# Engineering Standard

# I-SPE-STD-013
# Control Systems Design and Construction

## Document number: SPE-00361



| Ver No. | Description | Document Owner | | Document Approver | | |
|---|---|---|---|---|---|---|
| | | Position | Approval | Position | Approval | Approval Date |
| 9 | Amended Version | Team Leader Process & Analysis - P7404 | Refer to supporting Info in REX | Manager Service Delivery | Refer to supporting Info in REX | 07/05/2026 |
| This Engineering Standard was endorsed by an RPEQ on behalf of Seqwater. | | | | | | |

# Version History

| Ver | Date | Description | Author | SME | Owner | Approver |
|---|---|---|---|---|---|---|
| 1 | 16/11/2016 | First Issue | | | | |
| 2 | 04/03/2019 | Amended Version | | | | |
| 3 | 15/10/2019 | Amended Version | | | | |
| 4 | 02/11/2020 | Amended Version | | | | |
| 5 | 30/03/2021 | Amended Version | | | | |
| 6 | 08/11/2021 | Amended Version | | | | |
| 7 | 14/01/2025 | Amended Version | | | | |
| 8 | 30/07/2025 | Amended Version | | | | |

(Refer Controlled Document in REX for Author, SME, Owner and Approver details)

# Contents

# 1. Purpose

This document is part of a suite of Seqwater Engineering Standards which are in alignment with the Seqwater Quality Management System. Their purpose is to provide a consistent approach to the development, modification, and management of Seqwater infrastructure that is fit for purpose, economic over the life of the asset, and meets Seqwater's risk appetite and compliance requirements including Work Health and Safety obligations.

This Standard Specification provides the minimum requirements and recommendations for the procurement, design, installation, and construction of control systems implemented at Principal's assets including PLCs, SCADA, communications, and ancillary equipment.

This document must be used in conjunction with the documents it references to assist in ensuring fit for purpose infrastructure. This Standard Specification is not intended to be relied on solely for design, supply, and installation works; advice from specialist engineers and/or manufacturers may be required on a case-by-case basis.

These technical requirements encourage the standardisation of control systems, SCADA and communication network design and configuration across all facilities.

# 2. Scope

This Standard Specification applies to all Seqwater employees, contractors, suppliers and consultants working for or on behalf of Seqwater unless otherwise stated. It applies to all new assets and to all existing assets undergoing refurbishment or modification. It must be used in conjunction with other relevant Seqwater Engineering Standards and project specific documents to define the technical requirements for infrastructure design and construction.

Where single or discrete components of an existing non-compliant system are to be replaced, refurbished or modified, this standard should not automatically be applied to the entire system retrospectively, however consideration should be given, in consultation with relevant stakeholders, to the extent of the application of the standard outside of the components requiring replacement, refurbishment or modification, to ensure safe, economic, and fit for purpose infrastructure.

Seqwater Engineering Standards include Standard Specifications, Drawings, Procedures, Templates, Forms and Preferred Equipment Lists. Together they detail Seqwater's minimum requirements and recommendations to provide infrastructure that will be fit for purpose, safe, and cost effective to operate and maintain. However, compliance with these requirements and recommendations does not remove, and cannot be relied on as meeting, the designer's overarching responsibility for ensuring infrastructure designed is fit for purpose and safe to construct, operate, maintain, and demolish. The designer must exercise appropriate due diligence to identify and manage hazards so far as is reasonably practicable.

Designers must also ensure compliance with relevant Australian Legislation, Standards, Codes and Guidelines (including those produced by Water Services Association of Australia). Where no Australian Standard exists for a particular application, work must conform to the most current version of an industry accepted international standard. Seqwater Engineering Standards use the International System of Units (SI), unless noted otherwise.

Deviation from meeting the minimum requirements in this Standard Specification requires written agreement from Seqwater as per the deviation process detailed in Procedure X-PRO-STD-008 Asset Standards Management and Application. That process includes completion of an X-TMP-STD-022 Asset Standards Deviation Request Form together with relevant supporting documentation, and submission by the Seqwater Project Representative to the Seqwater Engineering Mailbox. Where noted in this Standard Specification that Seqwater approval, agreement, or acceptance shall/must be sought, such approval, agreement or acceptance must be gained through the Seqwater Asset Standard Deviation process, as outlined above.

Responsibility for ensuring compliance with Seqwater Engineering Standards lies with those engaged in the management and execution of design, construction, and modification of Seqwater infrastructure. This includes modifications to the functional design of the infrastructure including technical changes made which would extend an asset outside of its design operating envelope and/or approved operation and maintenance practices.

Any ambiguities or conflicts identified between specific requirements within this Standard and project documents, another Seqwater Engineering Standard or Australian Legislation, Standards, Codes or Guidelines, must be brought to the attention of the Seqwater Document Owner as listed in the document footer, via the Engineering Mailbox, for clarification. Where it is proposed to proceed without meeting the requirements of this standard, agreement must be obtained via the Deviation Process, as outlined above.

Seqwater undertakes regular updates of its Engineering Standards. Before utilising this Engineering Standard the complete list of Seqwater Engineering Standards should be reviewed to ensure currency and applicability of standards to be applied to the works. These can be accessed on the Waternet Seqwater Engineering Standards & Framework page or from your Seqwater project manager, design manager, or engaging officer.

# 3. Definitions

The following definitions in Table 1 apply to this Standard Specification.

**Table 1: Definitions**

| Term | Definitions |
|---|---|
| Alarm | An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. |
| Alarm Dialler | It is the system that dial out on alarm conditions to alert personnel. The alarm can be delivered in the form of a Voice phone call, SMS, Email. The alarms to be dialled out will configured according to site needs. |
| Contractor | The Contractor is the entity that, dependent on contracted scope, is responsible for the management and / or execution of the design, construction, commissioning, and operation of the asset for the duration of a project (i.e., the "work"). Seqwater can undertake the role of the Contractor. |
| Control Systems | A system that responds to input signals from the equipment under control and/or from an operator and generates output signals that cause the equipment under control to operate in the desired manner. Components of control system include but are not limited to PLC, SCADA, network switches, fibre optic or Ethernet communication network, historian, engineering station, operation station, software server, IO modules, remote IO nodes, control panels, relay panels, real time clock (GPS), switchboard, AC and DC UPS and AC and DC distribution system. |
| Equipment / Block<br>Object / Device | These terms have a subtle but important difference from a coding perspective. A block is code that forms part of Seqwater's library (see I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification (SPE-00526) for further details).<br>An equipment is a physical item where its control is achieved by assembled block(s) (see I-SPE-STD-009 Control Systems Topology(SPE-00358) for further details).<br>The terms 'object' and 'device' are commonly used throughout industry. Seqwater re-defines these terms on a case-by-case basis to terms of 'equipment' or 'block' to remove confusion. |
| Group controller / Supervisory controller | A supervisory control block provides a method for controlling groups of equipment or other control blocks. It is designed to initiate and monitor groups of devices that function together. |
| Manufacturer / Supplier / Vendor / Original Equipment Manufacturer (OEM) | The entity that manufactures or supplies equipment to meet the specifications of the Contractor. |
| Owner / Principal / Seqwater | The entity that engages the Contractor to undertake the work and takes custody of the outcome. The Owner may delegate responsibilities to other entities to act on its behalf (e.g., a consultant). |
| PLC | PLC stands for programmable logic controller. It is a digital computer used for automation of electromechanical process such as control of machinery on assembly lines or in manufacturing plants (like power stations or water treatment plants etc.) |
| REX | Seqwater Electronic Document and Records Management System. |

| Term | Definitions |
|---|---|
| SCADA | SCADA stands for supervisory control and data acquisition system. The major function of SCADA is for acquiring data from remote devices such as valves, pumps, transmitters etc. and providing overall control remotely from a SCADA Host software platform. SCADA Host platforms also provide functions for graphical displays, alarming, trending, and historical storage of data. |
| Sequencer | A sequencer is classified as a device, that indicates the functions/logic to transition between states. |
| Seqwater Approval / Acceptance | Written sign-off gained via the deviation process, as detailed in *X-PRO-STD-008 Asset Standards Management and Application*. |
| Shall / must | Indicates a mandatory requirement |
| Should | Indicates a recommendation |
| Tag | The unique identifier assigned to a process measurement, calculation, or device within the control systems. The same definition applies to “Point” in the Control Systems. |

# 4. Abbreviations

The following abbreviations in Table 2 apply to this Standard Specification.

**Table 2: Abbreviations**

| Abbreviation | Description |
|---|---|
| AM | Asset Management |
| AC | Alternating Current |
| AS | Australian Standards |
| BDSL | Broad Digital Subscriber Line |
| CCP | Critical Control Points |
| CMF | Central Monitoring Function |
| COTS | Commercial, Off the Shelf |
| CPU | Central Processing Unit |
| DC | Direct Current |
| DHCP | Dynamic Host Configuration Protocol |
| DIN | Deutsches Institut fur Normung (German national organisation for standardisation) |
| DMZ | Demilitarised Zone – Network Security Zone |
| E1/T1 | Data Transmission Standard for the European equivalent of DS1 (T1) (ITU-T Rec. G.703 and G.732), 2.048 Mbps |
| ELV | Extra Low Voltage |
| FTA | Fault Tree Analysis |
| FOBOT | Fibre Optic Break Out Tray |
| FOC | Fibre Optic Cable |
| GPS | Global Positioning System |
| HACCP | Hazard Analysis and Critical Control Points |
| HART | Highway Addressable Remote Transducer |
| HMI | Human Machine Interface |
| ICT | Information and Communications Technologies |
| IP | Ingress Protection |
| IP Protocol | Internet Protocol – Network Transmission Protocols |
| IO | Input / Output |
| IEC | International Electro-technical Commission |
| ISA | Instrumentation Systems and Automation society |
| ISO | International Standards Organisation. |
| LCD | Liquid Crystal Display |
| LEO | Low Earth orbit (it is satellite developed for communication, Starlink for example) |
| Mbps/Kbps | Megabits per second/Kilobits per second – Transmission Rates |
| MCC | Motor Control Centre |
| MTBF | Mean Time between Failure |

| Abbreviation | Description |
|---|---|
| MTTR | Mean Time to Repair |
| NBN | National Broadband Network |
| NEMA | National Electrical Manufacturers Association |
| NIC | Network Interface Card |
| ODBC | Open Database Connectivity |
| OIP | Operator Interface Panel or HMI (Human Machine Interface) |
| OLE | Object Linking & Embedding |
| OPC | OLE for Process Control (Open Communications) |
| OS | Operating System of Computer |
| OTE | Operational Technology & Energy |
| P2P | Point to Point Communications |
| P2M | Point to Multipoint Communications |
| PID | Proportional, Integral and Derivative control |
| PSTN | Public Switched Telephone Network |
| PV | Process Variable |
| RAID | Redundant Array of Independent Disks |
| RBD | Reliability Block Diagrams |
| RIO | Remote Input Output |
| RTD | Resistance Temperature Device |
| RTU | Remote Terminal Unit |
| SCSI | Small Computer Systems Interface |
| SFC | Sequential Function Chart |
| SNMP | Simple Network Management Protocol |
| SP | Set Point |
| SPD | Surge Protection Devices |
| SPO | Special Purpose Outlet |
| SOE | Sequence of Events |
| SOW | Scope of Work |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| REX | Seqwater's document management system |
| UPS | Uninterruptable Power Supply |
| UTP Cable | Unshielded Twisted Pair cable |
| VSD | Variable Speed Drive |
| WTP | Water Treatment Plant |

# 5. Roles and Responsibilities

The following roles and responsibilities in Table 3 are applicable in the context of this specification.

**Table 3: Roles and Responsibilities**

| Role | Responsibility |
|---|---|
| Manager, Service Delivery, DTI | Accountable for implementation and management of this specification. |
| Project Manager | Accountable for project compliance with this specification. |
| Team Leader, Process & Analysis | Responsible for implementation and management of this specification. |
| Workers / Employees | Be aware of and comply with this I-SPE-STD-013 Engineering Standard Specification |

# 6. References and Related Materials

The documents listed in Table 4 below, and the requirements therein, are relevant to this Standard Specification In their latest editions, these documents form a part of this document. Note that this is not an exhaustive list of documents relevant to the works.

Seqwater undertakes regular updates of its Engineering Standards. Before utilising this document, the complete list of Seqwater Engineering Standards should be reviewed to ensure currency and applicability for the proposed works.

**Table 4: Seqwater References and Related Material**

| Description | Location |
|---|---|
| FRM-01275 SCADA License Application Form | REX |
| PLN-00388 Monitoring and Control Systems (MCS) Asset Class Plan | REX |
| PRO-00006 Electrical – High and Low Voltage Procedure | REX |
| PRO-01617 Engineering Standard X-PRO-STD-009 Engineering Design, Construction, Operation and Maintenance Procedure | REX |
| PRO-01872 Engineering Standard X-PRO-STD-002 Engineering Drawing Numbers Procedure | REX |
| PRO-01873 Engineering Standard X-PRO-STD-001 Asset Standards Documentation Classification and Naming Structure Procedure | REX |
| PRO-01874 Engineering Standard X-PRO-STD-004 Development and Review of Asset Standards Procedure | REX |
| PRO-02140 Engineering Standard X-PRO-STD-013 Engineering Technical Hazard Study Procedure | REX |
| PRO-02187 Engineering Standard X-PRO-STD-007 Drawing and Spatial Data Standards Procedure | REX |
| PRO-02190 Engineering Standard X-PRO-STD-006 Asset and Equipment Identifier Procedure | REX |
| PRO-02205 Engineering Standard X-PRO-STD-008 Asset Standards Management and Application Procedure | REX |
| PRO-02234 Management of Change (Technical) Procedure | REX |
| PRO-02253 Engineering Standard X-PRO-STD-014 Drawings Management Procedure | REX |
| REG-01074 Engineering Standard X-LST-STD-001 Seqwater Preferred Equipment Register | REX |
| SPE-00321 Server Rack Assembly Specification | REX |
| SPE-00322 Engineering Standard M-SPE-STD-006 Bulk Supply Meters for Potable Water | REX |
| SPE-00342 Engineering Standard I-LST-STD-001 Control Systems Prescribed Equipment | REX |
| SPE-00346 Engineering Standard B-SPE-STD-003 Commissioning Requirements | REX |
| SPE-00349 Engineering Standard B-SPE-STD-005 Functional Description Documentation | REX |
| SPE-00352 Engineering Standard E-SPE-STD-001 Electrical Design and Construction | REX |
| SPE-00353 Engineering Standard I-SPE-STD-015 Instrumentation | REX |
| SPE-00357Engineering Standard I-SPE-STD-006 Alarm and Event Management | REX |

| Description | Location |
|---|---|
| SPE-00358 Engineering Standard I-SPE-STD-009 Control Systems Topology | REX |
| SPE-00359 Engineering Standard I-SPE-STD-010 Control Systems Tag Naming | REX |
| SPE-00360 Engineering Standard I-SPE-STD-011 Control Systems Testing | REX |
| SPE-00392 WAN Connection Standard Specification | REX |
| SPE-00431 Engineering Standard E-SPE-STD-004 AC Uninterruptable Power Supply (UPS) | REX |
| SPE-00434 Engineering Standard M-SPE-STD-009 Flow Meters | REX |
| SPE-00526 Engineering Standard I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification | REX |
| SPE-00530 Engineering Standard I-SPE-STD-022 Supervisory Control and Data Acquisition (SCADA) Objects | REX |
| TEM-00224 Engineering Standard X-TMP-STD-022 Asset Standards Deviation Request Template | REX |

## 6.1. Codes and Standards

The Contractor shall be responsible for obtaining a copy of and for correctly interpreting and applying the requirements of all relevant legislation, statutory local, state and commonwealth authorities and current applicable Australian Standards and WSAA guidelines. In case there is a conflicting requirement specified in Seqwater standards, Australian standard and/or the legislation, then the conflict shall be brought to the attention of Seqwater Approval and written agreement shall be gained prior to application of requirement.

## 6.2. Australian and International Standards

Unless otherwise noted Australian Standards shall take precedence over International Standards. If there is no applicable Australian Standard relating to the control systems equipment, applicable International Standards (IEC, ISA, IEEE or NEMA) shall apply before the manufacturer's standard.

The relevant Standards include, but are not limited to, the latest publication of the following:

**Table 5: External References and Related Material**

| Standard | Description |
|---|---|
| AS 60529 | Classification of Degrees of Protection Provided by Enclosures for Electrical Equipment |
| AS/CA S008 | Requirements for Customer Cabling Products |
| AS/CA S009 | Installation requirements for customer cabling (Wiring rules) |
| ASM Guidelines | Abnormal Situation Management Guidelines based on "ASM Consortium Guidelines Effective Operator Display Design 2013 standard" |
| AS/NZS 3000:2018 | Electrical installations (known as the Australian/New Zealand Wiring Rules) |
| AS/NZS 3008 | Electrical installations - Selection of cables - Cables for alternating voltages up to and including 0.6/1 kV |
| AS/NZS 3080 | Telecommunications installations - Generic cabling |
| AS/NZS 17799 | Information technology - Security techniques - Code of practice for information security management - Amendment 1:2008 |
| CCM HB29 | Communications Cabling Manual |

| Standard | Description |
|---|---|
| EEMUA 191 | Alarm System Design & Management guidelines |
| IEC 61131-2 | Programmable Controllers – Part 2 Equipment Requirements and Tests |
| IEC 61131-3 | Programmable logic controllers - Part 3: Programming languages |
| IEC 61131-4 | Programmable controllers – Part 4 User Guidelines |
| IEC 61158-2 | Fieldbus for industrial control systems - Part 2: Specification of the bit transmission layer (physical layer) |
| IEEE 1059 | Guide for software verification and validation plans |
| ISA 5.1 | Instrumentation Symbols and Identification |
| ISA S5.2 | Binary Logic Diagrams for Process Operation |
| IS18 | Queensland Government security standard |
| ISA 18.2 | Alarm Management Standard |
| ISA S71.04 | Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants |
| ISA S72.01 | LAN Industrial Data Highway |
| NEMA ICS 1 | General Standards for Industrial Control and Systems |
| NEMA ICS 2-200 | Controllers, Contactors and Overload Relays Rated 600V |
| Trusted Information Sharing Network (TISN) | Critical Infrastructure Resilience Strategy |

# 7. Control Systems Design Criteria

## 7.1. Operating Conditions

All control systems equipment will be required to operate continuously for 24 hours per day, 365 days per year under the conditions detailed below in Table 6.

**Table 6: Site Climatic Conditions**

| Condition | Detail | Value |
|---|---|---|
| Location | South East Queensland | |
| Altitude | Above mean sea level | 0-200 m |
| Humidity | Range (non-condensing) | 10 – 90 % |
| Ambient Temperature (Dry bulb) | Minimum | -5 °C |
| | Typical Maximum | 36°C |
| | Extreme Maximum | 45°C |

## 7.2. Safety in Design

All equipment shall be designed to perform its intended duty safely while unattended. All health and safety risks shall be “designed out” for both the construction and operational phases of control systems as reasonably practicable.

## 7.3. General Requirements

Designs shall be robust and practical, accounting for all constraints. Design services shall be performed as per the requirements and specified in Seqwater X PRO STD 009 Engineering Design Review and Approval procedure.

The following general requirements shall apply:

a. The control systems shall include all equipment required for fully automated operation of the plant or process.

b. The control systems shall be designed to meet the availability requirement as specified in the contract.

c. The control systems shall be capable of restarting automatically following a power supply interruption, without the need for any manual reset or other operator-initiated functions at the site.

## 7.4. Design Life

The design life of control systems equipment shall be in accordance with PLN-00388 Monitoring and Control Systems Asset Class Plan.

## 7.5. Software Licences

The Contractor shall provide the following minimum number of software licenses unless otherwise specified in the scope of work document or any project contract document:

For PLC: One Professional license for PLC programming or equivalent. The Professional license shall include all necessary packages required for PLC programming, simulation, tuning package for PID and advanced controls tuning.

For SCADA: For any new or upgraded licenses, provision shall be made to provide either full SCADA Server license or the required number of SCADA points, whichever is the greater, taking into account the 25% spare requirement. In case of additions to the existing SCADA system, spare SCADA tags may be used where approved by the Principal.

The Principal will allocate the number of SCADA tags available to the project. If the project requires more tags than the number of available spare tags then, the contractor shall provide an upgraded license, including additional spares as per the requirement of upgraded license stated above.

The final 5% or 150 (whichever is the greater) of the total number of licensed SCADA tags are always reserved for emergent maintenance purposes and shall not be consumed by the Project. All licensed software(s) shall be registered in the name of Seqwater (unless the licences are free issued to the Contractor by the Principal).

## 7.6. Temperature Protection and Heat Load Calculations

PLC(s) and SCADA server(s) should be located within an air-conditioned cabinet or building unless specified otherwise in the scope of work document.

All outdoor switchboards, control panels and remote IO cabinet(s) are to be supplied and installed with sun shields.

“Heat loading and ventilation cooling calculations” shall be provided to confirm the amount of heat generated within the cabinet and the amount of heat dissipated. The calculations shall clearly describe whether natural ventilation (through conduction & convention) will be sufficient for heat dissipation or forced ventilation (through suction and/or exhaust fans) is required to dissipate the heat generated within the cabinet.

## 7.7. Control Systems Availability and Redundancy

Control System availability shall be determined using FTA or RBD diagrams and submitted for the Principal’s acceptance. The diagrams shall inform the selection of the model architecture as per I-SPE-STD-009 Control Systems Topology. The control system shall comply with the availability requirements specified in I-SPE-STD-009 Control Systems Topology or as defined in the project functional description whichever is higher.

The following redundancy options for control systems shall be considered in order to meet the availability requirements of the plant:

a. PLC CPU level redundancy

b. SCADA server redundancy

c. IO server redundancy

d. Power supply redundancy

e. Using UPS power as a back-up to mains power

f. Providing functional segregation at remote IO node level – For example IO of duty/standby equipment (or duty/standby process areas) to be allocated to two remote IO nodes.

g. Providing functional segregation at IO module level – For example IO for dosing line A & B to be allocated to separate IO modules

h. Limiting the use of converters (protocol converters, serial to ethernet converters, ethernet to fibre optic converters) – They are the source of single point of failures

i. Use of ring network for field remote IO Layer, PLC Layer and/or SCADA Layer with self-healing capability

Refer to I-SPE-STD-009 Control Systems Topology for network redundancy requirements. Control system redundancy requirements shall also be as detailed in the project functional description.

## 7.8. UPS for Control Systems

UPS design requirements and electrical specifications are described in E SPE STD 001 Electrical Design and Construction standard and E-SPE-STD-004 AC Uninterruptable Power Supply (UPS).

Following are the technical requirements in addition to the requirements listed in E SPE STD 001 standard for selecting UPS for control systems:

a. All PLC cabinet(s) remote IO cabinet(s), network cabinets, switches, SCADA servers, operator stations and telemetry system shall be powered from UPS.

b. All AC UPS supplied SPOs shall be coloured red and labelled 'UPS – Control System Use Only'.

c. The UPS shall be connected to the control systems for monitoring of status.

d. 230 VAC UPS are to be used to power PLC cabinets, SCADA servers and network cabinets installed in air-conditioned environments.

e. 24 VDC UPS shall be used for field mounted remote IO cabinets which are not installed in air-conditioned environment.

f. The fans of the remote IO cabinets shall be excluded from UPS power to optimise sizing of the UPS

g. Three position (UPS / Test / Bypass) external bypass switch shall be provided for all AC UPS with 6 kVA or higher capacity. External Bypass Switch shall be installed such that switch can be operated in any position independent of UPS state.

h. Two position (UPS / Bypass or Mains) external bypass switch shall be provided for all AC UPS having less than 6 kVA capacity.

AC UPS shall provide the following indications and alarms to the control systems:

**Table 7: AC UPS Signals**

| Description of Signal | State 0 | State 1 | Comment |
|---|---|---|---|
| UPS External Bypass Switch UPS | Not UPS | UPS | Applicable for AC UPS with 6 kVA or higher capacity |
| UPS External Bypass Switch Test | Not Test | Test | Applicable for AC UPS with 6 kVA or higher capacity |
| UPS External Bypass Switch Bypass | Not Bypass | Bypass | Applicable for AC UPS with 6 kVA or higher capacity |
| UPS External Bypass Switch UPS | Not UPS | UPS | Applicable for AC UPS with less than 6 kVA capacity |

| Description of Signal | State 0 | State 1 | Comment |
|---|---|---|---|
| UPS On Bypass | Not On Bypass | On Bypass | |
| UPS On Battery | On Battery | Not On Battery | |
| UPS Battery Low | Low | Not Low | |
| UPS Fault | Fault | Normal | |

DC UPS shall provide the following indication and alarms to the control systems:

**Table 8: DC UPS Signals**

| Description of Signal | State 0 | State 1 |
|---|---|---|
| 24V DC UPS Operation Normal | On Battery | Normal |
| 24V DC UPS Buffer Operation Ready | Not Ready | Ready |
| 24V DC UPS Battery Charged > 85% | Not Charged | Charged |

The above indications and alarms can either be hardwired to the PLC or can be made available through UPS communication with PLC via PLC LAN. Acceptable protocols for UPS communication are Modbus TCP/IP or SNMP.

## 7.9. Control Systems Design Deliverables

Control systems design deliverables are project specific and will be listed in SOW for the individual projects.

This section is limited to describing the content of the control systems deliverables. It explains the technical requirements that shall be considered when these documents are produced during the detailed design stage.

### 7.9.1. Control Systems Network Diagram

The *I-SPE-STD-009 Control Systems Topology* standard describes the nominal control systems architectures for Seqwater works relating to new assets and to refurbishment or expansion of existing assets.

This standard shall be referred to produce control systems network diagrams for individual projects. The standard criteria shall also be used to determine the architecture class for the site for which the design is carried out.

All Required Network Drawings shall be produced in accordance with the requirements set out in I-*SPE-STD-009 Control Systems Topology*, *X-PRO-STD-007 Drawing and Spatial Data Standards*, *X-PRO-STD-002 Engineering Drawing Number Procedure* and *X-PRO-STD-014 Drawings Management*.

### 7.9.2. IO List

I-TMP-STD-003 IO List Template shall be referred to produce IO list(s) for a project. The format and the structure of the IO list produced shall the same as I-TMP-STD-003 IO List Template document.

The IO list shall contain the following technical details as a minimum:

a. Names of the PLC tags and SCADA tags along with their description

b. All hardwired signals that are connected to the PLC system

c. OFF state and ON state description for digital signals

d. Engineering range values corresponding to 4mA and 20mA for analog signal

e. Engineering units for analog signals

f. All spare IO channels available in the IO modules

g. Following are the technical requirements for populating IO's in the IO list:

   i. Functional segregation of IO signals considering process flow streams, duty/standby equipment, redundancy, and plant availability requirements. For example, if there are four sedimentation basins and plant availability requirements are to have three out of four sed basins available after any single failure, then segregate signals into separate digital or analog IO module for each sed basin.

   ii. Functional segregation shall be done at remote IO node level as well as IO module level. For example, if there are duty/standby pump arrangements, then IO allocation of duty pump can be done in one remote IO node and IO allocation of standby pump can be done in another remote IO node. However, if the duty pump is taking care of process streams 1, 2 & 3 (for example), then these process stream IO can be further allocated to different IO module within the same remote IO node. This will increase the overall availability of the system.

h. Avoid using abbreviations for numbering of equipment such as "No.", "Nr", "#", etc. Also, avoid using dashes "-" in the equipment names and the word "Command" in digital output signal descriptions.

i. Process signals shall be laid out starting from Slot 1 first and then fill in available spare groups of channels with ancillary signals such as DC UPS monitoring, network switch status, surge diverter status, etc.

j. Projects shall be responsible for providing communication IO tag lists.

I SPE STD 010 Tag Naming Convention standard shall be used to assign PLC and SCADA tags in the IO list.

### 7.9.3. Alarm Design

The alarm design shall comply with I-SPE-STD-006 Monitoring and Control System Alarm and Event Management. The Master Alarm List is the output of alarm Rationalisation process and contains the alarm configuration requirements. The Principal and the Contractor shall use the I-TMP-STD-008 Master Alarm Database Template as the Master Alarm Database.

### 7.9.4. FTA Diagram

Fault tree analysis diagram is used to determine theoretical quantitative availability and reliability of the control systems and communication networks during the design stages of the project. FTA shall consider all the single points of failure in control systems, instrumentation, communication networks and/or electrical system that can result in partial or full loss of production.

The list below describes the control systems equipment that can be a single point of failure. Following single points of failure shall be considered as a minimum requirement to perform FTA calculations:

a. CPU failure

b. CPU rack failure

c. Failure of redundancy module and associated sync cables for redundant CPU systems

d. Failure of communication modules (Example: Profinet module, OPC module etc.)

e. Remote IO node(s) failure

f. Power supply module(s) failure
g. IO module(s) failure – Digital input and output modules and analog input and output modules
h. Remote IO interface module(s) failure
i. Failure of Ethernet and/or Fibre optic switches
j. UPS failure
k. Failure of ring and/or Star network of the control systems
l. SCADA server failure
m. Protocol converter(s) failure
n. Failure of serial to Ethernet converters and/or Ethernet to Fibre optic converters
o. FOBOT failure
p. Radio Modems (wireless, 4G/5G)
q. Critical instrumentation failure such as main process flowmeters, e.g., raw water flowmeters, reservoir outlet main flowmeters, etc. used for control of chemical dosing.

In addition to FTA, RBD is also an acceptable tool to perform quantitative availability calculations of the control systems.

MTBF data shall be used from the manufacturer of PLC and SCADA system while performing availability & reliability calculations using FTA or RBD diagram(s). Evidence of the source for MTBF data used in the availability calculations shall be provided with the theoretical calculations.

The Principal will provide MTTR data for the respective site, which shall then be used to calculate annualised availability of control systems for that respective site.

### 7.9.5. CPU Loading & Memory Usage Calculations

PLC CPU loading, and memory usage calculations shall be submitted during the detailed design for any project or any modifications to a PLC.

The calculation shall show the CPU scan time in milliseconds achievable for the PLC by considering the following loads:

a. All the hardwired IO's connected to the PLC
b. Soft IO's (data coming from VSD, power meters, numerical relays etc.)
c. Communication load (PLC to SCADA communication, PLC to PLC peer communication etc.)
d. Control logic residing inside the PLC including all open loop controls, closed loop controls and sequence logic.

CPU loading calculations shall clearly specify the % CPU spare capacity available after executing the above loads in the PLC CPU. PLC shall be selected such that CPU loading shall not exceed more than 50% of the rated capacity by implementing all the hardwired IO, communication interfaces and the logic program inside the CPU.

CPU memory calculations shall also consider the above loads. The memory calculations shall show memory usage for both code as well as data. The memory calculations shall clearly specify % spare memory available after executing the above loads in the PLC. Memory utilisation of the PLC should not exceed 50% of rated capacity.

Evidence of the source for memory usage and CPU loading data used in the calculations shall be provided with the theoretical calculations.

### 7.9.6. PLC Structuring and Addressing Register Document

PLC structuring and addressing register document shall be submitted as a part of Functional Description Part B to the Principal before the start of PLC and SCADA programming.

The document shall describe the following technical details as a minimum:

a. Symbolic names used in the PLC code for all the function blocks, derived function blocks, datablocks, datatypes, derived data types and memory blocks

b. Name, number, and description of the Seqwater standard library blocks to be used in the PLC code

c. Name, number and description of the instantiated function and function blocks

d. Name, number and description of the function and function blocks used for sequence logic (sequential start-up and sequential shut-down sequences)

e. Name, number and description of the function and function blocks used for communication logic (peer to peer communication, PLC to SCADA communication blocks, VSD communication blocks etc.)

f. Name, number and description of the function and function blocks used for diagnostics and troubleshooting

g. Start and end addresses of the physical IO (digital inputs, digital output, analog input and analog output addresses)

h. Start and end address for datablocks, memory blocks, datatypes, derived datatypes, function blocks and derived function blocks

i. Start and end addresses for fieldbus device interfaces using communication protocols.

Contractor to ensure that there will be no clash of addresses in the new PLC program and existing PLC code. The document will also be reviewed to determine whether all the allocated addresses are required as per the functional and/or process needs of the plant.

### 7.9.7. IP Register

IP register document shall contain the following technical details as a minimum:

a. Reserved IP addresses

b. IP addresses for SCADA servers

c. IP addresses for SCADA workstations and HMI’s

d. IP addresses for PLC and remote IO nodes

e. IP addresses for switches

f. IP addresses for gateways, power monitors and miscellaneous equipment

g. IP addresses for drives

h. IP addresses for printers, terminal servers, wireless gateways, and other ancillary equipment.

Principal shall provide the range of IP addresses for individual projects. However, it shall be the responsibility of Contractor to populate the IP register with IP addresses for individual equipment. As a part of Functional Description Part B, the IP address register shall be provided by the contractor.

### 7.9.8. Functional Descriptions

The structure and requirements for functional descriptions is described in B-SPE-STD-005 Functional Description Documentation. The following is a summary relevant to this standard:

- Functional Descriptions are structured as a Part A and Part B.
- Both Part A and B are controlled documents and maintained as current through the life of the asset. Part B is a point in time document created to facilitate the implementation of control system.
- Part A describes the process design. Key content includes process envelops, normal and abnormal operation, automated protections such as interlocking and process hierarchy. It should come complete with piping and instrumentation diagrams (P&IDs) and cause and effect matrix.
- Part B transfers the process design in Part A into a control system design suitable to facilitate implementation by a systems integrator. The process hierarchy is presented as a control systems hierarchy made up from Seqwater's blocks library. Details on sequencing, calculations, scaling, control systems fault, interlocking and the like are further expanded to facilitate implementation. The master alarms list should be created at this same time.
- Part B is also focused on SCADA configuration and communications protocols. The document is a point in time document as once the control system is implemented, change control is facilitated on the implementation of changes.

### 7.9.9. Fibre Optic Layout and Termination Drawing

The Fibre Optic Layout and Termination Drawing shall contain the following technical details as a minimum:

a. Layout describing the locations of the FOBOT for remote IO network, PLC Layer and SCADA Layer network.

b. Termination details and patching details of fibre optic cables going IN and coming OUT from each individual FOBOT.

c. In case of a fibre optic ring network, the drawing shall clearly layout the physical ring, it's associated nodes along and the fibre optic switches and FOBOT used to complete the ring.

d. The type of fibre optic cable (single mode or multi-mode), the number of cores of individual fibre optic cables and spare cores of cables shall be clearly described on the fibre optic layout and termination drawing.

e. All Required Drawings shall be produced in accordance with the requirements set out in I-SPE-STD-009 Control Systems Topology, X-PRO-STD-007 Drawing and Spatial Data Standards, X-PRO-STD-002 Engineering Drawing Number Procedure and X-PRO-STD-014 Drawings Management.

The supplied communication equipment shall be labelled.

# 8. Standard Functionality

## 8.1. Hierarchal Philosophy

The process hierarchy, which is documented in functional description Part A, is used to inform the control system hierarchy, which are documented in functional description Part B. Processes are structured as process groups which consist of equipment and / or blocks that must operate together to achieve a process objective or outcome. The control systems hierarchy assembles code blocks from Seqwater's library into logical groupings. The following philosophies shall be applied:

- A group controller (called a supervisory controller, I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification) functions to permit lower hierarchy equipment to operate. There can be layering of supervisory controllers in a design.
- Control is at the lowest level of the hierarchy. Interlocking and permissives are preferred at this lowest level. Once a supervisory controller allows operation, the equipment will function protected by its own interlocking / permissives.
- Interlocking at a group controller level can be used where it is practical to do so. This has been used in Seqwater where interlocking from one process group to another is required and the whole process group would be required to stop operation on a condition. There should not be many of these types of these scenarios.
- Simple sequencing should be performed using interlocks, not Sequencer blocks of code. Sequencer blocks are used for complex sequence processes such as filter operation, see Section 8.10 for further details on sequencing.

This philosophy applies even with more advanced process control. Additional controllers or duty or sequencing or otherwise can be incorporated in the hierarchy under a group controller.

## 8.2. Equipment Controls Modes

Control systems shall support three distinct modes of control for equipment as outlined below.

### 8.2.1. Local Mode

The equipment can only be operated from the field independent of the control systems. Operation is free of control systems interlocks but retains hardwired equipment protection and / or hardwired interlocking. In this mode, local Start/Stop is done via local hardwired (control system bypassed) pushbuttons or through equipment HMIs (e.g., VSD keypad).

The "Local/Remote" switch in the field shall be in "Local" position for this mode to be active.

DOL/ VSD with Local controls will only be used after formal risk assessment is carried out for the specific applications and the Principal has approved their use. Variable speed drives and soft starters will have Local mode available via their respective keypads, however this can be disabled, if required, by drive configuration.

Due to increasing cyber security threats, the ability to operate equipment or groups of equipment or even whole facility in local mode shall assessed in the design phase, against the risks associated with being able to operate equipment independent of the control system.

Approval from the Principal is required to include the Local control mode of equipment or process groups.

### 8.2.2. Remote Manual Mode

The equipment can only be operated manually (typical minimum functionality including start/stop and change setpoints) remotely via the control system.

If installed, the “Local/Remote” switch in the field shall be in “Remote” position for this mode to be active. Control System Interlocking shall be active in this mode, see Section 8.8 for details on interlocking.

### 8.2.3. Remote Auto Mode

The equipment shall operate automatically, unless otherwise stated differently in Functional Description A/B specification. Automatic operation shall be sufficient to maintain the process in normal operation bounds and provide operators information to take responsive or remediation actions. It shall include capability such as start / stop, interlocking, sequencing, disturbance control, alarming, and the like.

## 8.3. Equipment Functions

Equipment (drives, valves, actuators etc.) shall have disable and maintenance functions. It may have a force function as well. All instruments (transmitters, water quality analysers etc.) shall have instrument calibration function, which is a specific version of the force function. Additional functions may be specified in the design documentation, such as functional descriptions.

### 8.3.1. Disable Function

Disable function is intended for use when the operator does not want to use equipment in the process via remote control. Disable will force the equipment to reach its fail-safe state (OFF state in most cases) and equipment will become unavailable to operate from SCADA. The equipment will remain energised so that it can be readily brought back into operation by enabling it.

The disable function is applicable for process areas (filters, chemical dosing etc.) as well as individual equipment.

When disabled, all alarms are masked. Hardware Interlocks will still be active in the field, but any alarming associated with the hardware interlocks will be masked, and the operator will become aware of these when the equipment is enabled. Specific status indication whilst disabled (e.g., valve position) may be included in the design for safe operation so that the operator will make an informed decision prior to enabling.

Equipment can be disabled only in Remote Auto or Remote Manual modes. Local operation is still possible even if the function is active, as disabled is only functionally relevant to the remote modes.

The disable function can be excluded for specific process critical equipment if determined in the design and with Principal approval.

### 8.3.2. Maintenance Function

The maintenance function can be configured for use. The maintenance function may be used to bridge code, such as interlocks or alarms, for specific equipment. The use of maintenance function should be confined to allow abnormal operation for known conditions for a defined period of time. All use of the maintenance function is subject to risk analysis and higher-level privileges above operator level, see Section 12.2.1

Requirement of the maintenance function for individual equipment shall be specified in functional description (Part A or B).

### 8.3.3. Force Function

Force function provides for overwriting a variable via SCADA. The function can be applied for digital and analogue signals. Key requirements for forcing include:

- Indication on SCADA to the operator that a variable is being forced.
- Alarms are to remain active, but these shall use the forced value, not the actual process value.
- Logging of the force function on SCADA.
- A configurable time out with automatic reset of the force function.

For process critical equipment, the design should consider whether or not to allow for the force function. If it is included in the design, a maximum time period must be decided during the design phase and configured for the equipment. Appropriate privileges to put equipment into force from SCADA should be decided in the design phase, based on a risk assessment.

### 8.3.4. Instrument Calibration

Instrument calibration is a specific application of the force function. The intent is to allow water quality analysers to be taken out of service for calibration.

Alarms, trips, and interlocks remain active for the forced value during the calibration function. Both the process value (forced) and the real value shall be displayed and trended during the force function duration. The trend shall also display that the Analogue Input is being forced. The display and trend will be used to indicate to the operator what the variable will return to when the force function is removed.

The use of the force function must be logged on SCADA. An operator should be able to see a summary of all devices in calibrate mode, on SCADA.

There is a risk that during the force time, a process upset occurs and a CCP alarm could be missed. Therefore, force must have a time out with automatic reset. The time out period has an upper limit, which cannot be altered by an operator. An operator can enter a time out value in SCADA, up to this limit.

When an Analogue Input is set to force a timer shall commence and the remaining time shall be displayed on SCADA. Once timed out, the force function shall automatically reset. Force function timers can be restarted while timing out by reselecting force. The force function can be individually turned off at any time.

## 8.4. Group Controller

The minimum functionality of a group controller, as described in Section 8.1, is to provide for operation of equipment and / or blocks within a process group[1]. The group controller (via supervisory controller, refer toI-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification ) is otherwise configurable to meet the requirements contained in a design. As this block has scope for variances in configuration, Seqwater shall be required to approve the proposed configuration for all group controllers. Documentation of the functional

[1] I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification uses the terminology ‘service’ to describe the function whereby an equipment / block receives an output that allows it to operate with interlocking / permissives. In practice the output can be to change the mode of the equipment to AUTO to allow it to operate. Note that the supervisory controller can be used for monitoring only but in this context, it would not be defined as a group controller.

requirements shall be included in Functional Descriptions Part A and B and must be provided as support for the adopted configuration.

The following functionality has been successfully used within Seqwater and may be included in a design:

### 8.4.1. Mode or Function Changes

For operator efficiency, the group controller can be configured to take the following actions for all or some of the equipment and / or blocks within a process group:

- Disable
- Auto mode
- Reset.

The design of the group controller shall consider the risks associated with including or excluding the functionality as noted above.

An example might be the requirement for an operator to place each equipment into disable one by one in a process group rather than a single group disable balanced against the potential for inadvertent use.

### 8.4.2. Monitoring

Monitoring can be configured and would be case specific and outlined in the design. However, common functionality includes:

- Display and alarm that a process group equipment is in fault.
- Process group equipment is available.
- Equipment is running.

This type of monitoring should not be applied as a norm to all equipment but be considered in the design process for key equipment conditions.

### 8.4.3. Shutdown

Shutdown is used to stop the process. A group controller shutdown could be configured to trigger with an operator initiation and / or a configured condition(s) being achieved. A shutdown may be configured to start a sequence or steps through to a process stop. Further details on shutdown functionality are included in Section 8.8.

### 8.4.4. Interlocking

Interlocking at the group control level may be included in the design. These have been used in Seqwater for inputs external to the group control which is required to stop all equipment that is part of the group control.

In the standard , I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification , the interlock is the crash stop functionality. These should be mapped to the equipment trip interlock. Group control interlocks should be considered to have the same concept as the trip interlocking as noted in further detail in Section 8.8.

## 8.5. Closed Loop Control (including PID Standard Functionality)

In Seqwater, the philosophy for closed loop control configuration has been to maintain a simple PID controller block (I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification ) with the functionality as noted

below. Additional functionality, e.g., cascade or indirect ratio control, is achieved by tying together PID controller blocks, additional calculation blocks or bespoke code as required by the design.

A PID controller should be considered as operating when all equipment that is part of the control loop is in remote auto mode. If the PID is used to execute closed loop control, then the following functionality are applicable:

1. **Manual:** the operator sets the Control Output of the PID controller directly. Manual mode allows the tracking of PID output. To remove confusion, the equipment that is part of the control loop will still be in remote auto mode, this 'manual' mode is that of the PID controller.
2. **Auto:** the operator sets the setpoint. The setpoint may be that of the PID loop or calculated and input to the PID. The PID controller is enabled in the PLC logic and calculates the control output based on the error (difference between the process value and the setpoint value) and the tuning parameters. Auto mode does not allow the tracking of PID output.
3. **Feedforward:** It is the additive or multiplicative manipulation of the PID controller Control Output. Typically, this function is used to help minimise measurable disturbances (e.g., main flow paced calculation for dosing pump output with a water quality analysis feedforward input in a chemical dosing arrangement). Feedforward can be performed with optional trim functionality. Trim can be used to set a limits range on the Control Output.

All PID Controllers shall be executed with a scan rate of 200ms unless agreed otherwise with Seqwater approval.

If PID is selected in remote manual mode, then "PID controller mode alarm" shall be generated after 5 minutes.

There is a risk of PID being left in manual inadvertently. This risk shall require assessment in the design and risk mitigations included. In Seqwater's installations an alarm after a definable time has been successfully used.

When selected in Auto or Feedforward controller mode, each PID Controller will feature the following alarms:

- Deviation alarm (SP - PV) > 5% of setpoint for 60 secs.
- Output High > 90%, for 60 secs.

The alarm limits given above are indicative only, the project specific values shall be detailed in the project's functional description.

Use of hardwired single loop controllers shall be avoided.

## 8.6. States/Status

States or Status can apply to all levels of the hierarchy. A state will reflect the status of the equipment or process group. Some states include, available, online, offline, starting, running, stopping, stopped and faulted. There may be procedures that are active in transferring from one state to another. This section outlines key states used in Seqwater and the definition of these states. Each design may have additional states / status which must be outlined in the functional description documentation.

### 8.6.1. Available

Process groups or equipment are in the available state when all conditions are satisfied that allow it to be operated from the control system. It would be either operating or waiting upon the command from a higher hierarchy to operate.

As a philosophy, 'available' is when everything from the field associated with the equipment is energised, healthy or not in fault such that it could operate. There is one logic consideration towards 'available' and that is the equipment is enabled (not disabled).

Available will equally apply to group controllers and other higher hierarchy blocks, controllers and / or group controls. However, the requirement for all equipment in a process group to be enabled (not disabled) may be unsuitable and alternatively outlined in the design. For example, a pump station may be configured so that one of multiple pumps can be disabled for maintenance purposes while the rest of the pump station can operate.

### 8.6.2. Fault

There are two types of faults that consolidate to represent a single operator representation of an equipment in 'fault', these are:

1. Equipment fault: aligns directly with the hardware interlocks described further in Section 8.8.
2. Logic based derived fault: these are additional faults that prevent continued operation. An example is a valve failing to make limit within the allowable time.

A fault status is conceptual and exists purely to support operator management of the process. A fault must be presented such that an operator can troubleshoot to find what is the cause of the fault.

### 8.6.3. Filter Process Group

Filter process group is common in Seqwater and to achieve consistency key mandatory states include the following:

#### 8.6.3.1. Online

Equipment is in Online state if it has successfully completed all the sequence steps to be Online. A filter may need to complete Fill, Reject and Online sequences in order to reach to Online state. In Online state Group Enabled shall be in "On" state.

#### 8.6.3.2. Offline

Equipment is in Offline state if it has successfully completed all the sequence steps to be Offline or all items of equipment have been manually operated to the Offline state, e.g., all valves associated with a filter are fully closed. In Online state Group Enabled shall be in "OFF" state.

## 8.7. Setpoints and Parameters

The control systems are designed to operate using a combination of SCADA configurable Setpoints and PLC parameters.

PLC parameters are not accessible from SCADA. They are hard coded inside the PLC program. All PLC parameters shall be specified in the functional description part B.

SCADA configuration setpoints are process setpoints, control setpoints or Critical Control Point (CCP) parameters.

Differing levels of authority shall exist for managing change to SCADA configurable Setpoints. Refer to Table 11: SCADA Security Privilege Levels for Plant SCADA Table 12: SCADA User Roles for Plant SCADA that explain SCADA security levels. All SCADA setpoints shall be specified in the functional description part B.

## 8.8. Interlocks and Permissive

The schematic below in Figure 1 shows a representation of a simple two variable process envelope. The schematic represents:

- **Operating Envelope:** In this operation the process would function within bounds that can be considered normal operation. The designer of the process would have provided for all operating windows representing different known conditions that the process would be required to function. Logic used to manipulate the process within these operating windows are called 'process permissives'. If the process deviates outside the bounds of operating windows but still within the operating envelope, typically an alarm would be the adopted risk mitigation, requiring operator intervention. Otherwise, the process should operate in this envelope with minimal operator intervention.
- **Design Envelope:** The design envelope contains the operating envelope and a margin. Interlocks are applied within the margin to prevent excursion of the process beyond design. There may also be hardware controls (e.g., pressure relief valves) in addition to automated controls. Interlocks should typically trip the process to a safe state requiring operator intervention and assessment prior to bringing the process back online.
- **Beyond Design Envelope:** The process should never deviate to beyond the design envelope as this would be an undesirable or unsafe state.

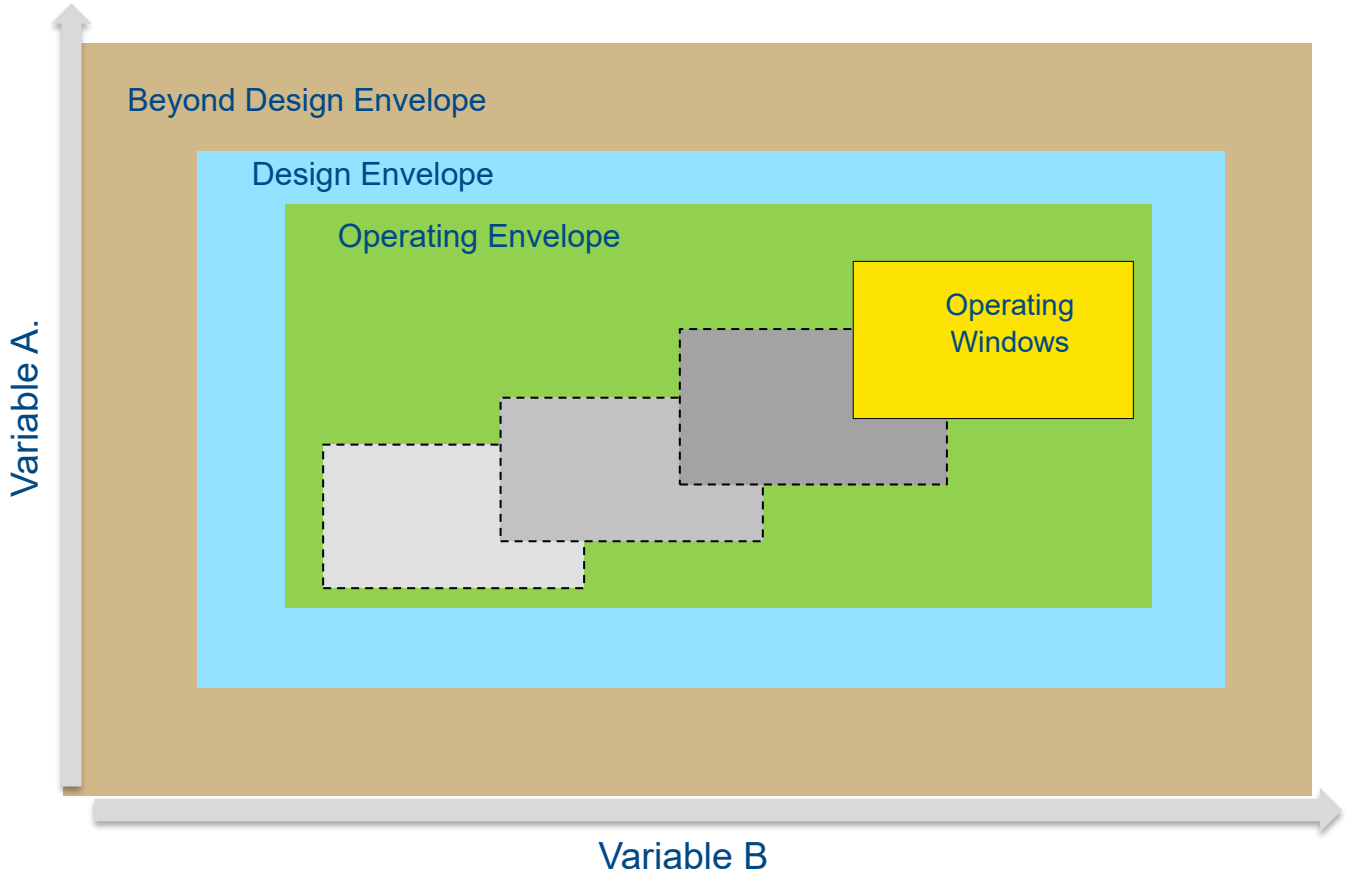



**Figure 1: Process envelopes schematic**

Detailed definitions of controls process management, applied in Seqwater, are:

### 8.8.1. Hardware Interlocks

These provide safety/protective functions (e.g., emergency stop, thermal overload); these interlocks need to be healthy for the equipment to operate in any control mode (Local, Remote Manual as well as in Remote Automatic control modes). This includes what is typically a generic fault within the device. All these errors or faults are presented as a grouping of 'equipment fault'. Sub-equipment (e.g., oil level low that trips a pump) also fit into this grouping. Examples that could consolidate to a hardware interlock include:

a. Loss of control power
b. Loss of mains power
c. High temperature
d. Oil in water in a pump
e. High torque in a valve
f. E-Stop active
g. Isolator open
h. Power factor high / low

Additionally, safety trips (e.g., high level in chemical storage tank interlocks a delivery power socket) that are hardwired to protect against a hazard in all control modes is included in this definition.

### 8.8.2. Trip Interlocks

Trip Interlocks provide protection against undesirable operating conditions (e.g., low-level switch on a tank that a pump is drawing from). These protect the process from excursion towards design limits. These interlocks need to be healthy for Remote Auto and Remote Manual control modes at both an equipment and a process group level. At the process group, trip interlock is achieved with the crash stop interlocking function, as noted in Section 8.4.4.

These interlocks will not be active in Local control mode. In SCADA Interlocks shall be shown as "ON" when the interlocking state is active and "OFF" when there is no interlocking i.e., when the conditions are healthy or normal. An override process can be used to manage interlocks to provide for abnormal operation requirements.

### 8.8.3. Process Permissive

Process permissives allow for normal operation within an operating window. These functions are used in Remote Auto mode but not for Remote Manual or Local control modes. An example of using process permissives is implementation of a simple on/off logic, such as start / stop a pump based on high / low level set points.

### 8.8.4. Start Permissive

Start Permissives are conditions that shall be met before equipment can be started in Remote Auto control mode.

### 8.8.5. Group Control Shutdown

A group control shutdown should be considered as a means to stop a process group as part of normal operation, i.e., within the operating window. The function is configurable so can be used to stop a process when equipment is in any remote mode, but auto mode is the standard implementation. It can be used for a normal shutdown at the bounds of the operating window, with an appropriate margin.

The types of interlocks available as per each control mode and equipment functions are summarised below:

**Table 9: Interlocks & Permissives compared to Control Modes and Equipment Functions**

| Interlocks | Control Modes and Equipment Functions | | | | |
|---|---|---|---|---|---|
| | Disabled Function | Maintenance Function | Local Control Mode | Remote Manual Control Mode | Remote Automatic Control Mode |
| Hardware Interlock | ✓ | ✓ | ✓ | ✓ | ✓ |
| Trip Interlocks | | configurable | | ✓ | ✓ |
| Start Permissive | | | | | ✓ |
| Process Permissive | | | | | ✓ |
| Group Control Shutdown | | | | configurable | ✓ |

## 8.9. Control Systems Fault

The control systems shall be designed to fail safely. The occurrence of any abnormal condition(s) within the control systems that affects *reliable, orderly, and safe operation* shall result in the automatic controlled shutdown of the affected area of the plant or the entire plant irrespective of the stage of the plant control sequence. The specific conditions that result in shutdown shall be determined through the design process considering the criteria of *reliable, orderly, and safe operation*.

During the design process if a control loop is identified as SIL rated, then the design shall consider use of Safety PLC systems in consultation with the Principal. However, most of the control loops in various units in Seqwater are non SIL rated loops, hence a non-safety system is predominantly used as per *I-SPE-LST-001 Prescribed Equipment List*. The design shall adhere to fail safe requirement through the configuration of the control system devices, or the logic developed shall be fail safe. Any control signal loss due to communication failure shall be designed to be fail safe.

Note that the requirements in this section should be considered to extend to the fail-safe provisions included in the standard library for all equipment. For further details refer to I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification

In the case of an abnormal event(s), the system shall be designed to be fail safe with all outputs returning to de-energised safe state.

A safe condition of control systems is one that involves no hazard to personnel and no unnecessary operation of plant or equipment.

## 8.10. Sequence Control

A sequence will consist of a group of one or more inter-related equipment which together carry out a particular process. Automatic sequence logic shall be provided in the control systems to control and monitor each sequence. The auto sequence logic will:

a. Control and monitor the ordered start-up or shutdown of each item in the sequence in accordance with a predefined program and designated process and time requirements

b. Whilst the sequence is running, continue to monitor each item and provide start/stop control and/or open/close control(s) for individual equipment in accordance with predefined process and time requirements.

c. The status of various steps in the sequence shall be displayed on SCADA system.

## 8.11. Duty/Assist/Standby Control

Definitions of equipment duty / assist / standby are as below:

**Table 10: Duty Assist Standby Sequence**

| | |
|---|---|
| **Duty** | Duty control is used when the process requirement is able to be provided by only one pump operating at any given time. |
| **Assist** | Assist is used when the process requirement is not able to be provided by the Duty device alone and requires the operation of an assist device to share the load of the process. In some cases, there may be a need for multiple Assist devices to meet the process requirements. |
| **Standby** | The Standby device is ready to become the Duty or Assist if either of these running devices becomes unavailable. The standby device can be shared by multiple duty/Assist devices |

Duty/assist/standby control(s) are only available in the remote automatic control mode. If the duty selected device is unavailable, then the standby equipment is to become duty. If no equipment is available to run in duty, then the process unit will fault.

## 8.12. Duty Rotation

The duty shall be operator selectable between fixed duty, time-based duty, or auto duty.

In fixed duty, the equipment selected for duty will operate if available. In time-based duty, the online equipment automatically rotates to the standby equipment, if available, after an elapsed time. In Auto duty, the duty rotation happens each time the process unit goes offline. This shall be achieved via a single SCADA selection box.

The rules as per the sections below shall apply for duty rotation of equipment.

### 8.12.1. Duty Tank Rotation

Duty selection between fixed / auto tank rotation:

The operator can select a fixed tank duty order that defines which tank to dose from and return to. If fixed duty is selected and the duty tank reaches a low level, then change to the next available tank in duty order.

*Automatic tank rotation shall be a part of design. Rotating duty tank on a time basis should be considered. As fit for purpose for the tank(s), the influence of chemical delivery size and frequency, water age, solids deposition and other factors shall be considered in the design.*

The tank rotation time shall be adjustable via SCADA HMI and the time remaining until the next tank rotation is also displayed in SCADA.

### 8.12.2. Duty Pump Rotation

Duty selection for fixed / auto rotation of the pair of pumps: If fixed duty is selected, i.e., 1/2 or 2/1, then the duty pump is operated, if it is available. If the duty pump becomes unavailable, then the standby pump, if available, is operated.

If the standby pump is operating and the duty pump becomes available again, then the duty changeover will happen from standby pump to duty pump in the fixed duty rotation. However, in auto duty rotation, the standby pump will keep operating until the standby pump goes offline.

If time-based rotation is selected, then the online pump automatically rotates to the standby pump, if available after an elapsed time (minutes).

The pump rotation time shall be adjustable via SCADA HMI and the time remaining until the next pump rotation is also displayed in SCADA.

This same philosophy should be extended to process groups with multiple duty pumps and a common standby. The goal in these multiple pump process groups will be to even the run hours of each unit. The design of multiple pump process groups duty rotation shall be described in the functional description parts A and B.

### 8.12.3. Duty Dosing Line Rotation

Duty selection for fixed / auto rotation for each pair of dosing lines: If fixed duty, (i.e., A/B or B/A), cyclic duty or dual duty is selected, then the duty dosing line is operated, if it is available.

If the duty line becomes unavailable, then the standby line, if available, is operated.

If auto dosing line rotation is selected, then the standby dosing line, if available, automatically rotates to become the duty line after an elapsed time (minutes).

The dosing line rotation time shall be adjustable via SCADA HMI and the time remaining until the next dosing line rotation is also displayed in SCADA.

## 8.13. OIP Functionality

Following design considerations shall apply whenever design identifies the requirement of OIPs:

a. OIPs should be limited to the functionality equivalent to push buttons i.e., supporting local mode only. Some status display is acceptable. Push buttons, as opposed to a touch screen, are permissible.

b. Additional functionality e.g., alarming, set points, control, is preferably achieved via a SCADA client.

c. Where the process requires multiple sites to operate in an integrated system, communication reliability will be achieved via redundancy, multiple servers, temporary client to server or other options depending on SCADA product. It is not preferred to provide for automatic operation via an OIP at multiple sites. A cost and risk analysis shall be carried out.

d. Consult the Principal for suitability of the OIP.

OIP design should otherwise comply with the requirements noted in this Standard.

# 9. PLC Hardware

## 9.1. PLC CPU and Components

The PLC hardware selection will be as per I-LST-STD-001 and as per Class selection in I-SPE-STD-009.

The PLC make and model shall be approved by the Principal during the detailed design stage.

## 9.2. PLC Communication Modules

PLCs shall be capable of interfacing to devices using communication interface modules or through an on-board communication port on the CPU. Permitted communications protocols are listed in Table 32: Network communication protocols.

## 9.3. CPU Loading and Memory Reserve Capacity

PLC CPU loading shall not exceed more than 50% of the rated capacity by implementing all the hardwired IO, communication interfaces and the logic program inside the CPU.

CPU scan time shall not exceed 200 milliseconds by implementing all the hardwired IO, soft tags, communication interfaces and the PLC program. Memory utilisation of the PLC shall be calculated by considering memory usage for all the hardwired IO, soft tags, communication interfaces and the PLC program. Memory utilisation of the PLC should not exceed 50% of rated capacity.

## 9.4. Time Synchronisation within Control Systems

Project design shall ensure that PLC time is synchronised with the site SCADA system.

The project design shall also allow for higher speed time synchronisation if required by the Control systems or with any specific equipment of the control systems (like Numerical relays). The requirement of higher speed time synchronisation (if any) will be approved by the Principal during the detailed design stage.

## 9.5. PLC Redundancy

The following technical requirements shall be followed when using a redundant PLC:

a. Redundant controllers shall have physical separation from each other. Redundant PLC racks shall be installed in separate control systems cabinets or in physically separated and isolated cells within the same cabinet.

b. Redundant PLCs shall not be installed on shared backplane

c. Redundant PLCs shall not be fed from single power supply source

d. Redundant PLCs shall utilise hot standby configuration with bump-less switchover between primary and secondary controllers and vice-versa.

e. Both CPUs of the redundant PLC shall execute the same user program. The system shall run in a master-standby arrangement and is required to provide bump-less transfer to the standby unit in events including, but not limited to:

    i. CPU failure

    ii. CPU rack failure

iii. IO communications fault

iv. Local Area Network communication fault

v. Communications Fault

vi. Power Supply module failure

f. Remote IO nodes and all the field connected equipment and IO's shall seamlessly switchover to the new master controller during switchover of PLCs in a redundant mode without interrupting the plant operation.

g. The Redundant PLC setup should be such that in no circumstances both Primary and Secondary PLC shall be offline.

## 9.6. PLC IO Terminal Arrangement

The input and output modules are to be provided with detachable prewired terminal blocks (or similar) to facilitate module exchange without interference to the panel wiring.

## 9.7. PLC Spare Capacity

A minimum of 25% installed spare IO shall be provided per IO panel location. 25% installed spare IO shall be for each module type (i.e., Digital input and output modules and Analog input and output modules).

All the spare IO shall be connected to the terminals. There shall be two spare slots in every PLC rack and/or remote IO node for future usage. The PLC enclosure shall be designed to provide spare space of 25% of installed terminals space.

In case of brown field minor changes (where the total requirement to add hardwired IO is less than 32 to the existing PLC system), PLC spare IO's can be used in case they are available. Principal will perform the IO allocation of the spare PLC cards and provide approval to use the spare capacity of the control systems for the minor works.

## 9.8. PLC Enclosures

All PLC components specified in Section 9.1 shall be installed in enclosures in accordance with Seqwater standard "E SPE STD 001 Electrical Design and Construction".

All Required Drawings shall be produced in accordance with the requirements set out in 'E-SPE-STD-001 – Electrical Design and Construction', 'X-PRO-STD-007 – Drawing and Spatial Data Standards', X-PRO-STD-002 – Engineering Drawing Number Procedure' and X-PRO-STD-014 – Drawings Management'.

Additionally, the following requirements specific to PLC enclosures and cabling shall be adhered to:

### 9.8.1. PLC Enclosures

Adding Low voltage to the PLC Cabinet / Marshalling requires additionally permits and regulatory and safety considerations, as below:

a. All PLC equipment shall be installed in accordance with its manufacturer's recommendations. Equipment spacing shall be at least to its manufacturer's minimum requirements.

b. Adequate cooling shall be provided for all PLC equipment.

c. 24VDC powered enclosure fan shall be used. PLC cabinet shall have temperature monitoring with alarm at 80% of PLC manufacturer's recommended maximum operating temperature.

d. Only ELV equipment/s shall be allowed in PLC cabinets and PLC marshalling cabinets..230VAC shall not be included within a 24VDC cabinet Instructions in E-SPE-STD-001 (SPE-00352) section 'Switchboard Internal Wiring' shall be followed. Extra Low Voltage green label to be fixed on the front of new panel, as per PRO-00006.

e. 24VDC LED lights shall be used for the enclosure illumination.

f. PLC cabinets shall be installed in sealed, air-conditioned environment unless approved by Seqwater.

g. Remote IO nodes can exist in PLC enclosures containing standalone or redundant controller's racks provided space limitation is not an issue.

h. Remote IO nodes can be installed within switchboard cabinets or at a field location which are not airconditioned provided heat load calculations are conducted and appropriate natural and/or forced ventilation arrangements are considered in the design.

i. Rooms housing redundant controller cabinets shall be fitted with dual 100% cooling capacity rated air-conditioner units.

j. If forced ventilation is required in redundant controller, standalone controller, or IO marshalling cabinets, then dual 100% capacity rated fans shall be installed in these cabinets

k. The PLC enclosure (containing either controller racks or remote IO nodes) shall have unimpeded space of at least 600mm with doors in any position.

### 9.8.2. PLC Cabling

PLC cabling shall be in accordance with requirements specified in E-SPE-STD-001 Electrical design & construction standard. Following additional requirements shall also be considered for PLC cabling:

a. 230V wiring shall be excluded from all IO marshalling terminal sections. For brownfield sites, where this wiring may currently exist, shrouding and clear labelling shall occur on all equipment above 50VAC or 120VDC for existing systems.

b. All IO modules and the individual IO Channels will be fuse protected.

c. Optical fibre terminations and FOBOTs shall be at the uppermost part of the cabinet.

d. . No side wall mounting of gear tray/s or devices shall be allowed

e. The bending radius of any cable shall not be less than the minimum bending radius recommended by the cable manufacturer or 6 times the cable diameter whichever is more.

f. PVC ducts shall be sized such that their cross-sectional area utilisation factor does not exceed 60% and should have extra space to align with the 25% IO growth requirement.

g. IO module terminal blocks shall be spring clamp terminal type.

h. Wiring on the "field side" of IO marshalling terminals shall be coloured as defined in E-SPE-STD-001 Electrical Design and Construction.

i. Sheathing shall be provided inside and to the top, of the duct, allowing a maximum of 300mm of individual cores being provided each PLC card.

j. Sleeves shall be sized so that they are in the manufacturer's recommended range of core OD and be 15mm long as standard, unless longer lengths are specifically required.

k. All cables shall be terminated with insulated bootlace ferrules in accordance with 'E-SPE-STD-001 Electrical Design and Construction'

l. A DIN rail shall be a single, continuous length extending the full length between wiring ducts.

m. Where marshalling zones are provided, a single piece of cable tray mesh shall be installed at the rear of the zone, to accommodate cables within this zone.

n. Terminals shall not be placed within Marshalling zones

o. All terminal types shall be fitted onto DIN rail with the opening downwards.

p. Terminals with hinged components, such as fuse and disconnect terminals, shall be hinged on the RHS unless advised by the Principal.

q. IO marshalling terminals shall be grouped per IO module and these groups of terminals are separated by an end bracket and a label bracket which is labelled with the associated controller rack and slot number.

r. Dual level terminals shall be used for marshalling Digital IO wiring. The upper-level terminals shall be odd numbered and the lower-level terminals shall be even numbered.

s. All digital input module terminal groups shall be together on the left-hand DIN rail(s) and all digital output module terminal groups shall be together on a different DIN rail, if space permits. All analog input module terminal groups shall be on another DIN rail with analog output module terminal groups below them.

t. The exposed end terminal shall be blanked off with an end plate.

u. Only one end bracket shall be used to separate each group of IO marshalling terminals.

# 10. PLC Software

## 10.1. PLC Software Requirements

The PLC programming software shall be selected as per I-LST-STD-001 Control Systems Prescribed Equipment. The TIA license has to be purchased with 12 months support and the Unity license will be provided by Seqwater, refer I-LST-STD-001, 'Control Systems Prescribed Equipment'.

Firmware version of PLC CPU, communication card(s) and any other intelligent micro-processor card(s) to be used in projects shall match the firmware versions as per site requirement after consultation with the Principal.

### 10.1.1. Selection of the Configuration Languages

PLC software shall support the following programming languages as a minimum based on the IEC 61131-3 programming requirements:

a. Relay Ladder Logic/Ladder Diagram (LD) (Preferred)

b. Function Block Diagram (FBD)

c. Structured Text (ST), use of ST shall be limited to Standard PLC Library blocks.

The use of SFC shall be considered only for special purposes and only after permission is granted from Seqwater. IL is not acceptable as programming languages.

## 10.2. PLC Programming Requirements

Following are the minimum requirements for PLC programming:

a. Adequate commenting in the PLC program code to clearly document all internal functionalities to facilitate on-going support. The quality of programming comments shall be verified during reviews, FAT and SAT stages of commissioning.

b. English language shall be used for PLC program code and comments. This shall include 3rd party packages and PLC as well.

c. Development of device and tag numbering in accordance with Seqwater I-SPE-STD-010 Tag Naming Specification standard.

d. Programming of the PLC logic in accordance with the Functional Description (Part A & B) of the respective project.

e. No password protection of any of the PLC logic, subroutine or function blocks is allowed unless approved by Seqwater in writing. Seqwater reserves rights for all logic developed for the project.

f. Any project specific Functional Block developed and tested, shall be delivered with Data sheet and Test sheet in Seqwater format and submitted to Seqwater for approval.

g. The use of UDT (User Defined Data Types) or DDT (Derived Data Types) for creating data structures for control blocks for pumps, valves, motors etc. shall need Seqwater approval.

h. While creating any data structures (function blocks, data blocks etc.), care shall be given to define all meta data.

i. Symbol names (along with their description) shall be specified for all data blocks, function blocks and memory blocks. No address in the PLC program shall remain undefined in the Symbol table of the PLC program.

j. Retentive memory shall be used to store program, process set points, SCADA set points, analog value settings and totalisation.

k. In case of duty/standby devices or equipment functional allocation of IO's shall be done in such a manner that IO's for duty and standby devices shall be in separate modules so that the failure of one IO module shall not affect the functionality of the duty/standby unit.

l. The quality of a signal shall also be considered (in addition to the value of the signal) to perform any control, interlock and/or alarming function in the PLC program. This means that any tag with bad quality shall not be used in controlling the process and the program shall ensure failsafe operation of the control loop in that scenario.

m. Quality of the signal (along with its value) shall be made available in SCADA system for indication, events and alarming purposes; if the requirement to display process variable quality is specified in the functional description document.

n. For redundant sensors, value selection logic will be developed as per FD A requirements, provided that the sensors / transmitters are healthy.

o. The use of pointers or indirect addressing shall not be used for addressing IO, timers, counters or to access tables of data in the data blocks. Prior approval from Seqwater is required in case there are specific requirements to use pointers in the PLC program.

p. AEST (UTC+10) time shall be used for PLC to process data

q. Loss of communication watchdog should form part of the code as well as it should be recorded.

r. For Intelligent Suppression of Alarms and Events refer to I-SPE-STD-006

s. PLC to SCADA communications shall be through a software-based OPC server using the OPC UA protocol.. Principal shall also be consulted for site specific requirements.

# 11. SCADA Hardware

## 11.1. Free Issued SCADA Hardware

The Principal shall "free issue" the following SCADA hardware unless specified otherwise in the SOW:

a. SCADA Server (rack mounted, large tower or small tower machine(s) will be supplied depending upon site requirements) along with monitor(s)

b. SCADA Client workstation (including keyboard, mouse, and monitor(s))

c. SCADA server cabinet(s): make, model and technical requirements for SCADA server cabinet(s) are specified in SPE-00321 Server Rack Assembly Specification.

d. Cabinets for Remote locations: 6RU 600mm Wide and 550mm Deep Wall Mount Cabinet can be used to install FOBOT's and/or Ethernet switches at remote locations in plants. The SOW of individual projects will specify the quantity and locations of these 6RU cabinets. These cabinets shall be free issued by the Principal. Refer SPE-00321 Server Rack Assembly Specification to determine the make, model, and technical specification for cabinets for remote locations.

The quantity of free issued, Thin Clients and HMI Panels will be specified in SOW of the respective project. Any SCADA operated Seqwater site shall contain a minimum of one SCADA client station in addition to SCADA server machine. During the design of control room layout, SCADA client station(s) shall be allowed for operational purposes only. SCADA server(s) machines shall only be allowed for programming, engineering, and control systems maintenance purposes. The SCADA hardware will contain preconfigured software(s) essential for the operation of windows operating system, Microsoft office, Vmware, and SCADA software. A user with privileges to be configured so that Seqwater can change the password at later stage.

Seqwater will free issue SCADA software. For license projects shall apply it through form 'FRM-01275', 'SCADA License Application Form' available on Seqwater intranet.

The Contractor shall procure licenses for VSD, power meters and numerical relays for the engineering workstation. The contractor shall handover these licenses, software, and the associated equipment for communication with Engineering workstation with their configuration requirements to Seqwater CSM.

Any other software as required under the SOW of the individual project shall also be installed and configured on Control Systems engineering laptop.

## 11.2. Project Supplied SCADA Hardware

The SOW will specify the list and quantity of SCADA hardware to be supplied by Contractor based on project requirements. The term SCADA hardware in this section excludes PLC hardware components. Section 9 of this standard shall be referred for PLC hardware specifications.

All hardware shall be procured as per the PRO-64146 - ICT Procurement of OT Infrastructure

Project shall approach ICT for purchase of this hardware.

BOM (Bill of Material) with corresponding datasheets shall be submitted to the Principal to obtain procurement approval for any project supplied SCADA hardware.

## 11.3. SCADA Server Locations

The location of SCADA servers shall be determined based on project requirements and site conditions. Principal shall approve the final location of SCADA server(s). Some common rules that shall be followed while deciding the SCADA server location are described in this section.

19-inch rack mounted servers shall be installed in server cabinet as per requirements specified in SPE-00321 Server Rack Assembly Specification. Tower mounted large or small server machines shall be installed in server room.

The location of server room and/or server cabinets shall consider the following requirements related to access, heat dissipation and damage due to moisture and dust.

### 11.3.1. Server Location – Access Requirements

a. SCADA server(s) shall not be installed in main access areas, main entrances, pathways, doorways, or storage areas in the plant.

b. SCADA server(s) installation within HV rooms is not acceptable.

c. SCADA server(s) installation in LV rooms within 1.5 metre radial distance of switchboard is not acceptable.

### 11.3.2. Server Location – Heat Dissipation Requirements

a. SCADA server(s) shall be installed either in a dual redundant air-conditioned environment or single air-conditioner with a provision of natural airflow to cool down the server cabinet in the event of air conditioner failure.

b. There shall be a provision of temperature monitoring for the room where the SCADA server(s) are installed. “SCADA server room high temperature alarm” shall also be made available in control systems.

c. Contractor shall comply with PDU (power distribution units) and UPS requirements for server(s) cabinets as per SPE-00321 Server Rack Assembly Specification.

### 11.3.3. Server Location – Moisture and Dust Prevention Requirements

a. SCADA servers shall not be installed in any open areas susceptible to dust or moisture. SCADA server cabinet(s) shall comply with SPE-00321 Server Rack Assembly Specification.

b. Any location which possesses a risk of damage due to the presence of moisture sources shall not be selected for SCADA server(s) and/or SCADA server’s cabinet.

c. Air conditioners shall have condensation drains that avoid moisture affecting SCADA server(s). SCADA server(s) shall not be directly installed below the fan cooling units of the air conditioner or within 1.5 metre distance of the air conditioner unit.

## 11.4. SCADA Server(s) Positioning

a. The SCADA server(s) cabinet shall be positioned such that access is available from a minimum of 3 sides. Front and rear access is mandatory and one of the side accesses shall be made available. 4$^{th}$ Side can be a non-accessible side.

b. Minimum of 600mm of free space shall be made available for access from 3 sides.

c. The access doors shall provide easy access and if the door/panel is hinged, then it shall be able to open/close freely to its full extent.

## 11.5. SCADA Server(s) Physical Security

a. The design shall implement level of physical security measures that minimises or removes the risk of information and SCADA equipment being made inoperable or inaccessible, or being accessed, used, or removed without appropriate authorisation. This requirement is as per “Protective Security Policy Framework V2018.3” policies, “policy15-physical-security-for-entity-resources” and “policy-16-entity-facilities”.

b. SCADA servers shall not be used for operational purposes. SCADA client’s stations shall be made available for use by operations.

c. SCADA server cabinet(s) shall have lockable doors to prevent unauthorised access.

d. SCADA server room shall have doors with ABLOY locks installed and swipe cards to prevent unauthorised access. SCADA server rooms are defined as locations where SCADA server(s) machines are kept physically along with their UPS, switches, modems, and associated communication hardware. SCADA server rooms are not required to be dedicated rooms for SCADA equipment. SCADA server room(s) can share space with ICT equipment and/or electrical LV equipment.

## 11.6. SCADA Server(s) Redundancy

Whenever SCADA server redundancy is specified in the SOW, following requirements are applicable:

a. SCADA system redundancy shall be designed as per the availability requirements in I-SPE-STD-009.

b. Redundant SCADA servers shall be located in different rooms. If two physically separated rooms are not available at any site, then prior approval shall be taken from Seqwater to determine the best location to install redundant servers.

c. The SCADA system shall support primary and secondary servers to provide automatic redundancy in the event of a primary server failure. Once the primary server is considered inactive, the node configured as the secondary server shall automatically assume the role of primary.

d. Changeover between primary and secondary SCADA servers shall happen within 3 seconds during redundancy switchover.

e. The SCADA system shall be configured to ensure that the secondary server is kept fully synchronised with the primary server, so that upon transfer to the secondary server, no loss of data occurs.

f. Upon restoration of the failed primary then it’s databases, trend histories, alarms and event logs are updated to ensure that the system is synchronised with the running secondary and there are no gaps in the historical data or logs.

g. Failure of any one redundant part shall not interrupt other system functions. A failure may include but not be limited to hardware failure, software failure, communications network failure, power supply failure or the loss of one AC feeder in a dual feeder system. Switchover to the secondary device shall occur automatically upon failure of primary device.

h. The failure of any client node shall not affect the functionality of the system. However, upon restoration of the client, then any locally held display databases, trend history, alarm and event logs are updated to ensure

that all displays are then synchronised with the SCADA server and there are no gaps in the historical data or logs.

i. Automatic and manual switchovers of redundant SCADA servers shall be recorded as event in event log (priority 5 alarm).

j. It shall be possible to manually switchover (change from standby to active status) any redundant module like redundant UPS or redundant SCADA server machines without interrupting the system operation.

k. Both the machines of the redundant SCADA servers shall have redundant power feeds coming from mains power supply and UPS power supply.

# 12. SCADA Software

The SCADA system shall provide supervisory control, indication and alarming for the plant equipment, process control, communication system and control systems.

This section provides the requirements for SCADA software.

## 12.1. SCADA Software General Requirements

### 12.1.1. SCADA Software Configuration

It shall be possible to make changes to SCADA database without interrupting points not affected by configuration changes. The SCADA software shall provide object-oriented configuration to ensure uniform representation of devices across the entire SCADA system.

The SCADA software shall provide functionality to allow addition of a new graphic without interrupting operator control and monitoring of the plant. The SCADA system shall support configuration of tool tips (small configurable windows with plain text information for the user) which automatically pop up when the operator moves the mouse pointer over the respective element.

Contractor shall prepare “work method statement” for each and every task to be conducted on live SCADA system. It is the contractor’s responsibility to submit the work method statement to the Principal and get it approved before conducting any SCADA configuration changes on live plant.

Complete backup of the SCADA system (including database, graphics, configuration, and history) shall be taken on a daily basis during FAT, SAT, commissioning, start-ups and POPT activities, till the site is completely handed over to the Principal. In case there is a requirement to perform live work on redundant SCADA servers, then as a first step the redundant SCADA servers shall be de-synchronised. Any new or modified software (graphics, database etc.) shall be downloaded to one of the SCADA servers. Once the performance of the modified software is tested, the redundant SCADA servers can be synchronised again with an approval from the Principal.

During the commissioning activities, if there is a need for any design changes (for example change in requirements described in functional description document, creation of a device faceplate that is not specified in detailed design documents etc.); the Contractor shall first raise the X-TMP-STD-022 Asset Standards Deviation Request. Once Seqwater approves the Deviation request, design changes can be implemented at site. Any design deviation executed without Seqwater’s approval shall be treated as non-compliance.

### 12.1.2. Operator Interaction

The graphic subsystem shall enable the operator to trigger an operator action within a maximum of three operator inputs.

As a minimum it shall be possible to trigger operator actions as follows:

a. Pressing the mouse button

b. Releasing the mouse button

c. Actuating keys (including function keys).

The following options shall be considered for data input by the operator:

a. Direct data input

b. Using the keys “up” and “down”

c. Scroll bar or slider.

All control actions triggered by the operator shall be recorded as a time stamped event which is stored in an event history as described in Section 12.5.

## 12.2. SCADA Software Security Requirements

The SCADA system shall provide the following security features:

a. SCADA configurations shall maintain full visibility of the plant while restricting control based upon a user’s assigned area of responsibility.

b. The SCADA access security shall provide access to specific levels of control and monitoring. A minimum of six (6) levels shall be supported as explained in “user roles and privilege levels” section.

c. All SCADA users be assigned individual logins.

d. SCADA security shall be integrated with Windows Integrated Security, Windows Domain group policies and the Seqwater control domain.

e. The SCADA client can be configured to enter view only mode upon start up. The preference is for Role Based Access Control to be implemented.

f. Periodic auto-logout shall be possible using SCADA idle time functionality. After a set period of time of inactivity, the user shall be logged out to the default ViewOnly login. This shall not impact the current graphics displays.

g. The lowest level of login shall be ViewOnly. This is the default user login on SCADA start up and on logoff.

h. In order to meet Seqwater cyber security requirements, the Principal will delete all the users and their corresponding password(s) which are created by the Contractor (during the design, software development or commissioning of the project) at the time of handover of control systems. Principal will create its’ own SCADA users and their corresponding passwords once the control systems is handed over to Seqwater.

SCADA physical security requirements are described in Section 11.

### 12.2.1. User Roles and Privilege Levels

Privileges shall be configured to be independent rather than hierarchical. For example, Level 3 Privileges do not guarantee the user has Level 2. The SCADA system shall as a minimum be configured for the following user privileges as described below:

**Table 11: SCADA Security Privilege Levels for Plant SCADA**

| User Level | Description |
|---|---|
| Level 0<br>View Only | Allows anyone to view all areas, alarms, and trends. Cannot control, acknowledge alarms, or save trends. |
| Level 1<br>Basic Control | Default level of control. User can change process setpoints such as high or low levels, issue commands, perform disable (or maintenance function refer Section 8.3.2), acknowledge alarms and reset alarms. |
| Level 2<br>Adv. Control | Higher level of control. User can change CCP Action parameters such as High High Limits and disable alarms. |

| User Level | Description |
|---|---|
| Level 3 Management | Privileges available for configuration of managerial functions and report generation. User can change CCP Critical parameters. |
| Level 4 Optimisation | Configuration for plant optimisation features. User can configure Group trends and modify PID parameters as well as other plant optimisation parameters where applicable. |
| Level 5 Configuration | User has access to the SCADA software development environments. Depending on the SCADA software, this level may inherent privileges above, but all actions must be consistent with the SCADA user role. |

It is permitted to assign "Sub user levels" under each level if required.

**Table 12: SCADA User Roles for Plant SCADA**

| SCADA Users | Level 0 View Only | Level 1 Basic Control | Level 2 Adv. Control | Level 3 Management | Level 4 Optimisation | Level 5 Config |
|---|---|---|---|---|---|---|
| Viewer Only | ✓ | | | | | |
| Operator | ✓ | ✓ | | | | |
| Supervisor | ✓ | ✓ | ✓ | | | |
| Plant Manager | ✓ | ✓ | ✓ | ✓ | | |
| Process Engineer | ✓ | ✓ | | | ✓ | |
| Control Systems Engineer | ✓ | ✓ | | | ✓ | ✓ |

**Table 13: SCADA Security Privilege Levels for System Platform**

| Role Name | Description |
|---|---|
| Administrator | Only a user with Administrator Role can unlock a Standard that may be locked by another user for editing or permanently delete an Obsolete Standard. This enables an additional layer of security. Before the Administrator unlocks the Standard, they must first save it and tag it appropriately before making further changes. |
| Creator | Creates and edits Standards and the Catalogue folders. Can make a Standard Obsolete. Cannot permanently delete a Standard. |
| Author | Edits Standards, sets Class hierarchies. Cannot create a Standard. |
| Reader | Does not have edit permissions. Can only view the information. |

For System Platform user roles will be defined via Windows membership defined in Control domain.

## 12.3. Alarms

Seqwater's detailed requirements for alarms, events and messages are outlined in I-SPE-STD-006 Alarm and Event Management (SPE-00357).

The Contractor or any authorised Control systems worker shall configure SCADA alarms as per requirements specified in I-SPE-STD-006 including but not limited to the following:

### 12.3.1. Alarm Filtering and Alarm Groups

SCADA alarms shall be assigned the following attributes as a minimum:

a. Time stamp, including date
b. Alarm Tag
c. Alarm Description
d. Alarm Name
e. Status
f. Category
g. Priority
h. Area.

The alarm window shall have the ability to be filtered multiple ways, based on selections made through the alarm configuration system. SCADA system shall support the following alarm filters:

a. Priority
b. Acknowledged alarms
c. Unacknowledged alarms
d. Reset alarms
e. Alarm Type (category)
f. Area
g. Disabled alarms

### 12.3.2. Alarm Priorities

The SCADA system shall allow for five (5) alarm priorities as defined in I-SPE-STD-006 Alarm and Event Management (SPE-00357); the five alarm priorities are critical, action, warning, information and events.

### 12.3.3. Alarm Escalation

The SCADA system shall support configurable alarm escalation to enable unacknowledged alarms to either increase in priority, provide off-site notification, or activate alarm dialler call, if not responded to in a set time period as detailed in I-SPE-STD-006 Monitoring and control System Alarm and Event Management

This time period shall be configurable by users with level 5 privileges, typically assigned to Control systems engineers and administrators only.

### 12.3.4. Alarm Notification System Support

Many of Seqwater's assets are either unattended or only attended during certain hours. The Control systems shall therefore have the ability to configure alarms to integrate to the following systems for alert of extreme and high priority alarms:

a. Hardware Alarm Dialler System (e.g., EDAC Dialler, Elite 24+, micro spider))
b. Software Alarm Dialler System (e.g., Scada Phone Dialler, WIN911) Alarm Logging to File.

The SCADA system shall support automatic alarm logging for a period of twelve (12) months minimum, to a designated alarm file, unless specified otherwise in the functional description document of the respective project.

## 12.3.5. Alarm Dialler System

The software and hardware alarm dialler selection will be as per I-LST-STD-001 Control Systems Prescribed Equipment.

The deployed Industrial Control Systems (ICS) for a particular site is dependent on the site criticality assessment as defined in I-SPE-STD-009 Control Systems Topology Standard Section 4. The site criticality shall dictate the requirement for redundancy of alarm diallers.

a. Software alarm dialler (e.g. Scada phone dialler, WIN911)

b. Hardware alarm dialler (e.g. EDAC, Elite 24+, micro spider)

**Table 14: Site criticality and level of alarm dialler technology required**

| Site Criticality | Alarm Dialler Technology Required |
|---|---|
| Sites requiring low robustness and reliability<br>(Class 1 or Class 2 as outlined in Section 4.10 of I-SPE-STD-009). | • Hardware alarm dialler is mandatory |
| Sites requiring high robustness and reliability<br>(Class 3 as outlined in Section 4.10 of I-SPE-STD-009). | • Redundant alarm dialler technology required – Both software and hardware alarm diallers are mandatory.<br>• Control systems failure shall be configured as part of the dialled-out alarms<br>• Alarm dialler failure will generate an alarm for the PLC |

For sites requiring high robustness and reliability, software alarm diallers will be the primary alarm dialler technology, and the hardware alarm dialler will be secondary. The PLC configuration shall include automatic switchover from primary to secondary alarm dialler if there is a failure with primary alarm dialler. Failure of both alarm diallers will be indicated as a diagnostic alarm.

An alarm prioritisation and rationalisation assessment shall be undertaken which will determine which alarms are to be dialled out (see I-SPE-STD-006 Monitoring and Control System Alarm and Event Management for further details).

The Principal shall provide designated phone numbers and escalation requirements for programming the alarm dialler system. The project shall define any delay times for the individual alarms on the alarm dialler during the alarm rationalisation.

The alarm dialler system shall be operational, commissioned and fully tested by the Principal before practical completion of the project.

### 12.3.5.1. Alarm Dialler Escalation

In the event of primary software alarm dialler failure, the hardware alarm dialler is automatically activated. Both software and hardware alarm diallers shall be configured with the same pre-defined escalation pattern. This ensures consistency in operator response processes regardless of which dialler is active.

The alarm dialler shall initiate Level 1 notifications using its escalation contact list. If no acknowledgement is received within the configured delay time the alarm escalates through Levels 2–4 as per the defined escalation pattern. The escalation cycle continues until the alarm is acknowledged. If there is no acknowledgement at Level 4, the alarm dialler loops back to the beginning of the escalation table for a pre-defined number of loops.

- Level 1 – On-Call Operator

  If no acknowledgement is received, the dialler escalates to next level

- Level 2 – Secondary On-Call Operator

  If unacknowledged, the dialler escalates to the next level.

- Level 3 – Operations Supervisor

  If unacknowledged, the dialler escalates to the next level.

- Level 4 – Operations Coordinator

  If unacknowledged, the dialler will loop to the beginning of the escalation table

Refer to I-SPE-STD-009 Control Systems Topology Standard for alarm dialler architecture patterns

#### 12.3.5.2. Alarm Dialler Requirements

The table below highlights the functional requirements for the alarm dialler.

**Table 15: Alarm dialler functional requirements**

| Requirement | Description |
|---|---|
| Voice call notifications | Direct pre-recorded voice call notifications through VOIP / NBN / PSTN and 4G/5G connection<br>There shall be redundancy in media over which the call will be dialled |
| Text-based notifications | Direct text message notifications to mobile |
| System Login | Store details of alarm acknowledge |
| Alarm Holding | If the second alarm comes while the first one is being dialled out the system needs to hold the second alarm till the device is ready to dial out. |
| Alarm Looping | Keep on looping till the alarm is acknowledged in a particular sequence |
| Alarm Escalation | If alarm is not acknowledged escalate the alarm as per site escalation table |
| Alarm Reports | Generate Alarm History Reports |
| Redundancy | Hardware alarm diallers shall have redundancy in service provider (Optus / Telstra) |
| Remote access | Support remote modification of escalation phone numbers and alignment with shift roster |
| Testing capabilities | Support operator daily test dial required prior to leaving site<br>Function testing capabilities |

## 12.4. Trends

The design shall provide real-time and historical trends as per the following definitions.

Real Time Trends: Real-time trends are dynamic in nature. They are updated continuously during run time. They are used to display real time data of Tags.

Historical Trends: Historical trends as the name indicates are used to view past values of the Tags.

control System data model of the respective site (if existing) shall be utilised to develop tag list for real time and historical trends. In case the functional description of the process area is available at the start of the project, then it shall become the basis to develop tag list of real time trends and historical trends along with control System data model.

The SCADA system shall use the following types of trend displays:

a. Fixed trends: These shall be preconfigured trends

b. Trend groups: These shall be collections of trends

c. Device trends: These shall be shown from device faceplates

d. User defined trends (also referred as ad-hoc trends): These can be populated by the user as required

For each trend, it shall be possible for operator(s) to configure online, the number of points and ranges displayed on the trends. All trend configurations shall be possible on-line without interruption to the SCADA system.

Historisation of data shall not be affected by changes to trend configuration. All analog and digital points in the Control systems shall be available for trend displays.

Operators shall be able to zoom in on information displayed on trend sets for closer inspection. They shall be able to move the trend set backwards and forwards across the historical records. The trend sets shall automatically access archived history files when scrolling back in time without operator intervention.

The SCADA software shall allow for one trend window (if required) to be displayed at a time on any screen. The system shall store at least the last 1800 samples of all points on trend for display. The trending system shall also provide the following features for real time and historical trending:

a. A minimum of twelve (12) points (process variables) can be allocated to a real time trend.

b. Ability to pre-select groups of a minimum of four points and to assign a group to a display page.

c. The operator shall be able to adjust the vertical scaling of the trend display anywhere within the range of 0-100%.

d. Operator shall be able to adjust the maximum (start date and start time) and minimum range (end date and end time) of the horizontal axes for all trends.

e. The operator shall be able to ‘scroll’ forwards and backwards ‘in time’.

f. It shall be possible to pan and zoom within the trend display area.

g. As a minimum, the trend group shall be displayed with a tag number and EU units.

h. On an individual trend the tag name, EU unit and description shall be displayed

i. The operator shall be able to select, via a vertical line or other similar method, a particular point in time on the display, and the value of the variables shall be indicated.

j. From the Menu Bar, there shall be available a selection of pre-configured trends for each of the process areas within the plant.

k. It shall be possible to define the colour and line thickness of each pen of the trend.

l. Operator shall be able to select pre-defined trend periods on the trend displays of 1 hour, 4 hours, 8 hours, 12 hours, 24 hours, 48 hours, 7 days, 30 days/1 month and 365 days/1 year.

m. If any analog or digital value on the graphics, faceplate or pop-up has associated trend with it, then the trend shall be made available by clicking on the parameter display.

### 12.4.1. Trends Sample Periods Requirements

Trends shall be configured as per below sample periods:

**Table 16: Trend sample periods**

| Sample Period | Description | Examples |
|---|---|---|
| 1 second | Real time trending for data on fast network like ethernet and fibre optic | Analog instrument like flow transmitter situated within WTP and connected to PLC remote IO node |
| 10 seconds or Higher | Real time trending for data on medium speed network like microwave, radio link, 4G/5G | Analog instrument like flow transmitter for remote Pump station where remote pump station PLC communicates to nearby WTP PLC on 4G/5G network |

"Latency review" shall be performed during the detailed design, whenever there is a data exchange happening on microwave, radio link, 4G/5G/NBN/LEO satellite communication networks. As a part of latency review, Contractor shall explore the best available bandwidth and speed possible on that network. The design shall try to achieve sampling period better than 10 seconds for high speed and high bandwidth networks.

Trend configuration shall ensure that one (1) second resolution is available for real time trending as well as historical trending for analog and digital data.

### 12.4.2. Historical Trends

SCADA system shall utilise the capability of Centralised Historian to access historical trends greater than 12 months old.

a. The operator shall be able to scroll backwards and forwards in time for the complete period of data storage without entering dates and times, etc.

b. The operator shall be able to adjust the vertical scaling of the display, and to select an individual sample for a more accurate display of value.

## 12.5. Events

SCADA system shall be configured to log all events for all status changes whether arising from an action by an operator or arising during operation of the process and the process control systems.

Types of events that shall be logged include but not limited to:

a. State change feedback – valve open/part/closed, pump or drive stopped/running

b. System diagnostics – All system and PLC diagnostic events (as explained in control systems diagnostic section)

c. Equipment or process offline/online state

d. Switch positions – remote selected, local isolator open/closed, Incomer position, E-stops operated

e. Operator events – As explained in "operator event log" section.

A time stamp shall be appended to all events at their point of origin. If events are generated in the controller, the time stamp shall be appended there. If events are generated in the operator works station (OWS), the time stamp shall be appended in the OWS.

It shall be possible to call and sort events according to the time of occurrence (ascending or descending order) or the type of event.

### 12.5.1. Operator Event Log

The SCADA system shall automatically store all operator actions that affect process control parameters or alarm acknowledgement in the SCADA database. This includes, but is not limited to, the following actions:

a. Operator Login events
b. Suppressing/activating/acknowledging/resetting alarms
c. Mode selection (Remote Auto selected or Remote Manual selected)
d. Command entry (start/stop and open/close commands)
e. Changing the setpoint of a controller
f. Changing alarm limits
g. Changing tuning parameters.

Operator event log entries shall include the following information:

a. Time stamp, including date
b. Operator account name
c. Action taken
d. Action privilege requirements
e. Area
f. Equipment tag
g. Alarm tag (if applicable)
h. Previous Value (if applicable)
i. New Value (if applicable).

## 12.6. SCADA Database

The SCADA system shall have an integrated SCADA database to perform historical logging of alarms, operator events and trend data and publish the data for reporting purposes.

All data shall be stored in SCADA database as well as in Centralised Historian. However, SCADA database shall not store more than 12 months of data. Any data greater than 12 months old shall reside in Centralised Historian/database.

In case the site is not connected to a centralised monitoring system and Seqwater does not have any plans in the next five years to connect that site to a centralised monitoring system (to be confirmed with the Principal), then the SCADA database for that site shall have the capacity store minimum of 36 months of data.

SCADA shall utilise the capabilities of Centralised Historian to generate historical trends and historical reports where more than 12 months old data is required.

The types of data to be collected and reported by SCADA database include but are not limited to the following:

a. Field instrument process values
b. Target process setpoints
c. Operator actions
d. Energy consumption
e. Chemical consumption
f. Production volume
g. Events
h. Alarms.

### 12.6.1. SCADA Database General Requirements

The SCADA system shall contain inbuilt SCADA database which is integrated with the SCADA software. The following requirements shall apply to the SCADA database as a minimum:

a. The SCADA database shall support access using SQL, OPC and ODBC.
b. Historisation of point data shall be configurable as an attribute of the SCADA point.
c. Historisation shall be provided for both digital and analog events and alarms.
d. Periodic logging intervals for analog and digital points can range from 1 second to a few hours.
e. State change of digital points shall also trigger event-based logging of points.
f. SCADA database shall store the historical data using AEST (UTC+10) time .
g. The SCADA database shall be stored on the SCADA server (or redundant SCADA server pair wherever existing); distributed databases stored on operator stations and other workstations are not acceptable.
h. SCADA databases on redundant SCADA servers shall remain synchronised using bidirectional incremental updates of historic data changes.
i. The graphical operator interface, alarms, trends, and reports shall be able to access the SCADA database.
j. SCADA Database shall be configured to perform all periodic data cleaning operations without stopping the system. Data cleaning refers to removing the unused points from the SCADA database and performing “Compact database” operation to ensure maximum memory is available as free memory for usage.

### 12.6.2. SCADA Database Sampling

Each point available in the SCADA system shall be categorised according to the following definitions to indicate its SCADA database sampling frequency:

a. Never – The point is available in the SCADA trending system but not transferred to the SCADA database. Examples include some ON/OFF indication for small valves or alarm flags that will be recorded in an event summary.

b. On Change – The point is only sampled upon significant change rather than at set frequencies to reduce storage space consumption. Analog signals which do not change often can be logged this way via dead band or hysteresis settings whereby the sampling is only triggered when the signal drifts beyond a pre-set percentage of its current value.

c. Periodic – The point is sampled at a set frequency which may range from one (1) second to a few hours.

The sampling frequency for each point shall be determined during the detailed design based on operational and engineering criticality requirements.

### 12.6.3. Periodic Logging Frequency of Instruments

Requirements for periodic logging frequency of Instruments and Analysers are specified in the below Table.

**Table 17: Periodic Logging Frequency of Instruments**

| Instrument Type | Periodic Logging Frequency |
|---|---|
| Pipeline instruments (Flow transmitters etc.) | 1 minute |
| Pipeline Chemical Dosing Instrumentation & Water Quality Analysers (including CCP Analysers & Instruments) | 1 minute |
| Pump Stations Instruments (level, Flow and Pressure transmitters) | 1 minute |
| Raw Water, Sedimentation, Filters, UV Reactor, Sludge, Chemical Dosing & Treated Water – Instruments & Water Quality Analysers (Turbidity, Chlorine, Fluoride, dissolved oxygen Analysers, level, pressure, differential pressure or flow transmitters) | 1 minute |
| Reservoir Instruments and Analysers (Level transmitter, Turbidity Analysers etc.) | 5 minutes |

## 12.7. Reporting

The design shall provide pre-configured standard reports and free format custom reports that are configurable by the user.

Enterprise Historian shall utilise the data from historian for reports, where more than 12 months old data is required.

The frequency of these reports (daily, weekly, or monthly) will be determined during the detailed design stage of the project with due consultation and approval from the Principal.

The Enterprise Historian reporting package shall be capable of the following:

a. Production of user-defined reports using real-time and historical data exported into a spread sheet file or a PDF file.

b. Export of reporting data to spread sheet or customised reporting programs such as SAP Crystal reports.

c. Reports shall be able to be either scheduled or produced on demand, as the user requires.

d. It shall be possible to print the reports to a file or to the display or to a printer.

e. It shall be possible to create and save reports for initiation and display by any user with the appropriate privileges, and to select a regular time period for automatic report generation.

f. The reporting package shall as a minimum support:
   i. Manual entry of values
   ii. Flagging of bad data
   iii. Statistical manipulation of values (average, maximum, minimum, standard deviation etc.)
   iv. Mathematical calculations on values, result of calculations shall inherit bad data flags if present on any of the variables
   v. Storage of completed reports on disk
   vi. Inclusion of any point name from the SCADA database
   vii. Reports to be output to disk, rather than a printer

### 12.7.1. Report Activation

Report activation shall be possible in any of the following ways:

a. Periodic Activation at user specified intervals
b. Operator Initiated
c. Event Initiated
d. Application Initiated.

### 12.7.2. Pre-configured Standard Report Types

Standard reports shall be created so they can be configured through the entry of schedule information and other information such as Point Name or wildcard, filter information, time interval for search and destination printer to fully configure the report. Specifically, no programming or scripting shall be required to generate these reports in operational environment.

SCADA menu should be capable of providing following pre-formatted reports:

**Table 18: Standard Report Types**

| Type | Description |
|---|---|
| Alarm/Event Report | Produce a summary of all alarms or events of a specified type occurring in a period |
| Operator Action Report | Produce a summary of all operator actions relating to a particular operator in a specified period |
| Point Trail Report | Produce a summary of all events of a specified type occurring in a period on nominated points |
| Alarm Duration Report | Produce a summary of all alarms and the duration of each. If a point is in alarm when the report is produced, then the report shall calculate the duration 'so far' and indicate that the alarm is still active |

| Type | Description |
|---|---|
| Point Attribute Report | A report shall be provided detailing the status of various point attributes. The following report types shall be supported:<br>• Out-of-service<br>• Alarm suppressed<br>• Abnormal input levels<br>• In Manual mode<br>• In Local mode. |
| Database Cross-Reference Report | Provide a list of the following information for a nominated point, or set of points:<br>• A list of Graphic numbers which reference the point<br>• A list of other reports in which the point is referenced<br>• A list of trends and groups in which the point is displayed |
| Disabled Alarms Report | Listing of all disabled alarms on the system for; last 24 hrs, weekly and on demand |
| Priority 1 alarms in Last 24 hrs report | Report, details of all priority 1 alarms which have occurred in the last 24hrs |
| Power Consumption reports (also referred as Energy Monitoring report) | Daily and monthly energy summaries for the total site load and for each MCC or distribution board rated at 100 amps or more:<br>• kW and kVA 15-minute maximum demand graph and highest daily maximum demands<br>• kWh totals for Peak, Shoulder, Off Peak periods, and daily total<br>Daily maximum, minimum and average values for amps, phase volts, power factor, total harmonic voltage distortion levels (Current and Voltage) |
| Running hours reports | Running hours of drives. |
| Number of start and stop reports | Number of start and stops of drives |
| Chemical usage report | Daily consumption of chemicals (for example alum, lime, caustic, hypo, chlorine, PAC etc.) |
| Bulk chemical inventory report | Report describing inventory remaining for chemicals (for example alum, lime, caustic, hypo, chlorine, PAC etc.) |
| Production report | Example: Treated water volume report, Total Flow and Total Pumped of individual WTP on daily basis |
| Metering report | Metered (Billed) volume report. |
| Water quality set-point report | Incorporating operational, action and critical limits and associated time-bands for CCP parameters |
| CCP action and critical limit alarm report | Alarm limits for CCP parameters |

### 12.7.3. Free Format Custom Reports

In addition to the pre-configured standard reports, Contractor shall provide configurable report generation facilities to allow custom reports to be produced. They shall be configurable at any time with the SCADA system online.

Report generator should be configured to allow for the following capabilities:

a. Access to all real-time and SCADA databases

b. The report layout shall be user-defined, up to 132 columns wide, and unrestricted length

c. Access to user entered data

d. Arithmetic calculation capability

e. Statistical calculation capability

f. User definable report format

### 12.7.4. Integration of Industry Standard Reporting Packages

Where third party reporting packages are required, they shall be integrated into the SCADA's reporting subsystem and operate in a similar way to any of the reports handled natively. It shall be indiscernible to the operator that the reports have been written on a separate package.

It is not acceptable that reporting software shall interrupt or remove focus from the SCADA display, i.e., Microsoft Excel be displayed on the screen while the report is being printed.

The installation of third-party software on the SCADA server to support this functionality is acceptable, however it shall not be required to be installed on the client stations.

## 12.8. Date and Time Stamping

Date and time shall be configured in the following format:

g. All dates displayed in Australian "short-date" format; DD/MM/YYYY.

h. All times displayed in military format, HH:MM:SS in local time.

# 13. Seqwater Control Systems Libraries

The management of Seqwater's Control Systems Libraries is outlined in I-PRO-STD-004 Control Systems Software Library Management. Contractor shall not modify or alter any Seqwater control systems library object(s) (where provided) without obtaining prior approval from Seqwater in writing. Seqwater will perform inspection checks during the FAT and SAT to ensure the source code and the version of PLC & SCADA library deployed in the project are not altered. In case, if any of the PLC or SCADA library objects used in the PLC or SCADA program is found to be different from Seqwater control systems library object, then Seqwater reserve the right to suspend FAT and/or SAT activity.

## 13.1. Seqwater PLC Software Libraries

Seqwater library of standard control blocks shall be used in the PLC program for all new and existing Control systems sites. These include WTP, pump stations, network sites, storage, and hydroelectric power plants. Contractor shall not modify or alter any Seqwater standard control blocks without obtaining prior approval from Seqwater in writing.

In case of vendor packages (like UV system, centrifuges system, ozone systems, governor controls for hydroelectric power plants etc.), if the Contractor intends to use already developed proprietary control blocks, then prior permission shall be obtained from Seqwater in writing for the use of proprietary control blocks in the PLC program.

The Contractor can produce project specific PLC control blocks in the case of none of the standard control blocks in Seqwater library meeting the requirements specified in the Functional description document or the SOW. Contractor shall first raise the need to Seqwater to generate project specific PLC control blocks prior to any development. Wrapping of control blocks within the control blocks is not allowed whenever any new standard control block(s) are produced. Any project specific control blocks shall be developed under the direct supervision of Seqwater. Contractor will have to produce datasheet(s), detailed testing and complete test report(s) for every project specific control block and submit it to Seqwater for approval along with source code of control block. The project specific control block shall not be locked, or password protected. Refer to I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification.

## 13.2. Seqwater SCADA Software Libraries

Unless specified otherwise in the SOW, the Principal will provide (where available) a relevant "Seqwater standard SCADA library" for the development of SCADA software for the project. The relevant "Seqwater standard SCADA library" (where available) shall be used for all new and existing sites. The SCADA library will contain standard symbols, shapes, and faceplates. In the event of issues being identified between the relevant library and any relevant SEQ Water Standard, agreement shall be reached with the principal as to the best solution.

In the instance where Seqwater standard SCADA library requires an additional symbol or device faceplate to meet the functional requirements of the individual project, the Contractor shall first raise the need to the Principal for addition to library prior to any development. The new symbol or faceplate developed by the Contractor shall match the requirements specified in Seqwater standard with respect to colour, font, and graphic visualisation.

All objects shall not be locked, or password protected. Refer to I-SPE-STD-22 Supervisory Control and Data Acquisition (SCADA) Objects

# 14. Control Systems Response Time Performance Requirements

SCADA, PLC, and Communications systems shall be designed to meet the following response time performance requirements:

a. Any operator-initiated control actions shall cause a confirmation of that action on the graphic within 1sec.

b. Within (up to) one (1) second, the required action from the SCADA graphic shall be initiated in the Plant (e.g., start/stop, open/close).

c. A further (up to) one (1) second shall be permitted for signalling to the graphic, the successful activation of the operator's request (e.g., sequence active / inhibited, request to run, valve requested to open).

d. For remote SCADA, a typical three (3) seconds (or as specified in the FD) shall be allowed for data transfer across the Control WAN. The three seconds of time starts when the command is issued from remote SCADA and the time ends with the activation of field device at site.

e. Response time for peer-to-peer communication between two PLC systems (of same make or different make) shall be one (1) second or better.

f. Response time for communication between PLC system and fieldbus devices like VSD, power meters, numerical relays, flow meters etc. shall be two (2) seconds or better.

g. Response time for successful alarm notification and acknowledgement through to SCADA shall be in one (1) second or better.

The SCADA system shall meet all these performance requirements when the system is fully loaded with the ultimate design capacity.

# 15. SCADA Graphical Design and Conventions

## 15.1. Functional Requirements for SCADA User Interface

Following functional requirements for SCADA user interface for design and configuration of SCADA Graphics shall apply to all graphical user interfaces including Server, Desktop Clients, Terminal Server, Terminal Clients, Thin clients and OIPs.

1. Efficient and intuitive navigation – access and navigation are structured and intuitive to navigate. Technical requirements that shall be considered to meet this functional requirement are:
    a. The hierarchy of any screens shall be flat and simple to navigate.
    b. A linked navigation system with the fewest actions required to access alternate screens.
    c. Ensure direct access to primary displays and intuitive access to non-primary displays.
    d. Use consistency in naming and numbering of equipment from field labels through, drawings, documents, and SCADA interfaces.
    e. Equipment numbering is to be based on X-PRO-STD-006 Equipment Numbering and Naming Convention.
    f. A common header and footer for each graphic.
    g. Header and footer shall always be visible on each and every graphic (shall not be hidden).
    h. Navigation shall be achievable through either mouse or keyboard operation.
    i. Ability to navigate to previous and next graphic.
    j. Display current time and date on each graphic.
    k. Display current user logged in on each graphic
    l. Develop consistent graphic layouts that are appropriate to process behaviours – as per ASM Consortium Guidelines Effective Operator Display Design 2013 Section 4.4:
        i. General rules such as piping left to right, top to bottom shall be followed
        ii. Flow direction for recycle shall be right to left
        iii. Consistent between different display levels i.e., a horizontal pipe on an overview graphic should be horizontal on the control window.
2. Display process and equipment status – the status of the process shall be displayed with a suitable degree of detail. Failed items of equipment shall alert the operator. Technical requirements that shall be considered to meet these functional requirements are:
    a. Graphical indicators to be used wherever possible as they provide information at-a-glance.
    b. Equipment that is operating normally (whether running or stopped) shall not attract the operators focus.
    c. Any equipment that is not functioning correctly shall draw focus.

d. Two-factors shall draw attention to unhealthy conditions (not a single factor). For example: symbol and colour.

e. Colour alone shall not be relied on to indicate status of equipment – colour and brightness are independent qualities.

f. "Passive" devices such as pipes and tanks shall not be animated.

g. If there is no control, interlock, alarm, and feedback associated with the equipment, then as a general rule it shall not be shown on the graphics.

h. Flashing shall not be used to display any normal or abnormal condition.

i. Depict equipment without excessive detail to facilitate quick identification. Things like the flanges for piping do not provide any useful information for operations.

j. Actionable items shall be clearly distinguished from non-actionable.

k. No use of 3D graphics, photos, and videos.

l. Position display of modulating valves – As a percentage rather than a small-scale graphic which cannot be easily read.

m. Indication of bad data shall be clearly displayed.

n. Analog values shall be displayed with some level of context using an appropriately scaled graph or converted to a percentage or any other way.

o. Integrated alarm management – alarms shall be meaningful, linked to relevant equipment and provide diagnostic assistance.

3. Technical requirements that shall be considered to meet these functional requirements are:

   a. Alarming shall be based on I-SPE-STD-006 Monitoring and Control Systems Alarm and Event Management standard.

   b. Equipment or process areas that are in an alarm state shall be easily identifiable.

   c. It shall be possible to navigate from an alarm in the alarm window to the relevant item of equipment or process on the user interface.

   d. Ability to filter alarms and it is possible to identify when filters are applied.

   e. Alarming is based on action limits, critical limits, and operational limits.

   f. Alarm banner with three highest priority active alarms shall be displayed at the bottom of each graphic.

   g. Reserved colours used for alarms shall be used for alarms only.

   h. SCADA user interface shall allow the ability to sort alarms by time, priority, site, process, equipment, and quality.

   i. SCADA user interface shall use breadcrumbing of alarms.

4. Ability to control equipment – equipment can be started, stopped, and controlled automatically or manually. Technical requirements that shall be considered to meet these functional requirements are:

a. Buttons shall be visible even when disabled.
b. Separate buttons shall be used for each function. Example: a separate start and stop button instead of the start button becoming a stop button once a pump has started.
c. Buttons and operator actions/inputs should only be accessible through faceplates and pop-ups.
d. All equipment shall be in “Remote Auto” to start an auto sequence.
e. Buttons that can’t be used shall be distinguishable from those that can i.e. greying out a start button when Permissive aren’t met.
f. When a button is disabled, it shall be clear to the operator why i.e. permissive not met, active alarm(s), insufficient privileges etc.
g. Pinning of faceplates and pop-ups (so that they remain on graphic even if the graphic page is changed) shall be made possible.
h. Functional requirements for controlling/manipulating a device shall only be possible with sufficient privileges – examples of control include:
    i. Swapping between manual and auto modes
    ii. Manually start
    iii. Manually stop
    iv. Reset of faults
    v. Ability to disable a device
    vi. Ability to enable instrument calibration function for analysers/instruments
    vii. Ability to enable maintenance function of devices
    viii. Ability to disable alarms for a device
    ix. Ability to manually control the sequence
    x. Access relevant trends
    xi. Acknowledge alarms
    xii. Override start and stop in auto mode shall be made possible (in case there is a functional requirement for override start and stop for valves as specified in Functional description document)

5. Setpoint management – it shall be possible to read values from the process and enter setpoints. It shall be possible to download, export, backup and restore setpoints easily and reliably of SCADA data. Technical requirements that shall be considered to meet these functional requirements are:
    a. It shall be possible to enter Setpoint values using either the keyboard or a mouse
    b. Operators need to be informed when and why an attempted action fails, i.e., entering an out-of-range value shall inform the operator that it isn’t valid but shall also tell the operator the acceptable range
    c. Setpoint backup can be initiated manually or by an automated process
    d. Reporting or exporting of Setpoint values shall be made available

e. Ability to trend Setpoints shall be made available

f. Automatic uploading of Setpoints during the start of the plant (or any process) shall be made possible

6. Perform maintenance and calibration – it shall be possible to place an equipment in a "maintenance function" and instrument/analyzers in "instrument calibration function". Technical requirements that shall be considered to meet these functional requirements are:

    a. Ability to fully calibrate control loops given the correct privileges without needing to access the PLC shall be made available

    b. Ability to manually set the output value of the control loop shall be made available

    c. The interface shall provide meaningful maintenance information including run hours, number of starts

    d. Integrate maintenance system data (example: date of last calibration/service) into the SCADA interface where possible

7. Integrated trending – provide trending to assist with decision making on performance over time. Technical requirements that shall be considered to meet these functional requirements are:

    a. Ability to create ad-hoc trends on process performance shall exist

    b. Integrated trending into interfaces provides graphical indicators that give information at-a-glance

    c. Trending shall allow for proactive intervention into process disturbances

    d. Trending shall support optimisation and troubleshooting activities

    e. Consistency of colours shall be followed across trends

8. Information sharing and collaboration – users can apply notes to equipment and process areas to indicate details or background information on equipment status. Technical requirements that shall be considered to meet this functional requirement are:

    a. Operator notes (or diary) shall be made available across users (see Section 12.2) and can be used for handover between different operators

    b. References to operational procedures and drawings shall be made available on SCADA user's interface, where applicable.

    c. Ensure that interlock and permissive status with supporting information is available for an equipment or process area

    d. Provide access to alarm reference database

    e. Ensure that online user assistance is accessible for infrequently used functionality

    f. SCADA user interface shall support direct links to electrical and mechanical documentation from SCADA graphics, as required included in the functional design.

    g. Remote access of SCADA user interface without affecting the local operational control shall be made possible

9. Reliable system access and performance – integrated navigation and automated access to information across graphics in multi-system configurations. Technical requirements that shall be considered to meet this functional requirement are:

a. Ensure that display call up time between graphics does not exceed 1 second
b. Update rates should be slow with a minimum of 500 millisecond to aid readability and avoid taking the operators focus away from more critical information such as alarm states
c. Single login is required to access the SCADA system
d. Security and access levels are clear to the user
e. Data can be exported between the control systems and corporate system
    i. Access is efficient
    ii. Resolution shall ensure that there are no gaps in data when exported
    iii. Screen shots can be exported
    iv. Alarm text can be copied to clip board and transferred to corporate system.

## 15.2. SCADA Graphics Design Requirements

Following are the requirements for design and development of SCADA graphics:

a. The SCADA system shall be capable to display all control, monitoring and status attributes of any analog and digital tags in graphics. For analog tags, this requirement refers to the measured values, setpoints, alarm limits, and outputs. For digital tags, this requirement refers to the input and output status. Status information includes the alarm status and operating mode status.
b. All objects are to be designed with goal orientated design to achieve Perception, Comprehension AND Projection level of understanding. The design shall deliver Situational Awareness to the operators.
c. Either equipment number or equipment name shall be easily selectable by the operator.
d. The SCADA system shall be capable to display the device status with multiple states (opened/closed/travelling for example) by means of a unique combination of foreground and background colours.
e. The SCADA system shall allow the hiding of inactive alarm(s) or status messages from the operator.
f. SCADA graphics shall provide an overview of the process functional areas clearly showing controlled equipment and process variables associated with each area. The relationship of process functional areas with the other areas shall also be clearly shown.
g. All graphics shall share a common screen layout with a top bar primarily for navigation and a bottom bar for status indication. Both the top and bottom bars shall be the same on every graphic. Individual graphic content shall be placed between these bars in the centre of the graphic.
h. All control related to a particular device and its process shall be on the one graphic. This allows the operator to see all relevant data and status of the plant process they are operating.
i. Controls are not permitted from the Overview graphic, only from the lower-level plant/area graphics or their sub levels.
j. Parent-Child relationship shall be shown on the overview SCADA graphics page.
k. Where a sub-system or process area is dependent on a downstream device that is not displayed (e.g., a receiving tank) for parameters which affect its control, the face plate for this sub-system shall contain any

necessary information related to the downstream device (e.g., level), in order that the control can be executed without referring to the graphic containing the downstream device.

l. Clear intuitive representation of the process and plant ancillary systems.

m. Graphics shall be logically arranged to allow intuitive navigation by the operator

n. Allow full visibility of the plant to all users while restricting controls based on user privileges

o. Real-time data shall be updated automatically in all the graphics and face plates

p. Refresh rates shall be designed with the process in mind but shall not be shorter than 500ms for digital, numerical or text values

q. SCADA graphics shall be developed in accordance with the recommendations of the ASM Consortium Guidelines Effective Operator Display Design 2013 listed in below Table.

**Table 19: ASM Guidelines for SCADA Graphics Design Conventions**

| ASM Reference | Recommendation |
|---|---|
| 1.2 | Use a process overview graphic covering the operator span of control |
| 2.3 | Ensure that graphics are available to view disabled and inhibited alarms |
| 2.5 | Use trend displays when operators need to make decisions about the performance of variables over time |
| 2.6 | Ensure that the number of graphics is at a minimum and appropriate for operator tasks |
| 2.11 | Use redundant indication of critical alarms |
| 3.10 | Use linked navigation to automate access to corresponding objects or information across simultaneous views in multi-level display configurations. |
| 4.1 | Ensure that the overall style incorporates an effective range of colour intensities that is consistent with visual attention to the critical information |
| 4.2 | Ensure that the overall style uses animation effectively and appropriately to communicate process-critical or safety-related activity |
| 4.3 | Depict equipment without excessive detail to facilitate quick identification |
| 4.4 | Develop consistent display layouts that are appropriate to process behaviours |
| 4.5 | Minimise the complexity of equipment and control relationships presenting them in a single view. |
| 4.6 | Make detailed and supporting information that contributes to display clutter available on demand. |
| 4.8 | Ensure that the display layout emphasized important information |
| 4.9 | Distinguish similar processes in parallel trains with visual coding |

## 15.3. Hierarchal Display of Graphics

Graphics created for use by the operator shall be structured in a hierarchical manner. The intent of this section is to provide for a consistent approach to the way in which graphics are organised for the operators, and a consistent approach in which operators can move (navigate) between graphics.

All users shall be able to navigate to all graphics/faceplates but the controllable objects within those graphics/faceplates shall be correctly setup to test a user's credentials thereby giving/denying them control.

The design of SCADA graphics shall enable the user to reach to any graphic or faceplate with minimum mouse clicks as defined in functional description, refer to Figure 2: Hierarchal Display of Graphics Example.

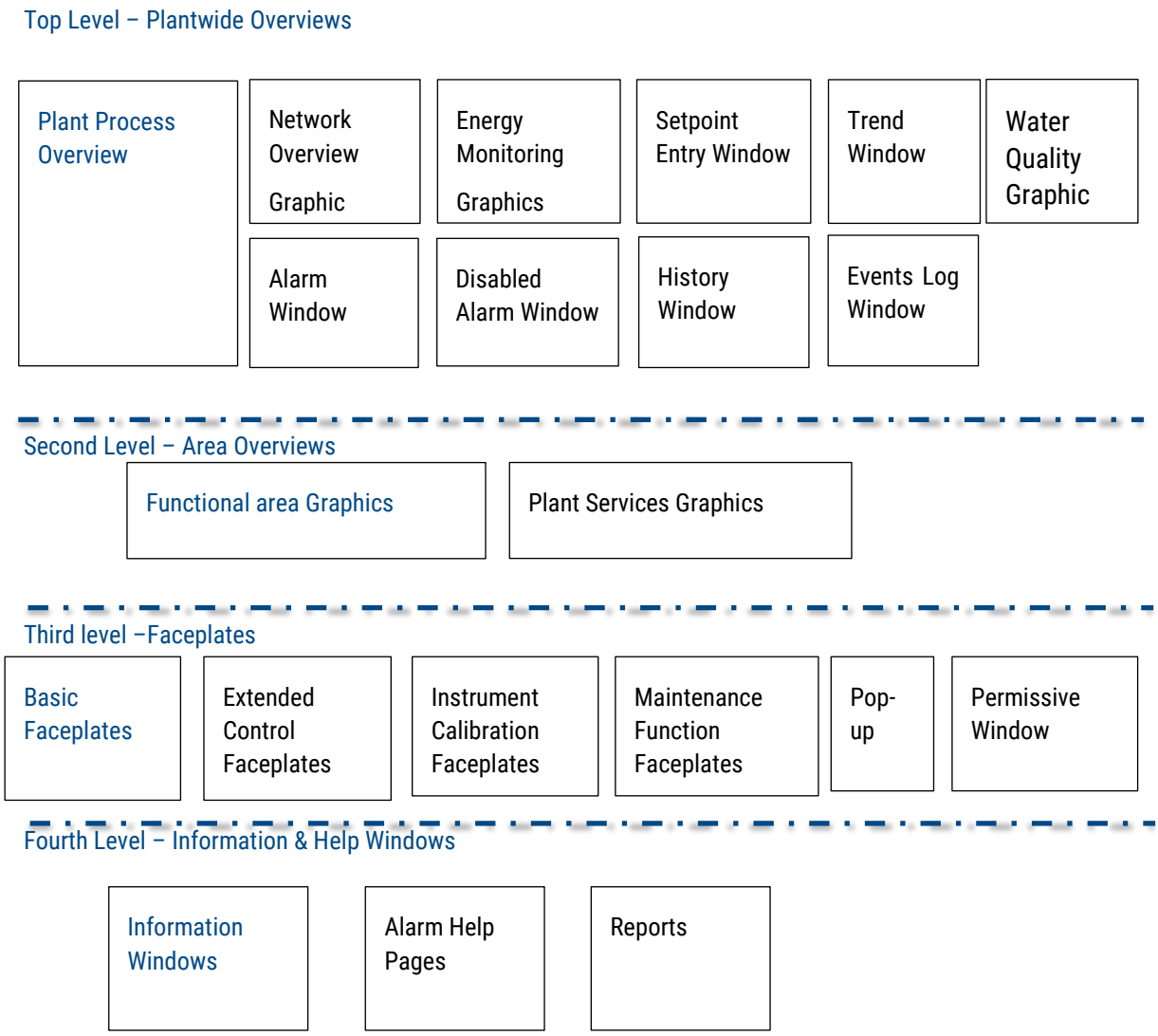



**Figure 2: Hierarchal Display of Graphics Example**

The SCADA system graphics shall include but not be limited to the following graphics:

a. Plant process overview graphic

b. Functional area graphic(s) for each process area of the plant complete with drill down functionality to sub-processes and equipment. These areas shall include but not be limited to the areas defined on the P&I diagrams and layout drawings.

c. Plant services graphic(s) (example: compressed air supply graphics, service water graphics etc.) in addition to functional area graphics.

d. Network overview graphic(s) displaying healthiness of SCADA server(s), SCADA client(s), PLC CPU, IO modules, remote IO rack(s), switches etc.

e. Energy monitoring graphic(s)

f. Trend window(s)

g. History window(s)

h. Alarm window and Disabled Alarm window

i. Event logs window(s)

j. Faceplates including control window(s), instrument calibration & maintenance function faceplates

k. Pop-Ups

## 15.4. SCADA Graphic Types

The SOW document shall list down the different graphics that need to be developed under the individual project scope. This section provides the technical requirements for developing the SCADA graphics for the project.

### 15.4.1. Plant Process Overview Graphic

Each site shall contain a plant process overview graphic. This graphic shall display all sub-process areas and major process area flows.

All sub-process areas shall be selectable as a target area for navigating directly to the process area overview graphic. Goal Orientated Dashboard (GOD) or plant process overview graphic shall be configured as home page and/or start-up page for every Seqwater site. Layout and design requirements for GOD will be approved by the Principal.

### 15.4.2. Functional Area Graphics

A process unit graphic shall be created for every process group in the system. These areas shall include but not be limited to the areas defined on the P&ID diagrams and layout drawings.

These graphics shall provide an overview of the process unit showing process pipe work, process equipment and process variables associated with each area. Process unit shall clearly indicate their relationship with other relevant sections of the plant. Rather than duplicate the graphics from the plant P&ID diagrams, effort shall be made to only show elements that are required for clear plant operation and logically follow the process flow of the plant. Items like reducers, expanders, isolation valves and manual valves shall not be shown on SCADA graphics if there are no SCADA controls, indications and alarms existing for the equipment.

a. Where more than one graphic is required for a process unit, the graphic shall show how many pages are associated with the area

b. All process unit graphics shall be linked to allow ease of movement, via the forward or backward keys, through the graphics

c. Equipment shall be depicted in the graphics using standardised device symbols

d. The values of all process parameters (including flows, temperature, pressure, and levels) shall be shown on the process unit area graphics.

### 15.4.3. Plant Service Graphic

Plant services in water treatment plant include but not limited to service water lines, compressed air lines and hydraulic supplies. SCADA graphics for plant services shall be created if exclusive P&ID's exist for plant services.

In case plant services are included in functional area P&ID's, then separate graphics are not required for plant services.

### 15.4.4. Network Overview Graphic

The control systems equipment and associated communication networks shall be displayed on the SCADA network overview graphic. The screen layouts shall be similar to that on the control systems network diagram.

The control systems shall monitor all PLC, computer, and network hardware. Faults, abnormal conditions, and high limits etc. are to be alarmed and displayed. The fault diagnostics on this graphic shall specify which components, modules or devices are faulty. The graphics shall be designed such that they support maintenance and operational staff in the diagnostics of faults in the Control systems. All diagnostics display categories shall be logically structured in such a manner that their position in the hardware architecture of the system can be recognised.

The network overview graphic shall show the status of all the following components as a minimum:

a. PLC CPU(s)
b. PLC racks
c. PLC remote IO modules (including power supply modules)
d. Communication network devices like remote IO switches, PLC LAN switches, SCADA LAN switches etc.
e. SCADA server(s) and client(s) stations
f. Site communication networks (e.g., remote IO ring network, Modbus TCP/IP network, Profinet network etc.)
g. AC and DC UPS (via SNMP or hardwired status signals)
h. Peripheral devices like printers, modems etc.

### 15.4.5. Energy Monitoring Graphic

Energy monitoring graphic shall include the following values for each main switchboard, MCC or distribution board rated at 100 amps or more in the dashboard format:

a. Latest 15-minute maximum demand
b. Maximum demand since the first of the month
c. Total kWh since midnight
d. Total kWh since the first of the month.

The SCADA system shall alarm abnormal plant consumption and demand conditions.

Alarm levels for 15-minute maximum demand level for each area shall be user configurable.

Each day shall be able to be monitored over three different time periods (Peak, Shoulder, Off Peak). The times for each period shall be configurable on the SCADA system.

### 15.4.6. Water Quality Graphic

Water Quality graphic shall include information related to water quality parameters like turbidity, dissolved oxygen, pH, chlorine, fluoride etc. Water quality graphic shall be made for the entire plant and/or individual process area (Raw Water, Sedimentation, Filters, UV Reactor, Sludge, Chemical Dosing, Treated Water etc.).

The layout and information to be included on water quality graphic shall be approved by the Principal.

### 15.4.7. Setpoint Entry Graphic

Setpoint entry graphic(s) shall allow the user with appropriate access level to enter the following Setpoints as a minimum:

a. High, high high, low, and low low Setpoints for analog instruments
b. Alarm off delays, alarm on delays Setpoints
c. CCP alarm Setpoints
d. PID Setpoints
e. Sequence start and stop Setpoints
f. Dose rate Setpoints
g. Control Setpoints
h. Setpoint needs to have single entry point.

PID Setpoints, dose rate Setpoints and Control Setpoints can sometimes be more appropriate to exist on individual device faceplates. Layout and design requirements of Setpoint entry graphics and/or Setpoint entry faceplates shall be approved by the Principal.

### 15.4.8. Basic Faceplates

A Faceplate is information interface page displayed when clicked on a device or an instrument.

Faceplates shall be provided for the basic control and monitoring of closed-loop control, discrete open-loop control, drives, valves, and all instruments. Faceplates shall be required to display the following information:

a. Tag name
b. Tag description
c. Process input, set point and output values in numeric display with physical units
d. Process input, set point and output in bar graphs
e. Remote Automatic/Remote manual mode status
f. Start, stop, open, close command buttons
g. Visual display of the device availability, alarm status and interlocks
h. Cumulative daily, weekly, and all-time total values for volumes, starts, run times as applicable for the relevant device
i. Symbolic and alphanumeric display of the discrete statuses of devices with two or more statuses.

Faceplates shall be configured such that they are opened on the screen when the corresponding process image (e.g. a symbol) is selected using the mouse.

An operator shall be able to issue basic commands from the faceplate (start, stop, open, close).

### 15.4.9. Extended Control Faceplates

Basic Faceplates shall be capable of being expanded to show detailed process information and allow for control functions beyond those required for everyday operations. Extended control faceplates are also commonly referred to as control pop-ups or control windows.

Where available, additional information shall be displayed in the extended control faceplate. This includes but is not limited to:

a. Online relevant water quality monitoring instrumentation
b. Access to pre-configured trends
c. Process values (flow rates, levels, pressure, temperature, humidity, pH etc.)
d. Drive speed
e. Power consumption (active and reactive power), current, voltage and power factor for electrical drives
f. Control levels selected
g. Status of individual permissive and alarms
h. Setpoints
i. PID setting values
j. Associated CCP alarm setpoints

The Extended faceplate shall also contain equipment control functions and Setpoints which allow the Operator to control equipment and adjust process parameters via the SCADA client. Where available these control Setpoints shall allow but not be limited to the following functions:

a. Cut-in/cut-out level adjustment
b. Process set point adjustment
c. Changing the setpoint and other parameters that can be set by the operator
d. Direct control of the outputs in manual mode
e. Changes to Duty/Standby modes
f. Reset/Pre-set of totalisers and cumulative values.

The SCADA system shall allow only reasonable and permissible values to be entered for process parameters. When a value that is out of range is entered, the user shall be notified of the acceptable range and the value should remain as the last good value. This functionality shall not replace hardcoded limits within the PLC for safety and equipment protection.

Where the SCADA user has advanced control (level 2) privileges it shall be possible to disable alarms and modify CCP alarm Setpoints. These actions shall require two-action operation such as a confirmation dialog due to the risk associated.

For Control Loops featuring PID of similar control schemes a SCADA user with optimisation (level 4) privileges shall be able to modify the PID coefficients or other tuneable parameters.

## 15.4.10. Force & Instrument Calibration Faceplate

All equipment with a force function shall have a force function faceplate. Requirements shall be approved by the Principal.

All instruments shall have an Instrument Calibration Faceplate. Instrument calibration shall be restricted to users with advanced control (Level 2) privileges. Instrument calibration faceplates are required to support the functionality defined in Section 8.3.3. It shall provide the following as a minimum in addition to basic faceplate functionalities:

a. Current Instrument Reading
b. Selection between actual, hold or forced value
c. Current Value (held or forced)
d. Time Remaining
e. Button for extension of time.

## 15.4.11. Maintenance Function Faceplate

The maintenance function faceplate shall be created for abnormal operation of equipment (pumps, valves etc.) for known conditions. “Maintenance function” enable button shall be added to the respective basic faceplate for all equipment which requires maintenance function as specified in SOW. Maintenance function extended faceplates are required to support the functionality as defined in Section 8.3.2.

## 15.4.12. Pop-Ups

A Pop-up is a page displayed when a SCADA object is clicked

Pop-ups shall be provided for process Setpoint entries, alarm Setpoint entries, alarm information pop-ups and to monitor and control the sequential start-ups and shutdown of process areas.

Setpoint entry pop-ups shall display the following information:

a. Tag name
b. Tag description
c. Button for Setpoint entries (with sufficient privilege levels).

Sequential start-ups and shutdown op-ups shall display the following information:

a. Start and Stop buttons for sequential start-ups and sequence shutdowns
b. Step number of each step and current step in execution
c. Device availability status of each step
d. Time elapsed and time remaining for each step
e. Alarms associated with each step, in case the sequence is halted at a particular step
f. Manual command buttons for jump steps or override steps

Pop-ups shall be configured such that they are opened on the screen when the corresponding process image (e.g., a symbol) is selected using the mouse, and can be repositioned on the screen.

## 15.4.13. Permissive Windows

Each device (valves, pumps etc.) and sequence logic (start-up and shutdown sequences) shall have a permissive window if there are interlock requirements to either start or run the device or sequence.

Permissive windows shall be linked to the device symbol shown on the graphics.

All the start interlocks, running interlocks and stop interlocks (if any) shall be made available on permissive windows for the associated device and sequences.

The layout and information to be included on permissive windows shall be approved by the Principal.

## 15.4.14. Alarm Window

The Alarm window refers to the full list of current (or active) alarms, these being alarms which are not acknowledged or that are acknowledged but not cleared. Not cleared means that the initiating condition is still present.

a. The SCADA system shall provide an alarm window that details all alarms chronologically with the most recent alarm at the top of the list.

b. The alarm page shall be accessible from a Menu Bar.

c. The alarm condition shall be the logic state description for digital signals, or the type of alarm (HIGH, LOW, etc.) for analog signals.

d. Alarms on the alarm window shall show the following information as a minimum:

   i. Date

   ii. Alarm Tag

   iii. Alarm Description

   iv. Status

   v. On Time

   vi. Ack Time

   vii. Off Time

   viii. Delta Time

   ix. Category

   x. Priority

   xi. Process Area

## 15.4.15. Disabled Alarm Window

The SCADA system shall provide a single list of all alarms which are currently disabled or inhibited for the entire site; this includes device disabled alarms and alarms for equipment in maintenance function.

It shall be possible to navigate directly to the equipment from the associated disabled alarm window.

### 15.4.16. Alarm Help Pages

The SCADA system shall be configurable to support “help pages” for alarms. Each alarm shall have a corresponding alarm help message set in the alarm’s configuration.

The SCADA shall be configurable to support the requirements for an alarm information pop-up for every alarm to be used to obtain additional information about that alarm. The following information shall be available from alarm information popup:

a. Operator Action Upon Alarm Activation
b. Reason Alarm Executed
c. Alarm Tag
d. Detailed Alarm Description
e. Asset/Tag under alarm
f. Category
g. Area

## 15.5. SCADA Graphics Naming Convention

All SCADA graphics shall comply with a standard graphic naming convention as outlined in below Tables. For example – TKY_O0001_Overview.

**Table 20: Graphic Naming Convention**

| Type | Convention |
|---|---|
| Graphics | LLL_ZYYYY_DDDDDDDD |
| LLL | Site where the IO Server will be run from (e.g., TKY) |
| Z | Representative character of the graphic type (see below table) (e.g., O) |
| YYYY | Sequential numeric (e.g., 0001) |
| DDDDDDDD | Description (Optional) (e.g., OVERVIEW) |

The graphic types in the system are defined by a character as defined below:

**Table 21: Graphic Types**

| Graphic Type | Suffix |
|---|---|
| Plantwide Overviews | O |
| Area Overviews | A |
| Faceplates & Pop-ups | P |
| Information and Help Windows | H |

## 15.6. Graphics Navigation

The operator shall be able to easily access specific displays and graphics: by pressing specifically reserved function keys or overview buttons, by selecting graphics from a hierarchical list in directories or menus, or by selecting from an alphabetical list of all graphics.

No more than two operator actions shall be required to switch between associated graphics with different or same hierarchal levels.

The SCADA system shall permit the operator to search the graphic hierarchy at the top of the screen to call up the desired display.

Graphics shall support inter-linked navigation such that process flows on one screen can be easily followed to the next screen by clicking short-cut arrows to take the operator to the next graphic of the process flow. Inter-linked navigation buttons shall be placed only at the left or right extreme of any given graphic.

## 15.7. Symbols and Conventions

### 15.7.1. Colour Conventions

The Main Body area of the graphics shall use the background colour grey. Limit the use of red, orange, and yellow for alarms or abnormal conditions only to draw the operator's attention readily.

The below recommendations from the ASM Consortium Guidelines Effective Operator Display Design 2013 shall be followed.

**Table 22: ASM Guidelines for Colour Conventions**

| ASM Reference | Recommendation |
|---|---|
| 5.1 | Use a minimum number of colour codes consistently across display hierarchy levels. |
| 5.2 | Reserve colours used for alarm coding for alarms only |
| 5.3 | Ensure that colour combinations provide acceptable and sufficient contrast. |
| 5.4 | Avoid colour combinations that are confusing for colour vision deficient perception |
| 5.5 | Use brightness coding sparingly for salience coding |
| 5.7 | Ensure that colour is redundant, visual coding of information |
| 5.8 | Ensure that colour codes avoid conflicts with cultural stereotypes and industry standards |

Generally, colours for Mimic shall be used as follows:

**Table 23: Colour Guidelines**

| Application | Sample | Details |
|---|---|---|
| Buttons | | Grey RGB (210,215,220) |
| Toolbar/popup/faceplate | | Grey RGB (182,190,198) |
| Info Bar | | Grey RGB (210,215,220) |
| Graphics Background | | Grey RGB (210,215,220) |
| Graphics Title Text | | Grey RGB (126,140,154) |
| Border | | Grey RGB (126,140,154) |
| Pipe / Equipment / Device outline | | Grey RGB (171,181,189)<br>Line weights 0.35 Pixel |
| Equipment / Device internals | | Grey RGB (171,181,189)<br>Line weights 0.16 Pixel |

| Application | Sample | Details |
|---|---|---|
| Equipment / Device Text | | Grey RGB (171,181,189) |
| Device Description text | | Grey RGB (52,60,68) |
| Device Detail Window | | Emboss Low Light RGB (120,146,154)<br>Emboss High Light RGB (238,240,242) |
| Device Off state/ closed state | | Grey (102,102,102) |
| Interlock in “OFF” state or inactive state | | Grey (102,102,102) |
| Device On State/ open state | | White RGB (255,255,255) |
| Device in Transition state | | Blue (0,32,96) |
| Interlock Active or “ON” | | White RGB (255,255,255) |
| Trend Background | | Black RGB (0,0,0) |
| Bar Graphs (e.g., Tank Level) | | Grey Fill (137,150,163)<br>Border Black (102,102,102) |

Generally, colours for mimics for symbols shall be used as shown below:

**Table 24: Mimic Colours**

| Mimic | Symbol | Colour Code |
|---|---|---|
| Calibrate |  | Grey (52,60,68)<br>Blue (110,217,250) |
| Disabled |  | Grey (52,60,68)<br>Yellow (249,232,0) |
| Force |  | Grey (52,60,68)<br>Blue (110,217,250) |
| Local |  | Grey (52,60,68)<br>Yellow (249,232,0) |
| Maintenance |  | Grey (52,60,68)<br>Yellow (249,232,0) |
| Manual |  | Grey (52,60,68)<br>Yellow (249,232,0) |
| Unavailable |  | Grey (52,60,68)<br>Yellow (249,232,0) |
| Reverse |  | Grey (52,60,68)<br>Yellow (249,232,0) |

| Mimic | Symbol | Colour Code |
|---|---|---|
| Trip / Crash(Only to be visible when there is an active interlock) |  | Border (102,102,102)<br>Symbol (102,102,102)<br>Fill White including proxy (213,255,255) |
| Analog_Value |  | Fill RGB (213,255,255)<br>Border (102,102,102) |
| Fill |  | Fill RGB (199,205,211)<br>Border RGB (102,102,102) |
| Fill when in calibrate |  | RGB (110,217,250)<br>Border RGB (102,102,102) |

## 15.7.2. Alarm Priority Conventions

Alarms shall be displayed using different colours based on priority as follows:

**Table 25: Alarm Priority Display Guidelines**

| Description | Symbol sample | Details |
|---|---|---|
| Alarm priority symbol text<br><br>Unacknowledged alarms / Acknowledge alarms | **Alarm font** | Segoe UI, Size 11, Bold<br>White Unacknowledged<br>Black Acknowledged |
| |  | Fill RGB (250,50,0)<br>Border (210,42,0), width 3 pixel |
| |  | Fill RGB (243,129,7)<br>Border (204,108,6), width 3 pixel |
| |  | Fill RGB (158,112,208)<br>Border (136, 82, 192), width 3 pixel |
| |  | Fill RGB (7,150,193)<br>Border (6,122,154), width 3 pixel |
| Acknowledge Text for alarm | Priority 1 | Text Segoe UI RGB (250,50,0) |
| | Priority 2 | Text Segoe UI RGB (243,129,7) |
| | Priority 3 | Text Segoe UI RGB (158,112,208) |
| | Priority 4 | Text Segoe UI RGB (7,150,193) |
| | Priority 5 | Text Segoe UI RGB (67,67,67) |

| Description | Symbol sample | Details |
|---|---|---|
| Unacknowledged Text for alarm | ***Priority 1*** | Italic Bold Text Segoe UI RGB (250,50,0) |
| | ***Priority 2*** | Italic Bold Text Segoe UI RGB (243,129,7) |
| | ***Priority 3*** | Italic Bold Text Segoe UI RGB (158,112,208) |
| | ***Priority 4*** | Italic Bold Text Segoe UI RGB (7,150,193) |
| | *Priority 5* | Italic Text Segoe UI RGB (67,67,67) |
| Hardware Alarm Windows Unacknowledged text (where separate alarm windows supported by systems) | *Priority 5* | Bold, Italics RGB (95,95,95) |
| Hardware Alarm Windows Unacknowledged text (where separate alarm windows supported by systems) | ***Priority 5*** | Text Segoe UI RGB (67,67,67) |
| Disabled Alarm Window (where supported by SCADA system) | ***Priority 5*** | Text Segoe UI RGB (67,67,67) |
| EU and tag/desc colour<br>font | system_analog<br>  <br>Syste_analog_cal | RGB (52,60,68)<br>Text (Segoe UI, bold, 12)<br>Alarm Border colours as per priority fill colours and width of 3 pixels |
| Fill |  | Fill RGB (199,205,211)<br>Border RGB (102,102,102) |
| Fill when in calibrate |  | RGB (110,217,250)<br>Border RGB (102,102,102) |
| Alarm Bar used in the above symbols |  | RGB (249,232,0)<br>Border RGB (102,102,102) |

Alarm Priorities 1-4 shall be displayed on graphics. Priority 5 alarms, which are events, shall not be displayed on graphics. They shall only be made visible on Event Window.

Events are classified as Priority 5 alarms however not all events are required to generate priority 5 alarms. Events like starting and stopping of drive and opening and closing of valve shall not generate priority 5 alarms. Events like turning the device into Local mode or in Remote Manual mode shall generate priority 5 alarms. Events list and Alarms list shall be approved by the Principal during the detailed design stage of the project.

All events (whether they are priority 5 alarms or not) shall be made available in events window.

### 15.7.3. System Fonts

All SCADA user interface fonts shall be Segoe UI including alarm acknowledged and unacknowledged texts. Font size shall be selected such that upper-case characters have minimum height of either 3mm or .005 times the typical viewing distance. This minimum value is to be used as a guide and legibility shall be confirmed on actual hardware during development.

**Table 26: Standard Fonts**

| Name | Font | Colour | Sample | RGB Code |
|---|---|---|---|---|
| **Page Text** | | | | |
| Fixed Text for objects outlines | Segoe UI | Grey | Sample Text | 171,180,189 |
| Fixed Text, Menu | Segoe UI | Dark Grey | Sample Text | 52,60,68 |
| Fixed Text – Area Title | Segoe UI | Grey | SAMPLE TEXT | 126,140,154 |
| Fixed Text – Equipment Label | Segoe UI | Grey | SAMPLE TEXT | 52,60,68 |
| Dynamic Text – Process Value | Segoe UI | Black | Sample Text | 0,0,0 |
| Dynamic Text – Process Value Calibration | Segoe UI | Black | Sample Text | 0,0,0 |
| Dynamic Text – Operator Input | Segoe UI, B | Black | Sample Text | 0,0,0 |

### 15.7.4. Numeric Values

a. Display-only values are displayed as black text with a grey background.

b. Modifiable values (e.g., SPs etc.) are displayed as black text with a cyan (213,255,255) background.

c. The number of decimal places associated with process values shall be one (1) unless otherwise specified in Functional description of respective site.

d. Numeric displays for whole numbers there shall be no decimal number shown e.g., number of starts for a motor.

e. The precision with which process values are displayed shall be consistent amongst all the displays on which the value appears.

Numeric values shall be displayed using different colours as follows:

**Table 27: Numeric Display Guidelines**

| Device State | Symbol | Description |
|---|---|---|
| Process Value Normal | 78.9 kg SEEExXNNN | Black text on light grey background |
| Disabled | X 78.9 kg SEEExXNNN | Black text on light grey background with disabled "X" as seen |
| In Maintenance | 78.9 kg SEEExXNNN | Black text on light grey background with Maintenance symbol as seen |
| In Maintenance and Calibration Mode | C 78.9 kg SEEExXNNN | Black text on Cyan background. Additionally, "C" symbol |
| Process Value with Priority 4 Alarm | 4 78.9 kg SEEExXNNN | Priority 4 Alarm |
| Process Value with Priority 3 alarm active | 3 78.9 kg SEEExXNNN | Priority 3 alarm active |
| Process Value with Priority 2 alarm active | 2 78.9 kg SEEExXNNN | Priority 2 alarm active |
| Process Value with Priority 1 alarm active | 1 78.9 kg SEEExXNNN | Priority 1 alarm active |

## 15.7.5. Level Display

Levels (or analog values like Flow) shall be shown with a bar indication (as appropriate).

Examples of different bar indications are shown in Figure 2.

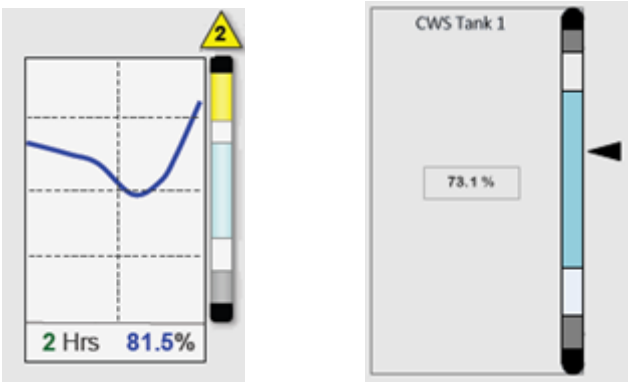



**Figure 3: Bar Display of Levels**

The first bar chart representation is a trend display of levels with alarm limits. The duration of the trend (shown as 2 hours) shall be made adjustable for the operator. Percentage level is also shown along with the trended value.

The second bar chart representation has a pointer to display the current level. The bar also represents the normal operating range and various alarm ranges of the level. Percentage level is also shown along with the pointer value.

Units of measurement shall be displayed along with measured value on any bar chart display of analog values.

Similar bar chart representation can be used to display other analog values like flow, pressure, turbidity etc.

### 15.7.6. Engineering Units

The display of numerical data shall use common units to aid in the rapid comparison of data.

The following engineering units shall be applied with care taken to ensure the use of correct case.

**Table 28: Standard Engineering Units**

| Description | Engineering Unit |
|---|---|
| Analysers – Aluminium | mg/L |
| Analysers – Chlorine | mg/L |
| Analysers – Conductivity | uS/cm |
| Analysers – Density | g/L |
| Analysers – Fluoride | mg/L |
| Analysers – Iron | mg/L |
| Analysers – Nitrate | mg/L |
| Analysers – pH | pH |
| Analysers – Turbidity | NTU |
| Communication – Port Speed/In rate/Out rate | kbps |
| Communication – Signal Power | dBm |
| Electrical – Active Power | kW |
| Electrical – Reactive Power | kVAR |
| Electrical – Total Power | kVA |
| Electrical – Energy | kWh |
| Electrical – Current | A |
| Electrical – Voltage | V |
| Electrical – Frequency | Hz |
| Flow – Pumps | L/s |
| Flow – Dosing Pumps | L/hr |
| Flow – Totalising / Report | ML/day |
| Level (Actual volume of Vessel to be shown) | % |
| Pressure (for vessels, pumps) | kPa |
| Pressure (for Pressure gauges in pipelines) | mAHD (Meter Australian Height Datum) |
| Speed – VSD | % |
| Temperature | C |
| Vibration | mm/s^2 |
| Weight | kg |

### 15.7.7. Standard Symbol Set

a. Symbols shall generally be diagrammatic elevations or cross-sections in two dimensions to provide a consistent process representation.

b. Pictorial or characterised elevations or three-dimensional styles designed to resemble the particular plant item shall not be used.

c. The device status is represented through the use of a symbol colour fill code.

d. Devices should not be flash or be otherwise animated.

e. Two sizes for each device symbol (big and small size) shall be made available in the standard symbol set. Due diligence shall be used in determining the usage of small and big size symbols in SCADA user interface. For example: big device symbols can be deployed in main graphics and small device symbols can be effectively deployed in faceplates.

f. Symbol updates shall be limited to 500ms minimum refresh time. The silhouette of a device symbol should not change.

The below recommendations from the ASM Consortium Guidelines Effective Operator Display Design 2013 shall be followed during the configuration of graphic symbols.

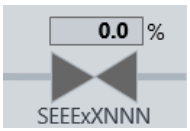
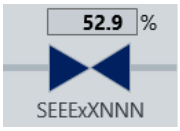
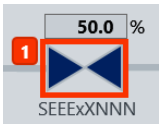
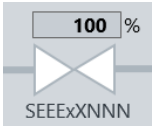
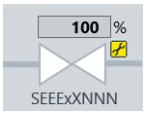
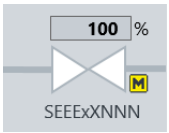
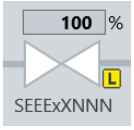
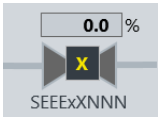
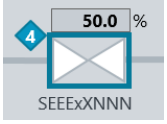
**Table 29: ASM Guidelines for Symbol Set**

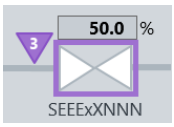
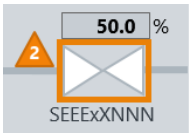
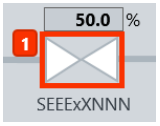
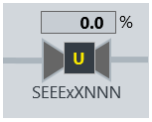
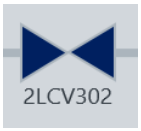
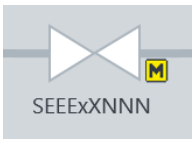
| ASM Reference | Recommendation |
|---|---|
| 6.1 | Use symbol and line coding that is understood easily with appropriate salience. |
| 6.2 | Use text and numbers that are legible at the user's typical position |
| 6.3 | Use coding and abbreviations that are consistent and understandable to users. |
| 6.4 | Use a minimalist approach when using lines to show controller and output relations |
| 6.6 | Use mixed-case lettering for text messages |
| 6.6 | Use consistent numeric formats to enable quick reading |
| 6.8 | Use numbers that have the appropriate level of precision |
| 6.9 | Ensure that users easily understand messages. |

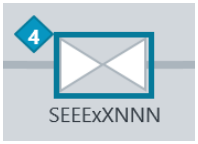
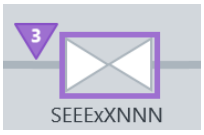
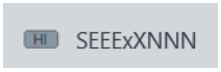
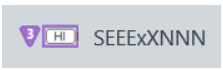
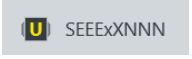
Table 30: Standard Library Device Examples for colour representation shows representation of colours for typical device states. The colour scheme in this table shall be followed in all graphic. The device library is for representation only.

**Table 30: Standard Library Device Examples for colour representation**

| Device State | Symbol | Description |
|---|---|---|
| **Pump** | | |
| Pump Stopped |  | Grey |
| Pump Running |  | White |
| Pump Running in reverse |  | White with reverse symbol |
| Pump in unknown state |  | Blue with reverse symbol |
| Pump in Manual and running |  | White with Manual symbol Running |
| Pump in Local and running |  | White with Local symbol Running |
| Pump in Maintenance |  | Grey with Maintenance symbol Stopped |
| Pump Disabled |  | Grey with Disable symbol |
| Pump unavailable |  | Grey with unavailable symbol |
| Pump priority 4 alarm active |  | White with Cyan 4 border and priority 4 symbol |
| Pump priority 3 alarm active |  | White with Magenta 3 border and priority 3 symbol |
| Pump priority 2 alarm active |  | White with Orange 2 border and priority 2 symbol |

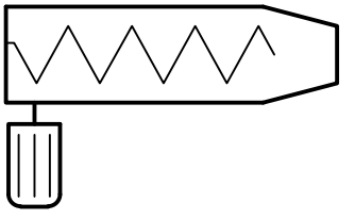
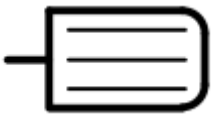
| Device State | Symbol | Description |
|---|---|---|
| Pump priority 1 alarm active and in local mode |  | White with Red 1 border and priority 1 symbol |
| Pump priority 1 alarm acknowledge and in local mode |  | White with Red 1 border and priority 1 symbol black text |
| **Control Valve with analog feedback** | | |
| Closed State |  | Grey with closed feedback ON |
| Transition State |  | Blue with both opening/closing feedback active |
| Transition State with no feedback |  | White with no opening/closing feedback active |
| 100% open |  | White with open feedback active |
| 100% open and in maintenance |  | White with open feedback and maintenance symbol |
| 100% open and in manual |  | White with open feedback and manual symbol |
| 100% open with open feedback and in local |  | White with open feedback and local symbol |
| Disabled motorised valve |  | Grey with disable symbol |
| Motorised valve with Priority 4 alarm active |  | White with Cyan 4 border and priority 4 symbol |

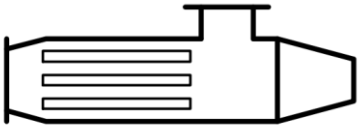
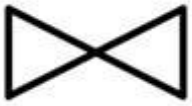
| Device State | Symbol | Description |
|---|---|---|
| Motorised valve with Priority 3 alarm active |  | White with violet border and priority 3 symbol |
| Motorised valve with Priority 2 alarm active |  | White with orange border and priority 2 symbol |
| Motorised valve with Priority 1 alarm active |  | White with Red border and priority 1 symbol |
| Motorised Valve unavailable |  | Unavailable |
| **Valve Digital** | | |
| Valve Digital Closed |  | Grey with closed feedback |
| Valve Digital Transitioning |  | Blue with no feedback |
| Valve Digital in transition (invalid state) |  | Blue with both feedback active |
| Valve Digital open |  | White with, open feedback |
| Valve Digital 100% open and in maintenance |  | White with open feedback and maintenance symbol |
| Valve Digital 100% open and in Manual |  | White with open feedback and manual symbol |
| Valve Digital 100% open with open feedback and in Local |  | White with open feedback and Local symbol |

| Device State | Symbol | Description |
|---|---|---|
| Valve Digital disabled |  | Grey with Disabled symbol |
| Valve Digital with priority 4 alarm active |  | Valve with Cyan border and with priority 4 symbol |
| Valve Digital with priority 3 alarm active |  | Valve with Purple border and with priority 3 symbol |
| Valve Digital with priority 2 alarm active |  | Valve with orange border and with priority 2 symbol |
| Valve Digital with priority 2 alarm active |  | Valve with orange border and with priority 1 symbol |
| Valve Digital unavailable |  | Valve with unable symbol |
| **Discrete Device** | | |
| Discreate device In-active state |  | In-active state |
| Discreate device Active state |  | Active state |
| Discreate device State active (High) with alarm priority 3 active.<br>*Follow the alarm symbols for other alarm priorities* |  | State active (High) with alarm priority 3 active |
| Discreate device Disabled |  | Disabled |
| Discreate device Unavailable |  | Unavailable |

Any deviation or further symbol device requirements will require Operation and Seqwater approval.

**Table 31: Common Standard Library Shape Set**

| Device | Shape |
|---|---|
| Air Compressor |  |
| Blower |  |
| Centrifuge |  |
| Clarifier / Thickener | Requires approval by the Principal and Operations. |
| Filter | Requires approval by the Principal and Operations. |
| Motor |  |
| Moving equipment e.g., feeder, bucket elevator, conveyor<br>Feeder | Example of a feeder, which will be a device.<br>  <br>The motor will be attached will also be a device.<br>  <br>And when combined it will show the feeder and motor running. |

| Device | Shape |
|---|---|
| |  |
| Off page Arrows |  |
| Pump |  |
| Silo |  |
| Tank | Requires approval by the Principal and Operations. |
| UV |  |
| Valve |  |

## 15.7.8. Pipework

Where pipes are displayed on graphics, the size of pipework shall vary to distinguish between main and auxiliary flow paths. The colour of the pipes shall be grey scaled as defined in “colour guidelines” table.

## 15.7.9. Cross over of lines

Pipes shall be orientated to minimise crossovers. Where crossovers are unavoidable, they shall be arranged by placing the main process flow over the minor. Where two minor process flows cross, a convention of precedence shall be established to be applied consistently throughout all the graphics for that plant.

## 15.7.10. Display Flow Convention

All flows (in pipe, duct, channel, etc.) shall enter and exit the graphic from the left or right perimeter of the graphic using an arrowhead to indicate direction. Any bidirectional flow (e.g., balance pipe) shall be contained solely within a single display as far as possible and shall not use arrowheads.

For bidirectional flow, the flow meter reading on SCADA graphics (or faceplates) shall indicate direction of flow in addition to flow value and measurement unit.

Process flows shall always be horizontal or vertical and all intersections shall be perpendicular. The process flow shall not form an overall zigzag (letter Z) path across the display due to the quantity of equipment to be displayed. Two graphics shall be used in such situations unless it is the overall plant overview, where for that graphic alone, all rules take secondary consideration to ensure that one graphic represents the whole plant.

## 15.7.11. Main process flows

Main process flows shall enter the display on the left and leave on the right following the convention that the upstream section of the plant is to the left of the graphic and the downstream section to the right.

Where space or symbol layout considerations permit, the relative heights of the entry and exit points shall indicate the process pressure gradient. A gravity treatment process shall enter high left and leave low right (no higher than the lowest in-line process element). Conversely, pump suction shall enter low left and delivery shall leave high right (no lower than the highest pump).

Where two (or more) graphics are connected in series, with multiple connections between the two, the height that a process flow exits the graphic shall be identical to the height that the same process flow enters the next display. In other words, both graphics to be treated as one, from the point of view of process pressure gradient.

## 15.7.12. Flow splits and feedback

Where possible Feedback flows shall be contained within a single page, when this cannot be achieved without negatively impacting display clarity, the following convention shall be applied.

Where the main process flow branches, if the off-take feeds back to an earlier portion of the process, it shall exit to the left. If the off-take feeds forward it shall exit to the right. Similarly, where process flows combine, if the combining line originates in an earlier portion of the process, it shall enter from the left. If it originates later in the process, it shall enter from the right.

Note: This guideline is for feedback flow such as backwash flow. Although contradicting the general left to right flow rule, it will better represent the actual process flow.

Feedback flows, which involve pumps, shall use the standard pump symbol with right facing delivery in all circumstances unless space restrictions make this impossible.

# 16. Communication Network

Following components are categorised under communication network for Control systems:

a. Ethernet switches
b. Routers
c. FOBOT
d. Media converters (including serial to Ethernet converters, Ethernet to fibre optic converters)
e. Protocol converters
f. Firewalls
g. GPS and its' associated equipment (Master clock, Modems etc.)
h. Radio Equipment (including radio modems, microwave etc.)
i. Mobile equipment (like antennas 4G/5G modems etc.)
j. Communication cards (for Modbus TCP/IP, Profinet, OPC etc.) installed in PLC racks
k. Communication cables (Serial, Cat 6a, Single mode Fibre optic cables etc.)
l. Software gateways
m. Communication software (including any virtual software's and/or licenses)

## 16.1. General Requirements

a. All communication network equipment shall be designed to operate continuously at rated designed load for 24 hours per day, 365 days per year.
b. Communication network equipment installed within air-conditioned building(s) shall operate without degradation in performance in temperature range of 10°C to 35°C. Industrial grade communication equipment is preferred in air-conditioned environment (where practical) so that the equipment can operate even in an air-conditioned failed environment.
c. Communication network equipment installed outside of air-conditioned building(s) shall be classified as "industrial grade" and shall operate without degradation in performance in temperature range of -5°C to 60°C.
d. The communication network equipment shall operate without degradation with relative humidity (non-condensing) in the range 10-95 % within the temperature range -5°C to 35°C and 10-75 % within temperature range of 36°C to 60°C.
e. All network communication equipment shall be designed for automatic restart and monitoring functionality after power supply interruption, without the need for any manual local reset(s).
f. All communication network devices (including Ethernet switches, Routers, GPS, Radio Modems) shall support SNMP logging level 2 as a minimum. In SNMP, logging level 2 is defined for "critical conditions".
g. Schedule and requirements for routine maintenance of communication network equipment shall be described in the operation and maintenance manual of control systems. Critical spares and consumables requirements shall also be included in the operation and maintenance manual.

h. For all greenfield projects Fibre shall be required.

The following communications protocols may be implemented for the SCADA, PLC, field RIO layer networks:

**Table 32: Network communication protocols**

| Protocol | SCADA | PLC | RIO |
|---|---|---|---|
| EtherNet/IP | | ✓ | ✓ |
| Profinet (preferred)/ Profibus(with Seqwater's consultation) | | ✓ | ✓ |
| ISO on TCP (Siemens S7 connection) | | ✓ | |
| Media Redundancy Protocol | ✓ | ✓ | ✓ |
| Rapid Spanning Tree Protocol | ✓ | ✓ | ✓ |
| Modbus TCP/IP | ✓ | ✓ | ✓ |
| OPC UA | ✓ | ✓ | |
| DNP3 | ✓ | ✓ | |
| Proprietary SCADA Protocols<br>Aveva CitectSCADA<br>Schneider ClearSCADA<br>Aveva System Platform<br>Aveva eDNA | ✓ | | |
| Proprietary PLC/RTU Programming Protocols<br>Siemens Step 7 Classic<br>Siemens TIA Portal<br>Schneider Unity Pro XL | | ✓ | |
| SAMBA File Share | ✓ | | |
| SNMP | ✓ | | |
| Control Services (Windows WSUS, Antivirus, Windows Active Directory, RDP, VNC, Backup) | ✓ | | |
| Layer 2 IP Protocols (DHCP) | ✓ | ✓ | ✓ |
| Layer 3 IP Protocols (eiGRP) | ✓ | ✓ | |

## 16.2. Performance Requirements

The following minimum performance requirements shall be met when designing Control systems communication network, unless otherwise specified in the Scope of Works. These requirements have been grouped as:

a. Local Area Network (LAN) requirements (includes remote IO Layer, PLC Layer and SCADA Layer as defined in I-SPE-STD-009 Control Systems Topology standard).

b. Wide Area Network (WAN) requirements (includes Control WAN as defined in I-SPE-STD-009 Control Systems Topology standard).

### 16.2.1. LAN Performance Requirements

**Table 33: Controls System LAN Performance Requirements**

| Class | Requirement |
|---|---|
| Reliability | Reliability Class: R4 (MTBF > 17520 Hours) |
| Availability | A > 99.99% (Downtime less than 0.88 hours/annum) |
| Data Integrity | IE ≤ 10-6 |

Data integrity, in the context of networking, refers to the overall completeness, accuracy and consistency of data. Data integrity shall be imposed when sending data through a network. If the data received isn't the same as the data sent on a network, then there is a problem, and it needs to be identified through error checking and correction protocols.

I-SPE-STD-009 Control Systems Topology standard shall be referred to for reliability and availability definitions for Control System LAN performance.

Care should be taken to avoid single points of failure for the communications network system and there should be no hidden failures (failures that are not identified in the control systems), especially for redundant elements in the design.

### 16.2.2. WAN Performance Requirements

The design requirements, connection requirements and network security requirements for Control WAN are specified in "WAN Connection Standard Specification" standard SPE-00392. The standard describes requirements for availability, latency, and bandwidth for Control WAN.

### 16.2.3. Surge Protection for Communication Network Equipment

Surge protection shall be supplied and installed for communication network equipment in accordance with:

1. AS/NZS 1768 Lightning protection
2. AS/NZS 4117 Surge protective devices for telecommunication application.

Surge protection shall meet the following requirements as a minimum:

a. SPDs (Surge Protective Devices) on each communication data cable running outside buildings or near higher voltage cables.

b. SPDs on all metallic communication lines which are not contained within the one building including any instrumentation and active network device.

c. SPDs on power supply cables (installed at both line side and load side) to network devices and switches.

d. SPDs shall be installed as per the manufacturer's guidelines.

e. All lightning arrestors shall be securely bonded to earth. Refer section 3.16 (Earthing) of *E-SPE-STD-001 Electrical Design and Construction* standard for detailed earthing requirements.

## 16.3. Network Communication Requirements

### 16.3.1. Control Networks

Sites shall include the following independent Ethernet networks as specified in *I-SPE-STD-009 Control Systems Topology* standard.

a. Field Remote IO Layer

b. PLC Layer

c. SCADA Layer

d. Control WAN

e. Device LAN

Field remote IO Layer, PLC Layer & SCADA Layer are categorised under the group "Control network".

Refer to I-SPE-STD-009 for further details about the Control network use.

### 16.3.2. WAN Site Connectivity

Remote site access and external datacentre connections are managed through the Control WAN and shall be designed and supplied by Seqwater ICT. Refer to I-SPE-STD-009 for inter site communication options.

Seqwater ICT shall supply and configure switch(es), router(s) and/or wireless router(s) for Control WAN interface. Refer "WAN Connection Standard Specification" standard SPE-00392 document for detailed specifications on WAN connections.

## 16.4. Wireless Communication

The requirements for wireless communications are applicable to plant control network as well as Control WAN network.

Telemetry (microwave, radio, mobile etc.) for remote assets such as dams, weirs, pumping stations and pipeline monitoring can be either Point-to-Point or Point-to-Multipoint and shall meet the following requirements:

a. Requirement for availability for wireless communication (for point-to-point or point-to-multipoint) shall be determined according to business requirements, or a value as specified in the Scope of Work for individual projects.

b. Any communication link with target availability requirement greater than or equal to 99.99% (downtime less than 0.88 hours/annum) shall require dual connection strategies utilising separate physical hardware and diverse network paths. Preferred topology for hardware redundancy in case of dual connection is active/active configuration. For example, in case of switch or router redundancy, both the switches or routers are hot and actively working.

c. Any communication link with target availability requirement greater than or equal to 99.9% (8 hours downtime) shall require spare hardware for communication equipment for emergency replacement, to be stored at Seqwater sites locally enabling replacement of failed equipment. It shall be the Contractors

responsibility to include these communication spares equipment in the list of “Critical spares”. It shall be made available to the Principal at the time of handing over of the project.

d. Communication network design shall support minimum bandwidth of 10 Mbps for any fixed wireless, microwave, 4G/5G connection. Minimum bandwidth for radio shall be equal to or greater than 50 Kbps.

Bandwidth refers to the transmission rate of a network connection, typically driven by the applications in use and the number of users using the service. It is measured in bits-per-second.

### 16.4.1. Point-to-Point

A point-to-point wireless connection refers to a communications connection between two nodes or endpoints. A WTP PLC communicating with single pump station PLC/RTU through wireless radio is a typical example of point-to-point communication. Cellular is not considered point-to-point and must only be deployed as part of the Control WAN.

The design requirements for Point-to-Point communications shall include the following as a minimum:

a. In case of radio, wireless ethernet radio communication shall be deployed

b. Shall support AES (Advanced Encryption Standard) 128 bits block size encryption

c. Automated re-routing following loss of communication layer (if alternative path available) shall be made possible. Any point-to-point network with routed (layer 3) redundancy shall have architectural input and be approval by the Principal.

d. ITU-R standard format such as STM-1 shall be supported

e. QAM (Quadrature Amplitude Modulation) capabilities shall be supported

f. Layer 2 switching capability shall be made possible

g. Shall support Integrated QoS (quality of service)

h. Native VLAN support shall be provided

i. Buffering of data for a minimum of half an hour at a transmitter level and/or receiver level shall be made possible during any event resulting in the loss of communication

j. Operate within the Australian Communications Authority LIPD (Low Interference Potential Device) Class License, notably 900Mhz, 2.4GHz, 5Ghz or 24Ghz

k. Point-to-point communication interface shall be designed such that the overall response time (i.e., the time between operator issuing the command from one node to the equipment operating in another node) is less than or equal to 3 seconds.

### 16.4.2. Point-to-Multipoint

A point-to-multipoint wireless communication is accomplished via a distinct type of one-to-many connection, providing multiple paths from a single location to multiple locations. A WTP PLC communicating to multiple pump stations PLC/RTU’s on wireless radio is a typical example of point-to-multipoint communication. Cellular is not considered Point-to-Multipoint and must only be deployed as part of the Control WAN.

The design requirements for Multipoint communications shall include the following as a minimum:

a. Minimum 30dB fade margin from repeater to each site

b. Capable of N+1 redundancy at points and paths levels

c. In case of radio, wireless ethernet radio communication shall be deployed

d. Shall support AES (Advanced Encryption Standard)128 bits block size encryption

e. Automated re-routing following loss of communication layer (if alternative path available) shall be made possible

f. Minimum 0.5 Fresnel in communication path

g. Operate within either the Australian Communications Authority LIPD or CB (Citizen Band Radio Stations) Class License ranges

h. Point-to-multipoint communication interface shall be designed such that the overall response time (i.e., the time between operator issuing the command from one node to the equipment operating in another node) is less than or equal to 4 seconds.

### 16.4.3. Poles and Antennas

When antennas are included as part of communication network infrastructure, the following shall be observed:

a. Depending on the application and the results of the radio signal strength survey, the radio antenna can be mounted on the top of the telemetry panel, the side of an existing structure (building or tower), or on a concrete tapered pole.

b. Where an existing structure is used for mounting antenna, the installation shall be designed to cater for safe access, adequate wind loading, and any structural calculations and modifications made to ensure compliance as per the manufacturer's recommendations.

c. Where a concrete pole is used, it shall be fitted with a ladder support for poles up to 8m high and shall be assembled and installed as per the manufacturer's recommendations. It shall be designed to cater for safe access.

d. The pole shall be designed and supplied to hold all the required antenna equipment with the adequate wind loading. The maximum allowable deflection criteria shall not be less than half of the narrowest beam width antenna.

e. Antenna cabling shall run inside the pole and underground to the switchboard. The conduit run between pole and switchboard shall be rigid conduit of a minimum size 32 mm. Large radius bends shall be utilised. Inspection and standard elbows are not acceptable.

f. Antenna cables shall be joined with an approved weatherproof connector and protected with a generous application of self-fusing splicing tape.

## 16.5. Communication Network Hardware

### 16.5.1. Communication Network Cabinet

All rack mountable communication network equipment and termination facilities for a site shall be housed in network cabinet(s) as defined by SPE-00321 Server Rack Assembly Specification. The communication network cabinet(s) shall be free issued to the Contractor unless specified otherwise in the SOW.

The communications cabinet shall use the same keying as that used for the SCADA Server racks.

GA (General Arrangement) and IGA (Internal General Arrangement) drawings of all communication cabinets shall be submitted to the Principal for approval prior to construction.

All Required Drawings shall be produced in accordance with the requirements set out in *I-SPE-STD-009 Control Systems Topology*, *X-PRO-STD-007 Drawing and Spatial Data Standards*, *X-PRO-STD-002 Engineering Drawing Number Procedure* and *X-PRO-STD-014 Drawings Management*.

### 16.5.2. Communication Network Outlets

Communication network outlets shall meet the following requirements as a minimum:

a. Outlets shall be dual RJ45 recessed mounted with pins up and all 4 pairs terminated to T568A sequence in accordance with AS 3080.

b. Outlets shall be CAT6a compliant to AS 3080 and are to be flush mounted and fit wiring duct of 35 mm depth.

c. LC fibre optic outlets shall be used for new projects. With principal's approval SC or SCA will be allowed as per the project requirement and to retain the existing type of connections. LCA shall be used for long-haul applications.

d. Samples of outlets shall be approved before installation (i.e., during the detailed design stage). Outlet faceplate colours shall match electrical outlets.

e. All outlets shall be labelled at both ends (walls as well as network cabinet end).

### 16.5.3. Ethernet Switches

Ethernet switches on the Control WAN shall be supplied and configured by Seqwater ICT.

The make and model of Ethernet switches on the Control network (Remote IO Layer, PLC Layer and SCADA Layer) shall be selected as per I-LST-STD-001, Control Systems Prescribed Equipment

All Ethernet switches shall include 25% spare copper port(s) capacity. If the switches contain fibre port(s), then 25% spare or one (1) spare fibre port shall be provided, whichever is greater.

Ethernet switches shall be powered with redundant power supplies and shall contain redundant power supply inlets, whenever the availability requirement of control systems is greater than or equal to 99.9%.

### 16.5.4. Serial to Ethernet Converters

Serial to Ethernet converters shall not be used for any interface requirements of the Control systems. The design shall select the Equipment (VSD, numerical relays, power meters, flow meters, communication cards of PLC etc.) that support inbuilt Ethernet port connectivity.

The Contractor shall take prior approval from Seqwater if the Equipment does not support inbuilt Ethernet connectivity and its interface with Control systems is required.

### 16.5.5. Copper to Fibre Optic Converters

The design shall avoid the use of copper to Fibre optic converters wherever possible. This can be done by selecting communication equipment (switches for example) that support inbuilt Fibre optic ports.

Prior approval from Seqwater is required if copper to Fibre optic converters are included in the Control systems architecture.

### 16.5.6. Protocol Converters

Protocol converter(s) shall not be used for any interface between systems. Due diligence shall be made during the selection of transmitting and receiving equipment to ensure that they both support common protocol, and their communication interface can be established without the need for protocol converter equipment.

Prior approval from Seqwater is required if protocol converters are selected in the Control systems architecture design

### 16.5.7. Fibre Optic Break Out Trays (FOBOT)

a. All fibre optic cabling shall be terminated in FOBOTs fitted with plug in fibre optic connectors.

b. FOBOT shall be mounted as close to the top of its network cabinet as practical.

c. FOBOTs shall be rack mounted or DIN rail mounted. FOBOTs shall not be side wall mounted.

d. All new termination/patch panels shall use LC and LCA (for long haul applications) type connectors unless approved by the principal.

e. All spare fibre optic cores shall be terminated and identified.

f. Each connector that is unused shall be fitted with a plastic dust cap at the completion of the fibre termination.

g. Cable management facilities shall be provided for all patch leads.

h. A warning notice detailing the hazards associated with optical devices shall be affixed to each termination enclosure in a prominent position.

## 16.6. Ethernet and Fibre Optic Cabling

### 16.6.1. Ethernet Cabling

Category 6A (Cat6a) Ethernet copper communication cabling (designed for transmission frequency to 500 MHz) shall be used to connect Ethernet capable devices located within a building (e.g., within equipment rooms, PLC enclosures and network cabinets).

a. Distance for Cat6a cable (Horizontal cabling between two connectors) shall not exceed 90 meters, and the distance between the patch panel and wall jack shall not exceed 10 meters on either side included.

b. Ethernet cabling shall be installed with the following minimum clearances if not installed within the conduits:

   i. 150mm from Piping

   ii. 150mm from LV Electrical Cabling

   iii. 450mm from HV Electrical Cabling

c. Standard RJ-45 quick connectors shall be provided to connect to LAN devices.

d. RJ-45 connectors shall meet class E characteristics.

e. Supplier approved cable and cable connectors shall be used for fabricating ethernet patch cables. The UTP cables shall have moulded snagless boots.

f. A site certification for installation and supply of UTP cables and associated equipment shall be provided by the Contractor at Practical Completion.

g. The communications rack supplied shall have dimensions to accommodate the minimum bending radius of Cat6a cabling. To accommodate this, the rack shall provide extra deep horizontal cable managers (e.g., for Panduit) and provisions for vertical cable management.

h. Ethernet cables installed for outdoor applications i.e., outside the buildings shall be UV sunlight resistant.

i. Ethernet cables when installed in electrically noisy environments (for example in switchboards or near to a drive) shall be industrial grade with the following specifications:

   i. Shall utilise bonded pair technology

   ii. Shall be shielded

   iii. Shall contain solid conductors

   iv. Installation stress resistant

   v. Shall contain industrial grade jacket

j. No cable ties shall be used to secure the ethernet/communication cables. Only wrap around labelling shall be used and 'hook and loop' fastener/strap shall be used for cable tie down. The cable tag will indicate the equipment at both ends denoted as "SXXXNNN – SYYYNNN Znnnn" with details as below. The cable shall have the same tag at both ends, e.g., 2PLC001-3RIO002 R1001, 2PLC001-3RIO003 R2001

| | |
|---|---|
| S: | Sub area number (X-PRO-STD-006, Section 7.3.3) |
| XXX: | Equipment code (Refer to Appendix A of X-PRO-STD-006), |
| NNN: | Equipment number |
| Z: | "S" = SCADA LAN; "P" = PLC to PLC LAN; "R" = RIO LAN, "D" = Device LAN |
| nnnn: | Unique cable number. User to take care that the number is spread across different subareas logically. |

k. The requirement of colour code for Ethernet cabling and tagging is listed in the below Table:

**Table 34: Standard Colour Code for Ethernet Cables**

| Application | Standard Cable Colour | Cable Tag |
|---|---|---|
| SCADA LAN | Yellow | Yellow |
| PLC LAN | Green | White |
| RIO LAN | Green | Green |
| Device LAN | Purple | Purple |
| Telephony (e.g., VOIP/PSTN) | Orange | Orange |
| Corporate LAN | Blue | Blue |
| Server management ports (iLO, DRAC) | Black | Black |

### 16.6.2. Fibre Optic Cabling

The fibre optic cables installed in duct, external tray, pits or direct buried and used for the purpose of Control systems, shall comply with the following requirements as a minimum:

a. Singlemode fibre should be used for new installations. Fibre attenuator shall be used on Singlemode fibre with shorter runs. The use of Multimode fibre will be restricted to less than 300 meters and shall be approved by the principal. Singlemode glass fibre shall be 9/125 µm (OS2) and if use of Multimode glass fibre is approved it shall be 50/125 µm (OM4)

b. Single mode fibre-optic cabling design shall provide sufficient bandwidth to support 10 gigabit communication.

c. Fibre cables and terminations shall be physically separate for the different applications (Control network, building Security, CCTV, Control WAN etc.)

d. Fibre optic cabling shall comply to requirements of AS/CA S009 and ensure that the installation does not expose the installer to any electric hazard. It shall also maintain minimum clearance of 150mm from any piping or other non-electrical hazardous services. The conductors and terminations of a Customer Cable shall be separated from the uninsulated and single-insulated conductors and terminations of an LV Power Cable by either a minimum distance of 150 mm or by means of a permanent, rigidly fixed barrier of durable insulating material or metal earthed.

All installations and product selection shall be undertaken as per Cabling Standards in Australian Communications and Media Authority (ACMA) AS/CA S009 and AS/CA S008 respectively and have the following minimum construction and features:

a. Complete non-metallic loose tube construction

b. Tubes shall be gel-filled to prevent ingress and axial migration of water, strengthened with flexible non-metallic armour bonded to the inner polyethylene sheath

c. Fibres and tubes shall be colour coded

d. For applications where underground laying is required, the cable shall have an outer protective jacket (nylon or polyurethane) and sacrificial sheath to protect the smooth, hard nylon jacket from being damaged during installation

e. A strain bearing, non-metallic member

f. Regardless of installation method (duct, external tray, pits or direct buried) the cable supplied shall offer a polyamide insect resistant jacket and rodent resistant armour

g. Surface printing includes marking at 1-metre intervals

h. A minimum of five (5) metres of spare cable shall be left at the termination ends (at both sides) of all cable installations

i. Fibre Optic cabling shall be installed in separate trays or conduits

j. Site based underground fibre optic cabling shall be installed in separate underground conduits where practical and secured to the side of cabling pits with additional aluminium protective covers to prevent possible damage.

k. Fibre optic cabling shall be designed in a ring topology for Class 2 and Class 3 architectures as per requirements specified in I-SPE-STD-009 Control Systems Topology standard. Fibres forming each part of the ring shall be in separate fibre cables, not cores in the same cable.

l. Fibre network shall have redundancy. Fibre shall be the primary communication path. Fibre is also the preferred communication path for redundancy. If fibre cannot be used for the redundant communication path, then Geo Satellite, Telecom network or Radio communications can be used after consultation with the principal.

m. The network shall be configured so that any single fault in the fibre network shall not result in loss of communication. For e.g., follow independent geographical routes

n. Fibre cable used for Intra-site shall be a minimum of 24 core and for Inter-site and pipeline it shall be a minimum of 48 core

o. Fibre cables shall provide a minimum of 25% spare core capacity (or four (4) spare cores, whichever is greater) in all fibre cables installations. Contractor to select the cable size in multiples of 12 (i.e., 24/36/48) which ever suits the spare requirement.

p. Fibre optic devices shall use pre-manufactured fibre patch leads for the connections to the patch panels.

q. Underground fibre optic cable shall include spare length at every second pit. Minimum 50mm conduit shall be used for underground installation of fibre optic cables.

r. The specifications for all fibre optic cables shall be submitted to the Principal for final approval prior to procurement of the cabling.

s. No cable ties shall be used to secure the fibre cables and/or its labelling. Only wrap around labelling shall be used and 'hook and loop' fastener/strap shall be used for cable tie down.

t. All fibre cables and cores(including unused) shall be labelled and spliced to FOBOT.

u. All unused FOBOT sockets/openings shall be sealed with termination/blanking plugs. Sufficient termination plugs shall be left within the FOBOT for all unused connections.

v. All fibre optic cores shall be fusion spliced, the splicer shall be suitable for the purpose intended. Mechanical splices shall not be used. The insertion loss of each splice in the fibre optic cable shall not exceed more than value stated in the latest AS/NZS ISO/IEC 14763.3.

w. The return loss shall meet the requirements mentioned in the latest AS_11801.1.

x. FOBOT faceplates shall be angled to eliminate the potential for patch lead boots to be pressed against a closed cabinet door. Installation of cable management panels is required above/below FOBOT.

y. Test equipment and testing procedures shall comply with the latest AS/NZS ISO/IEC 14763.3.

z. All Fibre cables shall be tested as defined in latest AS/NZS 11801.1 with following test result data requirements as a minimum. Detailed test results shall be provided for all cores as part of 'As Constructed' documentation and after any maintenance work is carried out on a fibre cable. If fibre is to be used prior to 'As Constructed', documentation being available, all cores showing a 'PASS' is required before any core is patched into service. The following shall be provided for each fibre cabling installation and after repair:

i. Light Source Power Meter (LSPM). Link and 'Insertion Loss' testing shall be conducted as per the latest AS/NZS ISO/IEC 14763.3. Test result data shall be provided in the native format supplied by the test equipment manufacturer.

ii. Optical Time Domain Reflectometer (OTDR) test results shall be conducted as per latest AS/NZS ISO/IEC 14763.3. All traces shall be provided in the OTDR's native format.

### 16.6.3. Overhead or Buried Installation of Fibre Optic Cables

When installed overhead, fibre optic installation shall use fibre optic aerial cable suitable for aerial installation and installed in accordance with all of the manufacturer's recommendations.

Single mode optical fibre used for either Control WAN applications or fibre optic cables installed between two sites, shall be a water blocked single loose tube non-metallic cable designed for long haul applications. These fibre optic cables shall be suitable for external tray, duct, and direct burial applications by either trenching or direct ploughing.

The minimum requirements of installation for the underground fibre optic cable shall be:

a. Cable to be rated for direct burial (underground conduits not required except for road crossings)

b. Minimum depth of cover shall be 600mm

c. Cable shall be suitable for direct burial. Sheath shall be rodent and termite resistant.

d. For a new installation contractor to provide a minimum 100m wide warning tape, 300mm above the buried cable. The warning tape shall be marked "Danger – Buried Communication Cable Below" and include a 316-grade stainless steel tracer wire to enable detection of the fibre optic cable route along the entire length.

e. For existing installation, wherever it is not possible to lay the steel tracer wire with fibre optic cable as per point d, a building wire will be installed along with a Fibre Optic cables.

### 16.6.4. Fibre Optic Cables Installation in Pits

In case of pits, the fibre optic cable is to be installed in one continuous length to avoid splicing in cable pits.

Fibre optic cables shall be kept clear of power cables (minimum 150mm from LV electrical cables and 450mm from HV electrical cables) in pits to maintain clear access to the power cables and for jointing work on the power cables. This includes avoiding the creation of restrictions to access to the pit, such as cables being passed too close to access ladders.

### 16.6.5. Fibre Testing

All fibre cores shall be tested after installation as per requirements specified in Communications Cabling Manual (CCM) HB29:2007 standard. Test sheets shall be submitted to Principal for approval. Test results shall include the following as a minimum:

a. Details of test instruments and method used for Fibre testing

b. Date of testing

c. Identification number for cables, fibres, and fibre cores

d. Measured length of fibres

e. Loss in dB

# 16.7. Network Security

## 16.7.1. Network Security Principles

The communication network shall be designed to prevent unauthorised access by denying, with access control on local routers, all traffic not specifically allowed to the Remote IO LAN, PLC LAN & SCADA LAN and to ensure that security is maintained at all times of operation.

The following security principals shall be incorporated as a minimum:

a. Provision for remote access through the centralised Seqwater ICT firewalls and VPN solutions provided by Seqwater ICT

b. Restricted access to SCADA information and configuration by user privilege levels

c. Centralised authentication of users and their privilege levels through control domain active directory. The implementation of control domain directory solution will enable the management and control domain for all SCADA systems (i.e., common, and consistent authentication, domain controllers, virus updates and software compliance capability).

d. Access Control Lists support on Routers and Switches.

## 16.7.2. Network Security Compliances

The Contractor shall comply with all the requirements specified in “Queensland Government Security Standard IS18” during the design, installation, and commissioning of communication networks. Seqwater is a “statutory authority” and as such is obligated to comply with IS18 standard.

The following standards are to be referred to as guidelines during the design, installation, and commissioning of communication networks:

a. ISO 27000 Standards

b. NIST (National Institute of Standards and Technology) Cyber Security Framework

c. AS/NZS 17799:2006 Information technology – Security techniques – Code of practice for information security management – Amendment 1:2008

d. Trusted Information Sharing Network (TISN) – Critical Infrastructure Resilience Strategy

e. Industry Best Practice (WaterIsac \ ISA).

# 17. Fieldbus Device Interface to PLC

Any fieldbus device (for example: Flowmeter, VSD, power meter, numerical relay etc.) shall communicate to the PLC for data acquisition and alarms. No fieldbus device shall communicate directly to a SCADA system unless approved by Seqwater.

All controls and interlocks signals between PLC and fieldbus device shall be hardwired. The communication interface between PLC and fieldbus device can be used for indication, feedback, and alarm purposes.

## 17.1. Flow meters

"M-SPE-STD-006 Bulk Supply Meters for Potable Water" standard shall be used to determine the IO requirements for bulk supply meters (revenue meters).

The flowmeter for control purpose shall provide as a minimum the following hardwired inputs to the PLC:

a. Flow Rate – Analog signal
b. Reverse flow rate (for bi-directional flow meters) – Analog signal
c. Direction Bit, where applicable – Digital signal
d. Flow meter general fault – Digital signal.

For any conflict of requirement for non-revenue meters with this standard and M-SPE-STD-009 Flow Meter, the requirement of the M-SPE-STD-009 shall take precedence.

## 17.2. Power meters

Where installed, power meters for switch boards and distribution boards shall communicate to PLC system and provide the following signals as a minimum:

a. Three phase Voltage
b. Three phase Current
c. Instantaneous Power
d. Instantaneous Apparent Power
e. Instantaneous Power Factor
f. Cumulative kWh
g. Maximum Demand (It is the maximum load recorded in last 24 hours)
h. Frequency.

## 17.3. Variable Speed Drives

Refer to E-SPE-STD-010 – Low Voltage Variable Speed Drives and Soft starters requirements for control and monitoring requirements. Contractor shall also refer to the applicable VSD schematic diagram in the E-SPE-STD-010.

There is a requirement to provide communication interface to PLC system for all three phase drives greater than or equal to 10kW. The following signals shall be made available through drive communication to PLC:

a. Drive communication Heartbeat
b. Instantaneous Power
c. Instantaneous Apparent Power
d. Instantaneous Power Factor
e. Three phase Current
f. Frequency
g. Three phase Voltage
h. Drive Temperature
i. Drive Winding Temperature
j. Bearing Temperature (at drive end and non-drive end)
k. Total Harmonic Distortion
l. Drive Reference Speed
m. Drive fault(s)
n. VSD fault (This signal is acceptable through communication interface for three phase drive less than or equal to 10kW)
o. Reference speed (This signal is acceptable through communication interface for three phase drive less than or equal to 10kW).

## 17.4. Soft Starters

Refer to *E-SPE-STD-010 Low Voltage Variable Speed Drives and Soft starters* requirements for control and monitoring requirements. Contractor shall also refer to the applicable VSD schematic diagram in the E-SPE-STD-010.

There is a requirement to provide communication interface to PLC system for all soft starters having rated current output of 50A or more and motor power output of 10KW or more.

The following signals shall be made available through soft starter(s) communication to PLC:

a. Operating hours
b. Switching cycles
c. Switch-off currents
d. Soft starter communication Heartbeat
e. Instantaneous Power
f. Instantaneous Apparent Power
g. Instantaneous Power Factor
h. Three phase Current
i. Three phase Voltage
j. Total Harmonic Distortion
k. Soft starter fault(s).

# 18. Control Systems Diagnostics

Control systems diagnostics is divided into three categories

a. PLC system diagnostics

b. SCADA system diagnostics

c. Communication network diagnostics.

Control systems diagnostics shall be historically logged and trended in the SCADA system. The associated alarms and events of Control systems diagnostics shall be made available in “Network overview graphic”.

## 18.1. General Requirements

a. Diagnostics shall be available for control systems components and IO modules including but not limited to controllers, SCADA clients, SCADA servers and communication equipment like switches and routers.

b. It shall be possible to monitor the status (online, offline etc.) and diagnostics (healthy, fault etc.) of all network connected fieldbus devices (including VSD, numerical relays, power meters, flow meters etc.) from the engineering station.

c. The operating system of fieldbus devices shall offer health status monitoring (of the state of all devices) and generate an event message to SCADA when a change is detected.

d. If a fault in a back-up device is detected, the operator shall be notified through SCADA and the fault shall be logged in SCADA.

## 18.2. PLC Diagnostics

The table below describes PLC diagnostics alarms and events that shall be made available in SCADA system.

**Table 35: PLC System Diagnostics**

| Diagnostic Alarm Description | Requirements to Generate the Alarm | Alarm Priority | Comments |
|---|---|---|---|
| SCAN Time error | If the PLC program exceeds the maximum scan time assigned in CPU configuration, then this alarm shall be generated. Default maximum scan time configured is 150mS for low end, mid-range or high-end CPU | Priority 3 | Applicable for both standalone controller as well as redundant controllers |
| CPU redundancy error | Loss of CPU redundancy shall be generated in the following conditions but not limited to:<br>Reserve-master switchover<br>Synchronization error<br>Error in a SYNC module<br>Comparison error (for example, RAM, PIQ) | Priority 4 | Only applicable for redundant controllers |

| Diagnostic Alarm Description | Requirements to Generate the Alarm | Alarm Priority | Comments |
|---|---|---|---|
| Power supply error | This error is generated in the event of a battery fault within the CPU.<br>Power supply module installed at remote IO nodes shall also generate this diagnostic alarm during failure condition | Priority 4 | Applicable for both standalone controller as well as redundant controllers.<br>Individual module diagnostic is required for power supply module |
| Module diagnostic fault (for analog input modules) | The diagnostic interrupt of the IO module shall generate this alarm. Seqwater requires that analog input module fault shall be generated when:<br>Channel temporarily unavailable<br>Short-circuit (current, 2-wire transducer)<br>Low limit violated<br>High limit violated<br>Module Error<br>Parameter assignment error<br>No load voltage | Priority 3 | Applicable for both standalone controller as well as redundant controllers.<br>Individual module diagnostic is required for Analog input module.<br>Individual channel level diagnostic is not required.<br>Unused analog input channels to be disabled in the configuration |
| Module diagnostic fault (for analog output modules) | The diagnostic interrupt of the IO module shall generate this alarm. Seqwater requires that analog output module fault shall be generated when:<br>Channel temporarily unavailable<br>Short-circuit (voltage)<br>Over temperature<br>Low limit violated<br>High limit violated<br>Module Error<br>Parameter assignment error<br>No load voltage | Priority 3 | Applicable for both standalone controller as well as redundant controllers<br>Individual module diagnostic is required for Analog output module<br>Individual channel level diagnostic is not required<br>Unused analog output channels to be disabled in the configuration |
| Module diagnostic fault (for digital input modules) | The diagnostic interrupt of the IO module shall generate this alarm. Seqwater requires that digital input module fault shall be generated when:<br>Load voltage missing | Priority 3 | Applicable for both standalone controller as well as redundant controllers<br>Individual module diagnostic is required for Digital input module<br>Individual channel level diagnostic is not required |

| Diagnostic Alarm Description | Requirements to Generate the Alarm | Alarm Priority | Comments |
|---|---|---|---|
| Module diagnostic fault (for digital output modules) | The diagnostic interrupt of the IO module shall generate this alarm. Seqwater requires that digital output module fault shall be generated when:<br>Load voltage missing<br>short-circuit | Priority 3 | Applicable for both standalone controller as well as redundant controllers<br><br>Individual module diagnostic is required for Digital output module<br><br>Individual channel level diagnostic is not required |
| CPU Hardware fault | The operating system in the CPU generates this fault when:<br>After memory errors have been detected and corrected<br>For redundant CPU: if there is reduced performance of the redundant link between the two CPUs<br>Error in operating system | Priority 3 | Applicable for both standalone controller as well as redundant controllers |
| Rack failure fault | Rack failure of the controller rack as well as remote IO rack shall generate this fault | Priority 3 | Alarm masking shall be done in the PLC while generating this alarm. If the rack failure fault is generated, then all the module(s) and channel(s) failure alarms associated with the rack shall be masked. |
| Remote IO node Error | Failure of remote IO node in the PLC system shall generate this error | Priority 3 | Alarm masking shall be done in the PLC while generating this alarm. If the remote IO node error is generated, then all the module(s) and channel(s) failure alarms associated with the remote IO node shall be masked. |

## 18.3. SCADA System Diagnostics

The table below describes SCADA system diagnostics alarms and events that shall be made available in control systems.

**Table 36: SCADA System Diagnostics**

| Diagnostic Alarm Description | Requirements to Generate the Alarm | Alarm Priority | Comments |
|---|---|---|---|
| SCADA servers redundancy switchover alarm | An alarm shall be generated whenever there is a switchover between primary and secondary SCADA server | Priority 4 | Applicable only in case of redundant SCADA configuration |
| SCADA servers loss of redundancy error | This alarm shall be generated in the following conditions:<br>The SCADA servers stops functioning in redundant mode OR<br>Both the primary and secondary servers become Masters OR<br>Both the primary and secondary servers are backup (i.e., there is no Master) OR<br>One of the servers is faulty | Priority 4 | Applicable only in case of redundant SCADA configuration |
| SCADA servers synchronization error | An alarm shall be generated whenever there is a loss of synchronization (or improper synchronization) between primary and secondary SCADA servers | Priority 4 | Applicable only in case of redundant SCADA configuration |
| SCADA server GPS time synchronization error | If the SCADA servers are connected to the GPS clock, then an alarm shall be generated whenever SCADA servers loses time synchronization with the GPS clock | Priority 4 | Applicable for both standalone SCADA server as well as redundant SCADA servers. |
| SCADA server hard disk free space alarm | A SCADA alarm shall be raised if the remaining free hard disk space in the SCADA server falls below a configured value (i.e., 10% of the rated memory capacity) | Priority 4 | |
| Historian process alarm | Whenever the historian process in the SCADA server stops running and/or historical logging is interrupted, an alarm shall be generated.<br>An historian can be an inbuilt historian in SCADA server machine, or it can be a dedicated separate machine for historian, in both scenarios “historian process alarm” shall be generated. | Priority 3 | |

## 18.4. Communication Network Diagnostics

The table below describes communication network diagnostics alarms and events that shall be made available in SCADA system.

**Table 37: Communication Network Diagnostics**

| Diagnostic Alarm Description | Requirements to Generate the Alarm | Alarm Priority | Comments |
|---|---|---|---|
| Remote IO LAN fault | Any hardware or software fault in the remote IO network shall generate this alarm. Most of the time, this alarm is generated from layer-2 managed switches forming remote IO fibre optic ring network | Priority 3 | Individual module diagnostic is required for remote IO network switches |
| PLC LAN fault | Any hardware or software fault in the PLC Layer network shall generate this alarm. Most of the time, this alarm is generated from layer-2 managed switches forming PLC fibre optic ring network | Priority 3 | Individual module diagnostic is required for PLC Layer network switches |
| SCADA LAN fault | Any hardware or software fault in the SCADA Layer network shall generate this alarm. Most of the time, this alarm is generated from layer-2 managed switches forming SCADA fibre optic ring network | Priority 4 | Individual module diagnostic is required for SCADA Layer network switches |
| Individual port diagnostic alarm from switch(es) | All the ethernet or fibre optic switches used in the communication networks shall generate individual port diagnostics. These alarms shall be made available to SCADA system through SNMP protocol | Priority 4 | Individual port diagnostics shall be made available from switches forming the remote IO ring (or star) network, PLC Layer network, SCADA Layer network or Control WAN network |
| Communication module(s) fault alarm | All the communication interface module(s) used in the control systems shall generate “communication module alarm” during any hardware or software fault condition which results in the malfunctioning of the module. Typical communication interface module includes but not limited to:<br>OPC communication module,<br>PLC to SCADA communication module,<br>Remote IO interface module,<br>Profinet interface module,<br>Profibus interface module,<br>Modbus TCP/IP (or serial) interface module,<br>4G/5G communication interface module or modem | Priority 3 | Logic takes the control value to Fail safe condition after certain time |

# 19. Changes from previous version

This Standard Specification will be regularly reviewed and updated, including the consideration of requested alterations, in accordance with Seqwater Procedure X-PRO-STD-004 Development and Review of Asset Standards. The table below notes the changes from Rev 06 to Rev 07.

This Standard Specification will be regularly reviewed in accordance with the requirements of the Seqwater Controlled Document Management Procedure. Reviews will include consideration of suggestions for alteration or improvement made in accordance with Seqwater Procedure X-PRO-STD-004 Development and Review of Asset Standards. Changes made from the previous version are summarised in Table 38 below.

**Table 38: Changes from previous version**

| Section Number | Change |
|---|---|
| 6 | Removed I-DSH-STD-072 PLC Standard Block Datasheet – Supervisory Control |
| 6 | Included I-SPE-STD-022 Supervisory Control and Data Acquisition (SCADA) Objects |
| 6 | Included I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification |
| 6.2 | Included AS/CA S008 Requirements for Customer Cabling Products |
| All | Replaced I-DSH-STD-072 PLC Standard Block Datasheet – Supervisory Control with I-SPE-STD-020 Programmable Logic Controller (PLC) Blocks Specification |
| 9.8.1.d | Only ELV equipment/s shall be allowed in new PLC cabinets. Removed requirements of IP2X rating for 230V to be included in PLC cabinets. |
| 9.8.2.d | No sidewall mounting of gear tray/s or devices shall be allowed |
| 9.8.2.a | Changed to 50VAC or 120VDC |
| 10.2.s | All PLC to SCADA communications shall be through a software-based OPC server using the OPC UA protocol. |
| 11.3.3.a | SCADA server cabinet(s) shall comply with SPE-00321 Server Rack Assembly Specification |
| 12.3.5 | Updated Alarm Dialler section |
| 13.1 | Added reference to I-SPE-STD-020 - Programmable Logic Controller (PLC) Blocks Specification |
| 13.2 | Added reference to I-SPE-STD-22 Supervisory Control and Data Acquisition (SCADA) Objects |
| 16.5.7.c | Added FOBOTs shall not be side wall mounted. |
| 16.6.1.j | No cable ties shall be used to secure the ethernet/communication cables. |
| 16.6.2.l | Added fibre network redundancy |
| All | Changed name of standard I-SPE-STD-009 Control Systems Topology |
| | |

# 20. Verification

Compliance with this document may be verified by internal audit.

# 21. Further Information

For further information please contact the owner of this document.