project shall comply with IEC 61511 and provide all the necessary supportive documentation as specified in IEC 61511 (e.g., Safety Requirements Specification).

Where SIFs are implemented in the SIS (or in any other 3rd party supplied system), this shall comply with IEC 61508.

The functioning of the safety related systems and instrumentation shall be fully independent of the control systems and control instrumentation. The SIS shall be designed to be fail safe.

Where SIFs are implemented in the SIS, the sensors (input), logic solver (SIS) and final control elements (outputs) shall be independent from process control field sensors, DCS Input / Output (I/O) and logic, and process control final elements.

4.4 Interface & Package Controls Philosophy

In general, controls and safeguarding shall be integrated into the ICSS. The package units' controls will be integrated into the ICSS to the maximum extent. Main drivers for this philosophy are unification and integration of the operator interface, standardisation of control implementation, maximisation of the HART signal implementation into IAMS, simplification of plant maintenance and optimisation of system lifecycle costs.

Where the control of package equipment is achieved by means of systems provided by the package supplier, these systems shall be integrated into the plant's ICSS such that the operator in the CPF has full monitoring and control capability over the package, including remote start up, continuous operation, safe process stops, and emergency shut down. Interface to the DCS shall be made by means of a serial link(s), protocol and redundancy requirements as specified in this document.

Where package unit PLCs are used, make and type shall be identical (e.g., Rockwell Automation – Allen Bradley). Configuration and programming of the PLCs and controllers shall also be similar.

Local control panels for packages shall be avoided and shall only be included if essential from an operational point of view and / or are required by the supplier e.g., for start-up or essential local instrumentation purposes.

The package types and its integration with the ICSS are as follows:

- **Packages Type 1**: The package is equipped with its instruments, but without junction boxes, cables, and cable trays. This package type is restricted to a unit with only a few instruments and shall be controlled / protected by the Plant ICSS and protected by the Plant SIS and FGS. Signals shall be wired by others to junction boxes outside of the package battery limits. Cables between instruments and related junction boxes are not part of the scope of the package supply except interconnecting cables between primary element (e.g., temperature element) and related transducer if field mounted (e.g., Temperature Transmitter);
- **Packages Type 2:** The package is equipped with its instruments, wired by means of appropriate cables and cable trays. The cables are connected to the junction boxes located at the skid battery limits. All the controls shall be implemented in the ICSS. The cables between Junction Boxes and CPF ICSS cabinets, excluded from the Package supply, will be in the EPC scope of supply; and
- **Packages Type 3**: This is a standalone design. The package is equipped with its instruments, wired by means of appropriate cables and cable trays. Cables are connected to the junction boxes located at the skid battery limits. Controls are in UCP(s) by Package supplier.

The UCP shall include separate control and safety controllers, which will be interfaced with plant ICSS. This configuration requires owner approval and shall be fully compliant with this document and project specifications.

Where required in the package, vibration monitoring shall be included by supplier in UCP. Package supplier shall provide the solution to integrate smart field instrument HART data into IAMS.

Field instrumentation shall be 4-20 mA/HART and the control panel shall include HART multiplexers to allow integration of the transmitters/valves within the package into the plant wide IAMS system.

Serial links shall be provided between the package PLC and the DCS per Section 4.6. PLC and DCS shall be interconnected using an Ethernet connection for time synchronisation using Network Time Protocol (NTP), or via the MODBUS TCP/IP link.

Where SIFs are part of the package unit control system scope, these SIFs shall be implemented in a dedicated SIS to be supplied by the package unit supplier. SIF related signals between package unit supplier SIS and main plant SIS shall be hard wired.

The Anti-Surge Control shall be supplied by Compressor supplier and should be incorporated into the Package supplier UCP. Transmitters and control valves specifications and performance requirements when used for Anti-Surge Control shall follow Compressor supplier's recommendations.

FGS detection for packages shall be integrated into the plant's main systems, and not be part of supplier's system, even when a UCP / PLC would be in his scope, any deviation requires owner approval.

4.5 Electrical Interfaces

The interface between the DCS and electrical systems shall be based on serial communication. DCS Controller cabinets located in the CCR will communicate with the Intelligent Motor Control Systems (IMCS) in the Switch Gear room. The Switch Gear room will have 400V power distribution normal and emergency panels fed from MCC. Interposing Relay Cabinets shall be located at main plant Sub Station & one switchgear room near the jetty area to interconnect SIS trip signals to the motor control centre's switchgear. Relays shall also be provided

for those status and trip signals that need to be hardwired to / from the SIS. All relays shall be by 24V DC powered.

An Intelligent Motor Control System (IMCS) shall be provided for each LV motor or consumer. MV equipment integration into DCS shall be redundant.

Each individual UPS System shall have a common alarm hardwired to the DCS. Each field located heat tracing distribution board shall have a common alarm wired to the DCS. (Note: Heat tracing locations and load requirements are to be determined during FEED / EPC.)

4.6 Communication Protocols

Proprietary protocols shall not be used, unless within the systems from the same manufacturer. Serial links shall be implemented with a proven and open industry standard protocol e.g., Ethernet, Modbus RTU, Modbus TCP, Profibus DP, OPC UA. Modbus TCP is the Project preferred protocol.

Serial links may be non-redundant, if used for monitoring only. When serial links are used for control, these shall be redundant. All serial communication shall be equipped with link health monitoring, and, in case of link outage, an alarm shall be generated in the DCS.

Functionality of each serial link shall be fully tested with the project hardware and software during a Factory Acceptance Test (FAT) prior to delivery.

4.7 Vibration Monitoring

Rotating equipment shall be protected and monitored by MCMS. The MCMS will monitor rotating equipment with detectors for XY radial vibrations, axial displacements, speed meters, accelerometers, key-phasers, rod drop and bearing temperature devices, all in line with API 670. The rotating equipment shall be monitored to initiate trip for unsafe conditions, and data for on-line analysis and fault trends of machine condition.

Rack mounted and distributed hardware should be used for better alignment of instrumentation in machinery applications.

The MCMS shall be used to monitor rotating equipment as well as to perform system configuration. The MCMS shall provide predictive analysis allowing reliability / rotating equipment engineers to determine necessary remedial action. Data archiving within the MCMS shall have 6 months capacities as a minimum. Configuration files from MCMS racks shall be retrievable via laptop.

MCMS cabinets, typically located in the CCR in case distance is greater than 300 m it may be located in other location. All analogue signals, status signals and system diagnostic alarms shall be transmitted to the DCS via single or redundant serial communication links in the CCR. An OPC interface to the DCS shall be provided in the CCR to interface required process measurements with MCMS server.

The machine monitors shall not generate machine trips. Instead, the monitors shall have digital outputs which shall be hardwired to the SIS to initiate equipment shut down. Vibration transmitters for air fin coolers will be connected to the MCMS.

4.8 Custody Metering Systems

The metering and quality monitoring of CO_2 will be at source destination/emitters only. There will be no metering and quality measurement at the inlet of the CPF. Emitters shall share the CO_2 quality and metering data on Ervia control centre. Emitters should share calibration records of CO_2 metering and quality monitoring instruments and analysers with Ervia. The emitters/source destination shall inform the CPF immediately if there is any deviation in quality of CO_2. The CPF should have ability to isolate poor spec CO2 from emitters. (See Ref. 4 for more details)

Metering and quality monitoring of stored CO_2 will be provided for CO_2 that will be exported from the CPF via ship.

Each metering system shall include one microprocessor-based flow computer per stream meter, a supervisory computer, and printers. The supervisory computer will be utilised as an interface to the DCS, to monitor

individual flow computer operation and to perform flow totalising for multi-stream operations. Flow computers shall be configurable from a dedicated laptop PC to be connected to each individual flow computer. Configuration from the front of flow computer keypad shall also be possible.

Each flow computer system shall include a redundant communication link to the DCS using Modbus TCP protocol and generate reports to a local printer. The flow computers will be mounted in the unit control panel (UCP) and will be installed in the CCR. The supervisory computer shall also be installed in the CCR. Flow computer serial data submitted to the DCS shall be comprehensive for generation of the necessary reporting. The major functions of the metering system are as follows:

- Acquisition and processing data from flow meters, temperature, and pressure transmitters. The density and viscosity required for the calculation will come from a laboratory analysis and be entered manually;
- Meter factor curve linearisation;
- Temperature, pressure, density, and viscosity correction;
- Automatic meter proving and control of prover functions;
- Generation of reports; and
- Provision for verification of proving data.

4.9 Pipeline Leak Detection System

Pipeline leak detection systems shall be installed to detect any leak in the pipeline system. The system control panel shall be installed within the CCR close to the point where the pipeline enters/exits the plant. The leak detection system shall be connected to DCS.

The leak detection technique to be deployed is Distributed Acoustic Sensing (DAS) and/ or flow mass -volume balance methods and pressure analysis with SCADA. For DAS, FO cable shall be buried along the pipeline underground in the pipeline corridor. Installation orientation of the cable with respect to the pipe shall be based on supplier's recommendations. The same FO cable shall also be used for communications & control including intruder detection system.

DCS shall include a display which will include a schematic of the pipeline covered by leak detection system, with all the system alarms, monitoring status and in the case of a leak, indicating the location of the leak. Because of the novel technology, the system shall be used for alarm only, and required actions are to be determined by the operators.

4.10 In Field RTUs

RTUs shall be installed at the Pipeline in-field locations (Valve Installation and pigging installations). The RTUs will provide required Control and Monitoring of DCS, SIS and FGS functions.

Each RTU shall have modular design. Since RTU Installation shall be direct at the site, RTU would be in a climate-controlled kiosk/building for weather protection. The RTU shall be a fail-safe design with a high reliability (SIL-2 and high availability).

In addition to all local functionality, each RTU shall be equipped with all necessary hardware (including fibre optic modems, patch panel, etc.) and software to achieve communications with Central Process Facility (CPF) control and safety networks via redundant Fibre Optic links.

It is preferred that the RTU will be supplied by the ICSS vendor. Power supply to the RTU shall be 230 VAC / 50 Hz. The RTU shall have its own internal UPS.

4.11 Berth, Mooring, Loading/Unloading and Ship to Shore Systems

The Navigation System shall provide precise vessel positioning via carrier located portable GPS satellite pilot unit and jetty laser system. The guidance systems are supported by a large 'Pilot' display board for Marine information located on the jetty head.

The Docking System shall monitor the mooring line tension of each hook and alert the Jetty Controller in the event of an abnormal line condition. Should a hazardous condition occur, the Jetty controller shall be able to release some or all the mooring hooks, locally or remotely, following consultation with the CO_2 Carrier Captain.

The MetOcean System shall monitor marine and meteorological data. The following instruments will be provided:

- Weather station to measure air temperature and barometric pressure, humidity, and rainfall;
- Seabed mounted tide and current sensor;
- Seabed mounted directional wave sensor;
- Sea water temperature; and
- Visibility sensor.

Loading arms shall have their own hydraulic power control system with loading arm position alarms for operation monitoring. The Emergency Release Coupling and Powered Emergency Release Coupling are also part of loading system and controlled by SIS system.

For emergency shutdown of the cargo transfer, a ship to shore communications link should be provided according to the Society of International Gas Tanker and Terminal Operators (SIGTTO) guidelines as well as local codes and standards.

JCR operator will communicate with ship using radio and hot line phone.

The system cabinets and workstation(s) will be installed in the JCR.

5 Common Requirements for Systems

5.1 Power Supply Systems

All AC supplies shall be distributed via separate AC distribution boards. AC supplies shall be 230 ± 6% VAC, 50 Hz, neutral earthed. Electrical supplies for instrumentation system shall be provided as follows:

Dual supplied AC uninterruptible, maintained power supply derived from redundant AC UPS units with back up time of 60 minutes.

AC interruptible power supply from emergency supply (Emergency Diesel Generator backup).AC general purpose supply.

All control / safety / emergency response systems / FGS and PAGA shall have UPS autonomy time of 60 minutes. For emergency response, FGS and Public Address and General Alarm (PAGA) systems shall be designed for 12 hours in case the Emergency Diesel Generator (EDG) is not operational. An alarm shall be generated in the ICSS when 30 min of the 60 min back up duration have passed.

Each instrument system or cabinet requiring power shall be fed by 2 separate feeders, from separate AC UPS distribution boards 'A' and 'B'. 230V 50Hz UPS power distribution within cabinets shall be redundant.

Instruments requiring 230V 50Hz from a single source shall have a single supply from the AC UPS distribution board, either 'A' or 'B'. Where redundant equipment is provided, these shall be 50/50 split over 'A' and 'B' distribution boards.

The AC voltage conversion to signal level shall be via redundant power supply units (PSU) serving each system or cabinet. 24V DC power output from these PSUs shall be made common using diode-oring-automatic balancing units.

The CCR shall have its own AC UPS and distribution, AC emergency power supply and distribution as well as non-UPS AC power supply and distribution. This shall be engineered during detailed design.

5.2 Fibre Optic Network

A plant / field wide integrated fibre optic (FO) network infrastructure will be installed which will form the FO backbone. The fibre optic cable along the pipeline route shall be used for leak detection, communication, and control purposes. The ICSS, other control systems in the plant as well as other disciplines shall all make use the same FO backbone. The FO Back bone shall be designed with either a star or ring topology, whilst there is a preference for star topology to be applied inside the processing facilities and ring topology may be applied in-field.

Routing between buildings shall be via dual diverse routing providing the required redundancy.

The single mode FO cable shall be utilised, and standardised FO connectors shall be used throughout the project.

5.3 Availability

All parts of the systems shall be designed to achieve an availability of 99.99% for the overall system, and 99.999% for SIS and FGS, considering a mean time to repair of eight (8) hours or less. This shall be achieved by implementing redundancy, fault tolerant technology, self-checking, and diagnostic capabilities.

SIL Determination and SIL Verification will determine the maximum allowable test periods of trip initiators and final elements. However, testing shall not be more frequent than one test per year, when testing requires a shutdown of the complete train / plant, the minimum test interval shall be the 4 years minimum.

When it is not possible to meet the required test frequency, manual bypass facility with status monitoring shall be provided to ensure production whilst SIF testing is carried out. Bypass status shall be displayed on the DCS.

5.4 System Segregation

Major units, processing trains or plant areas which can be operated independently shall have their instrumentation systems control and I/O processing hardware separated and segregated to enable maintenance, testing and card replacements to be carried out without having to physically interfere with or disturb the control and I/O processing hardware of other units/plant which may remain operating.

Within plant units, signals shall be distributed throughout the control and I/O processing hardware such that the number of critical control loops or outputs which could be affected by common mode failures is minimised.

Where identical process trains are implemented, system design for both hardware and software shall be identical.

5.5 Sparing and Performance Requirements

Spares shall be made available and distributed over process units. It is not allowed to lump them into only one section. Minimum 20% installed spare I/O capacity (wiring, termination, modules etc) and spare space shall be available after plant commissioning. Spares shall be evenly distributed over the various types of I/O cards.

CPU loads and communication highway loads shall not exceed 60% of load under all loading conditions. Power supply units shall include 50% spare capacity.

Spares for all major items shall be based on manufacturers' recommended spare parts and maintenance requirements.

5.6 Central Control Room (CCR) and Jetty Control Room (JCR)

The CCR and its Rack Room typically includes the following cabinets including instrumentation systems auxiliary equipment supporting the ICSS operator consoles:

- Communications interface equipment for DCS, SIS and FGS etc.;
- DCS, SIS and FGS I/O cabinets with cable termination;
- Fibre optic cabinets with patch panels;
- OWS, EWS and Keyboard and Printers;
- ICSS equipment, like network servers, backup servers, Virtualisation server and PCs;
- Pipeline Systems RTU;
- MCMS cabinets;
- PAGA system cabinets;
- Telephone cabinet and Telephone Main Distribution Frame; and
- Power distribution cabinets (UPS and non-UPS) for above mentioned equipment.

The Engineering Room (Separate room in CCR with glass partition) shall house DCS EWS, SIS EWS, FGS EWS, ICSS EWS, MCMS engineering station, Dedicated SOE station and other engineering stations as identified during detail engineering. The ICSS EWS shall be used to access ICSS sub systems like the IAMS, the backup servers etc.

EWS of systems other than ICSS shall have their own dedicated printer. Two plant network integrated printers shall be provided for ICSS EWS.

The engineering room shall be designed in such a way that all programmable electronic systems of the plant can be maintained, modified, and commissioned from this room. The engineering room shall have an access control system.

System cabinets shall be spaced with approximately (minimum) 1.2 m between rows and 2.0 m from walls. Cabinets will be free-standing, with front and rear access. In case the CCR is modularised, marshalling cabinets shall be provided against the wall of the container and one row of free-standing system cabinets in the middle.

Cabinets in CCR Rack Room shall be supported on frames. The frame floor shall have 600 /400 mm height above base floor for stick built / modularised CCR respectively. The cabinet support frames shall be provided for the complete length of a cabinet row. The CCR shall have a minimum of 30% spare floor space at the end of commissioning.

In case the CCR is fitted with an air lock, this air lock shall be protected by gas detection and differential pressure monitoring and alarm. CCR console and furniture shall be within the scope of MAC.

The JCR will house Ship to Shore System, Berthing and Mooring Cabinets & System, Loading/Unloading Arms Cabinets & System, Fire Alarm Panel, ICSS system/marshaling cabinets and 3rd party equipment such as Radio, CCTV etc. required for berthing, mooring and loading/unloading operations.

5.7 Analyser House

Analysers are typically installed at free standing racks, however due to process requirement they may be installed in Analyser Houses. Analysers will have a non-redundant serial link to DCS. The equipment inside the Analyser House shall be suitably protected for the hazardous area inside the house. Hardwired I/O is required to connect control / safety signals from analysers to the DCS.

The FO network will be extended to each Analyser House. Fresh air intake shall be provided with suitable means to protect against ingress of sand, dust, and toxic / explosive gas mixtures into the Analyser House. HVAC systems shall have redundant air blower / cooler systems meeting the minimum amount of air changes as required by the code.

5.8 Systems Hardware, Cabinets and Network Cabling

Vendor standard hardware shall be used for CPUs, I/O Cards etc. All hardware supplied shall be of proven technology. Separate cabinets shall be provided for marshalling and systems. Marshalling hardware shall be suitable for digital HART communication protocol.

Equipment shall preferably be 19-inch rack mounted and be installed in cabinets. System cabinets shall be prewired, and factory tested. The MAC shall propose a standard cabinet design for the DCS, SIS and FGS for owner approval.

Field Terminal Assembly cards and cross wiring shall be installed in marshalling cabinet(s). All incoming field cables shall be terminated on "knife switch" type terminals to provide a field disconnect. Fused terminals shall be used where necessary to protect I/O processing hardware as well as for powered outputs.

System cabinets shall consist of CPUs and I/O cards, power supply and terminals for terminating cables from marshalling cabinet(s). Each cabinet shall have common cabinet alarms and be wired to the nearest DCS cabinet.

All Cabinet cable entries shall be provided with protection against ingress of dust. Each cabinet shall be provided with cooling fans and filters to maintain good cooling and air movement. All plant network cabling (other than the FO back bone) shall be based on standard Ethernet cables according to CAT5e/6e specification.

5.9 Heating, Ventilation and Air Conditioning (HVAC) Requirements

HVAC system will be provided for the CCR and JCR. Controls for HVAC shall be executed directly from local HVAC control panels supplied by others. The HVAC control panel shall perform Differential Pressure & Temperature Monitoring and Control, Start/Stop of heaters & fans and auto-changeover of duty equipment.

Gas detection at air intakes shall be provided. In case of fire/smoke detection inside rooms, the HVAC system shall shutdown according to FGS logic specified in Cause & Effect (C&E) diagrams. The FGS shall interface with the HVAC to perform safety related functions such as Shutdown of HVAC Unit and Closing of dampers. Pressurised buildings shall be fitted with pressure monitoring with indication and alarming in ICSS.

The HVAC requirements shall comply with project HVAC specifications developed during FEED

6 Distributed Control System (DCS)

6.1 General

The DCS functionality shall include the following: -

- Operator's interface for the remote operation, monitoring, and control of the plant;
- Display for all alarms, process and auxiliaries, and process variable recording traces (real time and historical trend);
- Base level regulatory control and monitoring of the plant, keeping the plant operating within normal operating boundaries;
- Sequential, timed and logic control functions;
- Alarm display and alarm management;
- Reporting / printing;
- Read transmitter and valve data from HART equipment for inclusion in IAMS;
- Data archiving; and
- Interface to owner Business IT environment.

The MAC shall assume responsibility for the total systems for the design, engineering, delivery, installation supervision of the instrument systems in all the locations as applicable in the project as well as system integration tasks. Real time and historical trending are required for all measured variables as a minimum. Detailed requirements related to the DCS will be defined in the ICSS specification prepared during FEED.

6.2 Human Machine Interface

Control and monitoring of the facilities shall be from operating consoles in the CCR. The number of VDUs and keyboards required for the plant operation from the console shall be based on workload for the operators. A typical figure of 200 to 250 control loops per panel operator is realistic for process plants and utilities under normal operating conditions. The proposed operator console arrangement will be similar for all consoles. Each of the console bays will have (typically):

- DCS (Quad VDU) sections;
- Telecom sections;
- Owner PCs;
- Process CCTV monitors with mouse for operation; and
- Hardwired switch panel section(s) (Quantity as required).

All PC based stations shall be supplied with a 21" flat screen, Min resolution 1600 x 1200. The CCR shall be provided with two printers size A3, one color and one B/W.

DCS OWS shall be provided in the operations support room / shift supervisor offices in view only mode.

A 'single window' concept shall be applied and hence SIS, FGS and PLC data shall be integrated into the DCS. Fire and gas information will be monitored on DCS graphics showing plant, area, and unit overviews. One of the consoles shall have a FGS related switch panel for firefighting and firewater controls.

Emergency graphics shall be developed for critical alarm displays for use by the operator in case of emergency.

DCS HMI operator workstation PCs shall be installed in the CCR Rack Room and be connected to the screen/mouse/keyboard in the CCR by means of KVM switches. A thin client solution would also be acceptable.

The JCR will have a similar console and OWS as in the CCR.

Access to HMI shall be regulated by means of key locks / user accounts / password / managed privileges.

6.3 DCS Hardware

The following DCS components shall be redundant: -

- Power supplies;
- CPUs;
- Communication busses;
- Remote I/O busses;
- Analogue, discrete and sequence control and interlocking I/O including digital outputs;
- DCS data highway communication links to the SIS and FGS;
- Mass data storage; and
- I/O related to control shall be redundant.

MAC supplied system configuration meets the availability requirement of this philosophy.

6.4 HART DATA

All analog input and output modules shall have the capability to transfer the transmitter / valve positioner HART data to and from the DCS for maintenance management by the IAMS (without the use of multiplexers).

6.5 Software

In addition to conventional DCS functions, analogue, digital, logic/timer sequential control functions and data acquisition via hardwired I/O and serial links, special functions application software as specified in the P&IDs shall be configurable in DCS:

- Advanced Process Control;
- Specific control applications; and
- Fin-Fan Control.

6.6 Instrument Asset Management System (IAMS)

The IAMS provides maintenance capabilities by collecting HART data of the instruments, control valves, on/off valves, and motor operated valves. Instrument valve supplier software for detailed maintenance / diagnostics shall be integrated with the IAMS. The same is required for on/off valves and related (partial) stroke testing. Control valve / on/off valve supplier's software shall be server based and be accessible from any IAMS station. A sufficient number of licenses shall be included.

Where packages are provided with UCPs, these standalone UCPs shall be supplied with HART multiplexers to transmit HART data of the field devices to the IAMS. MAC shall integrate HART data from the package into the IAMS.

HART data refresh on the IAMS screen is less than 30 seconds. Signature test of control valves and on/off valves shall be performed during the FAT and be loaded into IAMS during loop test period.

The ICSS network may be extended to the Instrument workshop. IAMS workstation shall also be provided.

6.7 Time Synchronisation

Time Synchronisation shall be provided. A master time signal shall be obtained from a GPS driven time server. This time server will synchronise all system clocks in the DCS controllers, DCS EWS and OWS, SIS controllers, FGS controllers, and all other 3rd party supplied control systems. The DCS shall act as a master for all other systems. The time shall be synchronised at least once every twenty-four (24) hours.

Package unit PLCs shall have time synchronisation with DCS using NTP Ethernet connection. If required, the GPS antenna shall be installed on the roof of the CCR.

6.8 DCS Communications

The DCS equipment shall be connected to its own data highway network (or via FO link) communicating with all DCS equipment installed at various locations. The network shall be common for SIS and FGS.

3rd Party Control Systems will interface with the DCS using serial communication links. Serial links shall be redundant or single as indicated in this document. Serial link data transmitted from 3rd party PLC to DCS shall include SOE data. In case OPC is used, the communication link shall always include a firewall when communicating to/from 3rd party systems.

Package to be integrated	Preferred Protocol
3rd party PLC	Modbus TCP/IP
Analyser House	Modbus TCP/IP
Gas Chromatographs	Modbus TCP/IP
IMCS in Sub Station	Modbus TCP/IP
MCMS	Modbus TCP/IP or OPC UA
Custody Metering System	Modbus TCP IP

6.9 Central Processing Facility (CPF) Networks Architecture

Refer to CPF, Control System Architecture Drawings, MDE1234-BEC-03-CX-DR-E-0001.

6.10 Alarm Management and Sequence of Event (SOE)

EPC shall develop and implement an integrated alarm philosophy into the ICSS. The alarm management system shall allow static and dynamic alarm suppression, operator shelving of alarms and status of process units. The alarm management system shall be configurable with discriminating access levels for operator and shift supervisor. Depending on mode and access level, it shall be able to view active alarms, all alarms, set or alarm filters, or enable/disable alarm management rules.

SIS and FGS alarms with appropriate time stamp shall also be collected in the alarm management system. SOE data from package PLCs shall be collected using serial links between these PLCs and the DCS.SOE resolution time between events shall be 1 millisecond.

The alarm management system shall segregate ICSS system alarms from the process alarms. Transmitter maintenance related alarms derived from HART instruments shall not be routed to the operator but to the IAMS, where the maintenance engineer shall take appropriate actions

Alarm management system data / SER data shall be stored electronically, A dedicated SOE viewing station shall be installed in the CCR Engineering Room.

6.11 DCS Anywhere

Using a network connection between the ICSS and the owner office network infrastructure, the authorised personnel shall be able to view applications on owner office PC. Similar functionality shall be provided to any OWS within the ICSS architecture.

6.12 DCS Large Screen Displays

Each console in the CCR shall have a large screen installed above the console. The purpose of these screens is to display DCS overviews, graphics or FGS graphics and / or CCTV images.

Large screens shall have their video input from various OWS PCs installed in the CCR Rack Room. Each console shall have a dedicated graphic that lists the available screens to be displayed and when the operator makes his selection, the applicable graphic shall be displayed on the large screen (which has redundancy).

7 Safety Instrumented System (SIS)

7.1 General

The safeguarding philosophy shall be designed for each item of equipment by implementing SIFs for alarming, protection and emergency shut down to prevent or to mitigate operational upsets, hazardous events, and exceedance of mechanical limits of plant / equipment. These events may lead to injuries to personnel, significant production/ equipment loss and/or environmental damage. Manual and automated shut down actions shall be executed upon detection of these events.

The assessment of SIFs and method of implementation in the DCS or SIS will be verified during the SIL determination. According to the targeted SIL assigned to SIFs, the SIFs are implemented (<SIL-1) in the DCS or as a trip function (>=SIL-1) in the SIS. DCS control and SIS trip functions shall be fully segregated. However, if SIF loops with different SIL ratings relate to the same piece of equipment, they are implemented according to the highest class. Each process unit shall rely on SIFs which are independent from other process units.

SIL Verification shall be performed and document that all SIFs are designed correctly and meet their respective SIL ratings per IEC 61511 and IEC 61508. All required data and documentation as per IEC 61511 shall be developed. The SIL verification tool and all data shall be documented with approval from owner. The SIL Verification tool shall be certified software such as Exida or equivalent.

SIF functionality shall be specified as per Safety Requirements Specification (SRS), P&ID, C&E diagram, and SIS-FS (safeguarding narrative). The EPC shall update and complete these documents to reflect the engineering development during the detailed design implementation phase.

Emergency Shutdown logic shall be designed in shutdown levels to allow for a structured implementation.

- Level 1: Equipment or local shutdown;
- Level 2: Train or sub-system shutdown; and
- Level 3: Facility Shutdown.

The SIS shall be designed to be fail-safe. The logical 1 state represents the plant healthy state or energised output state, and the logical 0 state represents the fail-safe state or de-energised output state.

SIS logic shall not rely on cascading process effects and related equipment shall be tripped immediately without the need for subsequent safety instrumentation to sense the consequential impact from the first process setup that caused the initial trip initiator to act. However, consequences of process trips should be carefully evaluated as it is unnecessary to trip complete processing plants. The process design should allow for surge volumes in certain process vessels so that trips caused by process upsets do not immediately have an impact on overall plant production. This is in line with Process Control and Safeguarding Philosophy MDE1234-RPS-01-CX-RP-Z-0004

SIS safety related signals shall comply with the following: -

- Signals to/from the SIS shall be hardwired;
- SIS circuits shall be de-energising to trip in fail safe state;
- Signals shall be wired to redundant I/O;
- Digital inputs originating from the field shall be line monitored for line break and short circuit;
- Digital outputs that are normally de-energised shall not be used, however exception may be used for certain blow down valves, subject to owner approval;
- Signals related to 2oo3 voting schemes need not be wired to separate I/O cards; and
- SIS safety bus is integrated within the ICSS data highway, SIS peer to peer communication shall take place over a dedicated safety net using deterministic communication, with communication protocol and FO infrastructure approved for use in SIL-3 applications.

SIS non-safety related signals to / from SIS shall comply with the following: -

- SIS I/O for reset switches and MOS Enable switches may either be routed via the redundant integrated DCS/SIS network or hardwired; and
- Hardwired non-safety related circuits shall be arranged such that any failures cable/termination faults, power supply loss etc. will not cause shutdowns or compromise the safety system integrity.

The modules of the SIS shall be capable of HART data interface for transfer to the IAMS.

7.2 Measurement Devices

All instruments shall have separate process connections. Pressure, flow, level, and temperature transmitters shall be used rather than switches. The use of a single measurement device for control and shutdown shall not be permitted.

Instruments connected to SIS and DCS for the same process measurement shall have the same calibration range and a deviation alarm shall be generated in the DCS for any discrepancy in the readings.

The use of redundant sensors allows signals to be compared so that fault conditions can be detected before they become significant. A single field device fault shall not result in a spurious trip which results in shutdown of a compressor or isolation of a section of pipeline.

7.3 Final Elements

Typical SIS final elements include shutdown valves and motors. Shutdown valves connected to the SIS system will be designed to move to a safe position on loss of control signal, power, or air. Depressurisation valves will be provided with secure air reservoirs to enable valves to be operated on loss of instrument air header pressure. The direction of valve failure shall be as per the P&ID.

7.4 Partial Stroke Testing (PST)

The manually initiated PST of SIS On/Off valves shall be implemented per SIL verification recommendation. Blow down valves do not require valve stroke testing. Scope of PST testing also includes in-field on/off valves at the Valve Installation and pigging installations. Valves connected to the DCS do not require PST.

Valve positioner shall have dual 24V DC signal connections, one from SIS and one from DCS. The DCS connections shall be 4-20 mA HART based and only be used for valve testing and position feedback. Shutdown actions shall always overrule any control action initiated via the HART signal connection. Valve stroke test results shall be documented in the IAMS. Devices used in PST shall be such that they will never jeopardise the required safety function and will not interrupt plant operations.

Routine operation of the PST shall be from dedicated operator graphics. In case PST is initiated from the IAMS, this shall only be possible when permitted by the operator (enable set from operator graphic). In both cases, the results shall automatically be documented in the IAMS.

Genuine trip actions shall be considered during proof testing. SOE shall track the trip events where trip action is simultaneously reported during proof test.

7.5 Reset

SIFs shall have either auto reset or manual reset from control room and / or local. Refer to Process Control and Safeguarding Philosophy MDE1234-RPS-01-CX-RP-Z-0004. Unit specific reset requirements are documented in the SRS.

SIS operated valves shall not have a field mechanical reset on the solenoid valve.

7.6 Sequence of Event (SOE) and First Out

The SIS shall have Sequence of Event. The SOE function shall be combined with the alarm management application. Refer Section 6.10

Each SIS alarm is indicated in a logic group. Each logic group shall have first failure alarm to identify the first out alarm from the group.

7.7 Maintenance Override Switch (MOS)

Testing of sensors and actuating elements of SIS are required to maintain the reliability of a system and to comply with local requirements. Maintenance Override Switches (MOS) and Maintenance Override Enable Switches shall be provided on these elements to enable testing and maintenance of I/O without interrupting the process. Refer to Process Control and Safeguarding Philosophy MDE1234-RPS-01-CX-RP-Z-0004.

EPC shall define MOS Enable switches for the various process units. All MOS functions shall be captured in the Cause & Effect Diagrams. Function of MOS Enable shall be documented in the SRS.

7.8 Matrix Panel, Emergency Shut Down

The operator consoles in the CCR shall be fitted with a Matrix Panel as common services console. In general, all switches on the Matrix Panel shall be of the direct push in / latch type, push-in again to reset, complete with lift cover. Push button shall be fitted with back illuminated lights to show that the action has been executed.

For manual shut down of major equipment like compressors, switches located on the Matrix Panel shall be hardwired to the SIS. The switches shall have red backlights, activated when the trip of the equipment has been executed. Contacts shall be wired fail-safe and NC contacts shall be used.

8 Fire and Gas Detection Systems (FGS)

8.1 General

The Fire and Gas detection systems (FGS) will provide the interface to a range of field monitoring devices / sensors/manual call points and in the event of a detected or confirmed hazard (fire or gas leakage), take appropriate actions to ensure safe operation or controlled shutdown of the facilities.

The FGS shall be identical to the SIS with respect to system design, cabinet layout, use of CPUs, power supplies and I/O cards, etc. The FGS shall be Energise-To- Activate System. The system shall be designed as per local authority requirements.

The analogue input modules of the FGS shall be capable of HART data interface for transfer to the IAMS.

At the entrances of buildings and analyser houses, Fire Indication Panels shall be provided to warn and alarm personnel upon fire or gas detected inside building.

A FGS Overview Display in CCR and JCR shall be provided. This will be an overall plant geographic plan. It shall be used to display critical FGS status and alarm indications. The main graphic shall incorporate a wind speed and wind direction indicator, the signals shall be taken from weather monitoring station. Detailed FGS graphic displays and status of alarms shall be displayed on the DCS HMI on the operator consoles.

Total plant wide alarming for either fire or gas being detected shall be interfaced to the Public Address and General Alarm (PAGA) system. The interface shall include two hardwired signals, one for confirmed gas detected and one for confirmed fire detected.

In case of a confirmed hazard the system will also be responsible for initiating the appropriate visual and audible alarms in the CPF CCR and JCR and pipelines (Valve installation and pigging installations).

The FGS shall interface with an automatic fire extinguishing system for equipment rooms, typically substation, facility rooms, CCR and JCR buildings.

8.2 Fire and Gas Detectors

The choice of detectors for an area shall reflect the anticipated hazard of a fire or gas release. The location of detectors shall be selected in such way that the anticipated fire or gas characteristics may be easily detected. Flammable gas detectors, smoke detectors, heat and heat rise detectors, IR/UV flame detector and manual alarm call points shall be considered for F&G detection.

Certain installations may also require linear heat detection and / or respiration systems.

A High Sensitivity Smoke Detection (HSSD) system shall also be considered for all equipment and server rooms and any location where critical control / telecoms equipment may be installed.

FGS devices shall use 0 – 20 mA / 4 – 20 mA input signals. 0-4 mA under range shall be used to transmit field device health status information to the FGS. The sensors shall be of the HART type.

8.3 Fire and Gas Detection in Buildings / RTU

All signals from the buildings/ RTU F&G detectors shall be connected to the respective local fire alarm system panels. The local fire alarm panel shall interface directly with the HVAC system for executive action in case of confirmed hazard detection.

Local Panel will interface with the DCS/RTU via redundant serial communications for status monitoring in the CCR.

8.4 Fire Fighting Actions

The FGS shall activate firefighting equipment as specified on the P&IDs and C&E diagrams. FGS will be interfaced with FM-200 or equivalent, Fire Water Pump and Deluge Valves. Activation of these systems shall be automatically, or remote-manually from CCR or locally from field.

Deluge valves shall be fitted with a secure instrument air supply.

9 Supervisory Control and Data Acquisition (SCADA)

SCADA will be used and under normal conditions for the Pipeline System (including the Valve Installation and pigging installations) and will be operated from the CCR through the SCADA system. The SCADA system will communicate via a fibre optic network with the control system at each station. Motorised valves will be controlled remotely from the CCR when isolation of pipeline section is required or when the flow of gas needs to be configured for either CO_2 export or CO_2 import scenarios. The following control / supervision shall be possible via the CCR:

- Setting and supervision of the main process parameters such as overall system throughput;
- Remote switch-over between pipeline runs;
- Flow path monitoring;
- Supervision of the SIS and FGS detection system status;
- Emergencies stop of stations; and
- Opening / Closing of pipeline motorised valves.

The critical SCADA servers, operator workstations, and network equipment will be installed in the CCR. The CCR SCADA will continuously monitor and control the overall pipeline.

There shall be no single point of failure on any critical system component which will lead to an interruption of service. A critical component is any component whose failure directly and adversely affects the system's overall performance or its ability to continue performing the critical SCADA functions of monitoring and control.

The fibres provided for communication networks for SCADA will be located at 10 o'clock and 2'o clock fibre optic cable along the pipeline. There will be two fibre optic communication cables from the CCR.

Data exchange between SCADA system and Demilitarised Zone (DMZ), offline simulation server, pipeline monitoring system, is controlled by firewall hardware and software.

Control systems to be controlled and monitored by SCADA system are stated below:

- Station control system at metering stations;
- Remote terminal units at Valve Installation; and
- Remote terminal units at pigging installations.

The Valve Installation and pigging installations are unmanned stations to be controlled and monitored from CCR, however during loading / launching / receiving and removing the pig, physical presence by operator will be required at the pig launcher / receiver station.

In case of telecommunication failure, maintenance of telecommunication equipment or other operational requirements; these remote sites need to be controlled at their physical location. For this purpose, there shall be provision for changeover of control to RTU through local HMI at the Valve Installation and at pigging installations. The CCR shall be able to grant control of each station to the RTU if the operator located there requests a changeover of control from the CCR by use of handover procedure.

SCADA system hardware, SCADA system software, SCADA system active communication equipment and SCADA system IT passive infrastructure shall be designed to satisfy the redundancy.

Process data base server, report management server, historical data base server, Network Time Protocol (NTP) Server, online simulation server, offline simulation servers shall be configured as independent hot standby servers. The communication system supporting SCADA shall be configured as redundant pairs.

The SCADA system shall enable authorised operator staff to monitor and control by predefined monitoring and controlling rights through operator workstations.

The SCADA system shall make connection to corporate or other networks in such way that a failure of any of these networks shall not affect the SCADA system's ability to perform its critical functions. User permissions and security restrictions regarding all aspects of the SCADA system shall propagate seamlessly across the SCADA system's distributed architecture.

The system shall not be dependent upon specialised, unique, or proprietary equipment or software available from only a single supplier. The SCADA system equipment shall have self-diagnostic, self-recovery software for preventive maintenance and troubleshooting. The system shall be capable of recovering itself with critical functions and devices being monitored by health monitoring software. SCADA system self-diagnostic and self-recovery software shall check critical components for failures and take the least intrusive course of action to recover from any failure.

SCADA Process Data Base servers shall receive alarms, events, and other operational data from remote terminal units at the Valve Installation and at pigging installations. The SCADA system shall transfer data to third party users and corporate users through servers located at Demilitarised Zone (DMZ).

Pipeline monitoring system servers shall be interfaced to SCADA at the CCR. Pipeline monitoring system leak detection data shall also be integrated with SCADA.

Operator workstation hardware shall enable operators to control and monitor all equipment by showing process graphics, alarms, events, current values, historical values etc. Engineer workstation hardware shall be capable of processing all functionalities of operator workstation. In addition to this, update and diagnostics of control software and data communications shall be handled in the engineering workstation.

The SCADA network shall use two separate L3 switches at all stations. All network switches shall be provided with dual processors, dual RAMs, and dual power supplies.

The SCADA network shall have an installed spare capacity of 20% at the end of plant commissioning.

In addition to redundancy applied at the fibre optic cable level, VSAT terminals may be provided for SCADA at the CCR, Valve Installation and at pigging installations. VSAT terminals will be used in case of FO outage of communication to/from the station.

The SCADA network shall operate at a minimum data speed of 1 Gbps. L3 switches shall provide communication by use TCP/IP.

The entire SCADA network shall be synchronised to a common time reference provided by a GPS based NTP server primary reference clock to ensure accurate and consistent time stamping of signals and events.

10 ICSS Interface and Communication Systems

10.1 General

The scope and requirements for the interface with the owner MIS shall be addressed based on project contract.

The following systems, functions and services are to be part of the ICSS system architecture and MAC scope of supply:

- Automated backup solution providing daily/weekly incremental and complete backups of all controllers, servers, and workstation PCs of the system. The system shall store back up data on hard disk;
- A DMZ shall be provided to segregate the ICSS from owner IT infrastructure. DMZ shall include firewalls, patch, and anti-virus server;
- Server and domain controllers;
- Network monitoring server that monitors and reports any network issues;
- Terminal servers for applications;
- ICSS system site services until commissioning are in the MAC scope;
- The system shall be anti-virus protected for the complete architecture and shall allow for automated updating of anti-virus;
- System shall allow for manual installation of operating system software patches;
- A fire wall shall be installed for all external connections to controllers e.g. OPC connections to external systems;
- Virtualisation of above indicated servers shall be considered.

Level 4 MIS (office domain) data communication is owned by IT discipline. FO link will be provided to support client IT systems.

10.2 Cyber Security

Cybersecurity measures shall be incorporated as required to protect the system from intrusion using methodologies compliant with applicable codes.

In general, the reported cyber security incidents are often caused by malware, including viruses, worms, and trojans. Also, it is found that security breaches often occur due to inadvertent action by plant employees, who simply are not aware of proper security procedures.

A cyber-secure plant shall have a solid mix of technologies, policies, and procedures in place to combat potential threats effectively.

Many vendors usually ship the products with default password used during the Factory Acceptance Test (FAT). Leaving default passwords and security settings in place shall not be permitted. The passwords and security settings policy shall be enforced to all third-party vendors and shall be documented for further handling during the start-up and commissioning phases.

Other cyber-security tools are available such as application whitelisting. Application whitelisting is a proactive security technique where only a limited set of approved programs can run, while all other programs (including most malware) are blocked from running by default. Application whitelisting enables only the administrators, not the users, to decide which programs can run. All vendor supplied systems shall follow cyber security requirements.

The plant network infrastructure will be segmented in secured layers. Communication between these layers must pass through a protected and monitored network layer conduit, a path that regulates the flow of data between zones and allows for more secure communications.

Microsoft Windows Operating system and ICSS software patch management, anti-virus updates, which are extremely critical to maintaining a secure network shall be implemented in the project. These patches keep the system's software up to date and are often released when new vulnerabilities are identified.

The ICSS vendor shall assist in qualifying anti-virus software and should be involved in qualifying patches such as Microsoft security updates.

Policies around the use of portable storage devices such as memory sticks shall be defined and enforced. Plugging a memory stick into a USB port circumvents all network security mechanisms that were put in place to defend against a virus infection.

Another very important security policy is regarding disabling all unused/ spare communications ports as these could be used as open gates for security breaches.

Cybersecurity responsibility between owner, ICSS vendor and other stakeholders will be finalised during FEED/EPC