NWC STANDARDS & SPECIFICATIONS FOR SCADA & INSTRUMENTS

National Water Company

Riyadh Business Unit

Saudi Arabia

DOCUMENT TITLE: **NWC Standards & Specification for SCADA & Field Instruments**
DOCUMENT TYPE: **Standards**
DOCUMENT Owner: **Smart Operations General Manager**
REVISION: **3.0**

SUMMARY OF AMENDMENTS:

Rev #	Date	Page #	Section	Initiated By	Nature Of Amendment
3.0	10/9/2019	All	All	Masoud Alanazi	Revised & Updated all the document

Table of Contents

CHAPTER-1

INTRODUCTION

1. Introduction:

The National Water Company (NWC) SCADA standards document provides a standardized approach to SCADA system and infrastructure development and implementation within its jurisdiction. In order to ensure consistency in SCADA and control system design as well as electrical and instrumentation equipment procurement and implementation, which may from time to time be completed by different consultants for a given project, it is imperative that the standards be followed. NWC requires that these standards are followed by those consultants wishing to carry out work within its jurisdiction.

The purpose of this section is to provide standards and other technical information from which vendors, contractors and ACWWA personnel can create PLC, computer and SCADA programs, graphics and other documents. In addition, this section will provide specific information on PLC and input-output module hardware as well as electrical and instrumentation equipment manufacturers. This section provides a set of guidelines, that when followed, will result in software that is consistent with the rest of NWC operations.

1.1 Terminologies

The following table lists acronyms used throughout this document:

Acronym	Definition
HMI	Human-Machine Interface. A set of graphics driven screens run on
I/O	Input / Output. Field devices connected to a PLC that interfaces with instrumentation, equipment and communications gear.
IT	Information technology.
PLC	Programmable Logic Controller. A small process computer located in the field or near the equipment being controlled.
RTU	Remote Telemetry Unit. A unit in the field, a well site, for example, that consists of a PLC, I/O cards, radio link and an enclosure.
SCADA	Supervisory Control And Data Acquisition. A broad term that covers computer programs that provide a graphical interface to all processes that make up the NWC

	operation. Historical data collection, trending and reporting also fall under this umbrella.
NWC/RCBU	National Water Company/RIYADH CITY BUSINESS UNIT
HQ	NWC Head Quarters
PTFE	Polytetrafluoroethylene
OT	Operation Technology
RFP	Request for Proposal
MCC	Motor Control center
IO/DI/AI	Input Output / Digital Input/ Analog Input
VFD	Variable Frequency Driver
SDI	Silt Density Index
STP	Sewage Treatment plant
RPM	Rotations Per Minute
TCP/IP	Transmission Control Protocol/ Internet Protocol
TUV	TUV certification means a sampling of the product has been tested for safety and found to meet the minimum requirements of the German Equipment and Product Safety Act.
DMA/DMZ	District Metering Area / District Metering Zone
HYSD	High Yield Strength Deformed Steel
CITC	Communication And Information Technology Commission

CHAPTER-2

Design Philosophy and Guidelines

2. Design Philosophy and Guidelines

2.1 General

The overall goal of the standards is to ensure that all new construction can properly integrate into the existing central SCADA systems. They should also have the same "look and feel" so to ensure continuity for the operators across all of NWC. The standards also ensure that all upgrades and expansions to existing infrastructure is carried out to the same standard.

2.2 Purpose

This document intends to outline the standards and regulations to govern the features and technical aspects of all projects and RFP's pertaining to SCADA and ICS (Industrial Control Systems). The goals of standardization are to ensure that consistency for operations, maintenance, engineering, and management, as well as the regulatory compliance and procurement departments.

2.3 Control Modes

2.3.1 Sequence of Operation

The general description for the Sequence of operation:

MCC Control Panel has two Mode:

- Local Mode : (MCC Local Control Mode)
- Remote Mode : (SCADA Control Mode)

2.3.1.1 Local Mode

Selection of Local mode is done when the auxiliaries are to be controlled Locally i.e. via MCC. In this position there are two modes which can be chosen by operator:

Hand Mode: The Start/Stop for equipment should have local push buttons located on the local control panel. This position is out of PLC control. The operator controls the equipment with local on/ off pushbuttons.

Auto Mode: (MCC Local Auto Operation Sequences) uses microcontroller with hardware AI or DI signals.

Selection of local mode is done when the auxiliaries are to be controlled locally. It can have three options to be controlled locally:

- Local Control Panel (hand mode)

- MCC Control Panel (electric circuit)
- Remote Auto (PLC)

2.3.1.2 SCADA Mode (Remote Mode)

Selection of SCADA mode or Remote mode is done when the auxiliaries are to be controlled remotely i.e. via SCADA workstation (Central SCADA Workstation). In this position there are two Modes, which can be chosen on SCADA workstation.

Automatic Mode: The equipment is controlled by PLC without any operator intervention. The Auxiliaries are controlled as per the preprogrammed interlocks as advised by the client's requirements. During changeover from manual to Auto mode, equipment will start or stop depending upon Auto start interlocks at that point of time. It is not recommended to change from manual to auto mode when the equipment is in running condition or the valve is in open position. We recommend operator to stop the pump and close the valve and then change it to Auto mode.

Manual Mode: The equipment is controlled manually by operator from SCADA. During Change over from Auto to manual mode, equipment will remain in its last position for a smooth transfer. For example, if the pump/valve is running/open in auto mode and if operator has selected it to manual mode, pump/valve will keep running/open till it is switched off manually from SCADA workstation.

When the operator turns the switch to remote position, he should select Automatic Mode or Manual Mode on SCADA

- Pump run hours and minutes are calculated in PLC based on the run status (Run Feedback) from MCC (in any mode) and it will be displayed on SCADA screen for operator reference. Two types of Run hours will be calculated 1) daily run hours, 2) Reset able run hours. SCADA Supervisor or SCADA administrator has rights to reset the run hours & minutes from SCADA screen, 3) none resettable run, SCADA Supervisor or SCADA administrator has rights to reset the run hours & minutes from SCADA screen (Total Hours).
- For both Manual and Automatic mode of operation, start and stop interlocks are provided for safety of the pumps and open and close interlocks are provided for the safety of the valves.
- Pump Fail to RUN fault will be generated if there is no RUN feedback with in time delay of defined seconds (programmable) of start command from PLC.
- Valve Fail to OPEN or CLOSE fault will be generated if there is no OPEN or CLOSE feedback with in time delay of defined seconds (programmable) of start command from PLC.

- Logical Alarms along with color animation appears on screen describing fault. A fault alarm will appear on the SCADA workstation. Operator can reset the Fail to start fault by pressing RESET/ACK button on the pump control popup screen after the fault is rectified by maintenance staff. Operator can also reset the Fail to OPEN or CLOSE fault by pressing RESET/ACK button on the valve control popup screen after the fault is rectified by maintenance staff. Without resetting this fault, pump or valve cannot be started from PLC. Pump cannot be started in automatic mode or manual mode as long as the fault signal appears. Valve cannot be open or close in automatic mode or manual mode as long as the fault signal appears.
- Hardware Alarms (Overload, Temp, etc) cannot reset from SCADA ever unless the hardware fault is rectified by maintenance staff.
- Pump start and stop interlocks are provided for safety of the pumps & to achieve operation philosophy needs.

2.4 Control Philosophy

A system or a complete site is usually spread over a long geographical distance. SCADA is the central system for control and monitor of such a site or system. A Programmable Logic Controller (PLC) or a Remote Terminal Unit (RTU) automatically performs the main site control process. The host control functions in most cases are limited to the capability of supervisory level or site override.

- Automatic/Manual selector switches is to be provided on each field station for selecting the control mode for each individual device or piece of equipment.
- Manual controls will only function when the selector is in the Manual position.
- Computer control will only occur when the selector is in the Automatic position.
- A discrete contact will be present to provide an indication to the computer that the device/equipment is in Automatic mode, and available for computer control.
- Control circuits will be designed such that transfer between Automatic and Manual conditions does not affect operation of the equipment/device ensuring a smooth transfer. The physical switching between Automatic and Manual will not change the ‘pre-‘switch conditions by itself.
- Automatic to Manual A motor will continue to operate in its previous state (on or off) until manually changed at the Local Control Panel; a valve will carry out its last instruction for settings (open/close/in between), prior to accepting further manual instruction. (In some valves cases its

depend of valves plate settings), and in other cases its depend of the auxiliary contact relay set (normally open or normally close)

- Manual to Automatic: The computer will override the Manual local instructions, and resume automated control, using its evaluation of the conditions and parameters that are programmed to indicate start/stop or open/close of the equipment in question with fully auto sequences according to the approved philosophy
- The designer will be required to evaluate all conditions for bump less transfer between Auto and any Manual condition.

2.5 Alarms

The SCADA system should allow for the functionality of alarms to be announced against user defined limits (Alarm Points). The priority of the alarms will be defined by the user which covering all risks on the sit (safety alarm, operational alarm, security alarm, Etc.) The alarms should be logged and retained in the SCADA historian database with deferent level of escalation or physical alarm system depending on approved condition by the owner.

2.6 Safety and Permissive Interlocks

Equipment and personnel safety interlocks should always be locally hardwired, to operate independently of the automated control system:

- Well/ wet well Low Level Switch (prevent pumps from running dry).
- Pump discharge Valve Limit Switch (prevent pump operation against closed valve)
- Pump Seal Water Pressure/ Flow/ leakage (prevent pump operation w/o seal water)
- Lock-outs should consist of disconnect-style switch complete with padlock connection.
- Motors controlled by computer or other automatic means should have a power disconnect switch. This switch should be located on a local panel within sight of the motor.
- An auxiliary contact for the disconnect will also be present, which will be open when the switch is open. This will prevent operation of the starter coil, or a starter contact, which would give a false 'Motor Running' reading to the computer.

2.7 Prepackaged Equipment Interfaces

- Equipment such as chemical make-up systems are often part of a complete system package with their own instrumentation and controls.

- It will be necessary for the control systems designer to evaluate and incorporate these existing controls and monitoring capabilities into the overall system being constructed. This will include definition of process variables, and alarm & status conditions to be monitored by the system, plus any controls for which the system should operate the equipment.
- Any interfacing should be documented within both the mechanical equipment and electrical specifications, to ensure system co-ordination and compatibility.

CHAPTER-3

Facility Design

3. Facility Design

The facility design will be site specific to individual process elements and operational requirement. Each facility will have a template developed for each process element will incorporate:

- Analytical & precision instruments
- PID Control Loop
- Trends
- Protection
- Alarms
- Reports

An example of a template can be seen in Appendix A & B

Some examples of the facility design can be seen below.

3.1 Water Treatment Plants

As a minimum, the following monitoring and control in each process in water treatment plants should be provided and the PLC should to collect all existing IO's (Redundant PLC if applicable). All safety requirements & protection should be connected to automation system and running in auto mode

3.1.1 Wells

- Pump alarms (Overload, Vibration, Temperature, Leakage …etc.) (if applicable)
- Pump motors current if present through soft-starters or VFD equipment.
- Pump and valves status and fault signals
- Outlet flow, total flow, pressure, well level and temperature (if applicable)

3.1.2 Cooling System

- Cooling system alarms (Overload, Vibration, Leakage …etc.) (if applicable)
- Inlet & Discharge flow & total flow and Temp (if applicable)
- Precipitator Level with alarms (if applicable)
- Discharge valves status (if applicable)
- Fan motors current if present through soft-starters or VFD equipment.
- Fan and valves status and fault signals

3.1.3 Precipitator

- Inlet & discharge flow, total flow, turbidity and temperature.
- Precipitator Level with alarms (if applicable)
- Discharge control valve position (if applicable).
- Pumps & valves status and fault signals

3.1.4 Softener

- Inlet & discharge flow
- Suction tank level with alarms (if applicable)
- Delivery control tank level with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pumps motors current through soft-starters or VFD (if applicable)
- Pump and valves status and fault signals
- Moister level (submersible pumps)
- Vibration, temperature & leakage (if applicable)

3.1.5 Chemicals

- Inlet & outlet flow, total flow & pressure with alarms
- Tanks level, turbidity, chlorination, iron, SDI and pH values with alarms (if applicable)
- Suction tank level with alarms (if applicable)
- Pumps motors current through soft-starters (if applicable)
- Pumps and valves' status and fault signals
- Delivery Control Tank Level with alarms (if applicable)
- Discharge control valve position (if applicable)

3.1.6 Filters

- Status and fault signals of inlet & output filter valves
- Delivery control tank level with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pumps motors current through soft-starters or VFD (if applicable)
- Pumps, air blowers and valves' status and fault signals
- Outlet flow, total flow, pressure , filter level, turbidity and pH values (if applicable)

3.1.7 Mixing Tank

- Outlet flow, total flow, tank level & pressure
- Turbidity, chlorination, temp. and pH with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pumps and valves' status and fault signals

3.1.8 Dechlorination

- Outlet flow, total flow & pressure values
- Tank level and chlorination with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pumps & valves' status with alarms

3.1.9 Reverse Osmosis (RO)

- Inlet & outlet flow, total, flow & pressure with alarms
- Tank level, turbidity, chlorination, iron, SDI and pH values with alarms (if applicable)
- Suction tank level with alarms (if applicable)
- Control valve position (if applicable)
- Pumps' status alarms (overload, vibration, temperature, leakage …etc.) (if applicable)
- Pumps motors current if present through soft-starters or VFD equipment.
- Pumps and valves' fault signals
- Delivery and Discharge Pressure with alarms
- Moister level (Submersible Pumps)

3.1.10 Power Stations

- Electrical Overload alarms
- Status and fault signals of switches, circuit breakers and transformers.
- Status and fault signals of capacitors and batteries.
- Voltage and current magnitudes & total values with alarms
- Generator IO's (Start, Stop, Run FB, Local, Remote…etc.) (if applicable)
- Generator alarms (Temp., Vibration, Oil level …etc.) (if applicable)

3.2 Environmental Water Treatment Plant

As a minimum, the following monitoring and control in each process in waste water treatment plants (STP) should be provided and the PLC should to collect all existing IO's (Redundant PLC if applicable)

All safety requirements & protection should be connected to automation system and running in auto mode

3.2.1 Inlet Work & Screening System

- Gates' status and fault signals
- Inlet flow & total flow values
- Oder and gas analyzer status and fault signals
- Delivery control tank level with alarms (if applicable)
- Valves' position, status and fault signals (if applicable)
- Pumps status and fault signals
- Pump motors current & voltage with alarms (if applicable)
- Outlet flow, total flow, pressure, well level and temperature (if applicable)

3.2.2 Aeration

- Pumps, air blowers and valves' status and fault signals
- Outlet flow, total flow, pressure, filter level, turbidity and pH values (if applicable)
- Aeration system alarms (Overload, Leakage …etc.) (if applicable)
- Level with alarms (if applicable)
- Discharge valves status (if applicable)
- Pumps motors current if present through soft-starter
- Pumps and valves status and fault signals

3.2.3 Clarifiers & Thickeners

- Inlet & discharge flow, total flow, turbidity and temperature.
- Discharge control valve position (if applicable).
- Pumps & valves' status with alarms
- Inlet & discharge flow, total flow, turbidity and temperature.
- Clarifiers Level with alarms (if applicable)
- Discharge control valve position (if applicable).

- Pumps & valves status and fault signals
- Pump motors current if present through soft-starters or VFD equipment

3.2.4 Dryer System (Decanters or Belt Press)

- Inlet & discharge flow
- Suction tank level with alarms (if applicable)
- Delivery control tank level with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pump motors current if present through soft-starters or VFD equipment.
- Pump and valves status and fault signals
- Vibration & temperature with alarms (if applicable)

3.2.5 Filters & Tertiary

- Status and fault signals of inlet & output filter valves
- Discharge control valve position
- Pump motors current if present through soft-starters or VFD equipment.
- Pump and valves status and fault signals
- Moisture level (Submersible Pumps)
- Discharge control valve position (if applicable)
- Pumps, air blowers and valves' status and fault signals
- Outlet flow, total flow, pressure , filter level, turbidity and pH values (if applicable)
- Delivery control tank level with alarms (if applicable)
- Discharge control valve position (if applicable)
- Dissolved Oxygen meters to install

3.2.6 Chlorination

- Discharge control valve position (if applicable)
- Chlorine tanks and valves' status and fault signals
- Dampers fan status and fault signals
- Chlorine detectors status and fault signals
- Temperature status

- Pump and valves' status and fault signals

3.2.7 Power Stations

- Electrical Overload alarms
- Status and fault signals of switches, circuit breakers and transformers.
- Status and fault signals of capacitors and batteries.
- Voltage and current magnitudes & alarms
- Generator IO's (Start, Stop, Run FB, Local, Remote…etc.) (if applicable)
- Generator alarms (Temp., Vibration, Oil level …etc.) (if applicable)

3.3 Pumping Stations

As a minimum, the following monitoring and control in each process in pumping stations should be provided and the PLC should to collect all existing IO's (Redundant PLC if applicable)

- Discharge flow, total flow, tank level & pressure
- Pressures for each pump's inlet suction and discharge
- Suction Tank Level with alarms (if applicable)
- Delivery Control Tank Level with alarms (if applicable)
- Discharge control valve position (if applicable)
- Pump motors current and voltage values with alarms
- Pumps and valves' status and fault signals
- Moister level (Submersible Pumps)
- Vibration, Temperature & Leakage (if applicable)
- Running hours values with alarms

3.4 Reservoirs

As a minimum, the following monitoring and control in reservoirs should be provided, and the PLC should to collect all existing IO's (Redundant PLC if applicable)

- Tank level with alarms
- Inlet & Outlet Flow (if applicable)
- Inlet & Outlet Pressures (if applicable)
- valve position (if applicable)
- Valves status and fault signals
- Discharge chlorine residual

- Where applicable for health and safety reason, process optimization, optimal chemical usage, process automation, remote process control operational decisions, site security, and/or required for compliance reporting C of A requirements) the following monitoring should also be provided:
    - Pre-chlorination chlorine residual if chlorine is added at facility.
    - Post fluoridation fluorine residual if fluorine is added at facility.
    - Chemical storage tank volumes and chemical feed volumetric flow rates for each chemical and chemical feed line. Chemical, for purposes of this clause is defined as any addictive used to enhance the treatment process.
    - Chlorine storage volumes, volumetric flow rates for each chemical feed line, dosage and chlorine residual on the discharge side at locations with chlorination.

3.5 Distribution Chambers

As a minimum, the following monitoring should be provided.

- Line Pressure
- Where pressure regulation is provided, individual line pressure for each line upstream and downstream of the pressure regulation device.
- Where applicable for health and safety reasons, process optimization, optimal chemical usage, process automation, remote process control operations decisions, site security, and/or required for compliance reporting C of A requirements), the following monitoring should also be provided.
    - Dangerous gasses should be represented by levels in ppm and should be provided in all locations where there exists the possibility of gas collection and/or oxygen depletion that are not classed as confined spaces.

3.6 Gates and Valves

The criteria for degree of monitoring and / or controlling of gates and valves are dependent upon both the type of, and frequency of, use of the unit itself.

3.6.1 Open/Close Control Valves

Monitoring of fully open and fully closed positions is required for automated flow routing devices. Travelling indication should be included for larger valves. Also, the valve fault signals should be provided which indicate either valve jam or motor fault.

3.6.2 Modulating Control Valves

All operating valves for which intermediate positions are set by controller or keyed input require, as a minimum, limit switches for fully open and fully closed positions. A 4-20 mA DC signal for monitoring valve position between open and closed will generally be required, based on the process requirements. Also, the valve fault signals should be provided which indicate either valve jam or motor fault.

Where specified, limit switches and position sensors are to be furnished by the manufacturer, as an integral part of the gate or valve unit.

3.6.3 Monitored Valves

Hand operated valves should have limit switches for both fully open and fully closed positions, as a minimum.

Monitoring requirements for gates and valves, which are not part of the normal process or operation, will be a function of the amount the gate / valve is used. The threshold for valve use frequency will be established by the Primary Water Supply and is to be evaluated by the designer. Those units used for maintenance or isolation (e.g. pump suction valves or routing isolation valves) should not be monitored, unless an improper position creates a safety hazard.

Monitoring requirements for gates and valves, which are used under emergency or non-standard conditions (Bypassing), should include monitoring of fully open, and fully closed.

To avoid any unexpected power failure or PLC stop mode its very importance to specify the valve auxiliary contact relay should be normally open or normally close in this case.

3.7 Electric Motors

The following physical parameters are to be monitored for all electric motors:

- Fault condition.
- Motor Running/stopping status
- Motor current if provided by a soft-starter or a VFD.
- Motor running hours
- RPM (if applicable)

These additional parameters are to be monitored for larger electric motors over 100kW:

- Bearing Temperature
- Winding Temperature
- Power Consumption
- Vibration

Using engineering judgment the following parameters will be provided, based on specifics of equipment, for all process machines (e.g. pumps):

- Unit Bearing Temperature
- Casing Temperature (Larger Pumps)

Each piece of motor-driven equipment is to have a local 'Automatic/Manual' hand switch to override the computer. Each 'Automatic/Manual' hand switch should be provided with "Automatic Position" contacts, to ensure the signal for Automatic operation is confirmed.

'Motor Running' and 'Motor Fault Status' should be monitored regardless of the position of the 'Automatic/Manual' hand switch.

Each motor starter should have auxiliary contacts, to repeat Fault and motor running conditions.

Some motors have RPM control feature, i.e. Acid injection pumps.

CHAPTER-4

Field Instruments Specification

4. Field Instruments Specification

4.1 General Specification

The Primary Water Supply has standardized on a limited number of field instruments to reduce the ongoing instrument maintenance costs.

- Instruments to be provided should be proven both of high reliability & low maintenances.
- Analog signals from instruments should be communicate through 4-20mA DC, HART, foundation field bus protocol and TCP/IP (Transmission Control Protocol/Internet Protocol). Two wire transmitters are to be used, where possible. Four wire system also possible depending on the application in the system. (free spare recommended)
- Transmitters and transducers are to be installed as near to measuring point as practical, minimizing the need to address confined space Entry. (Subjected to the Site condition & Approval)
- Instruments to be generally accessible (for both reading and cleaning) from grade level. Instruments not readily accessible to have permanent platforms/ladders, as a function of frequency of maintenance schedule/space availability.
- Signal and power cables should be lay separately in a rail and covered properly. This is to avoid interference that cause/s reading instability also for maintenance purposes (Subjected to the Site condition & Approval)
- Check valve to the gauges to ease the maintenance without stopping any lines.
- Calibration certificate should be provided by the supplier/manufacturer to guarantee the efficiency of the instruments.
- The supplier should calibrate the meter at minimum three-points 10%, 50% and 100% of the maximum value for each size of meter and should submit the calibration report for approval to NWC-RCBU prior to dispatch.
- Supplier should confirm the Ingress protection and provide manufacturer certificate against the conformity. Provide certificate No ingress of dust; complete protection against contact (dust tight). A vacuum should be applied. Test duration of up to 8 hours based on air flow. The equipment is suitable for continuous immersion in water under conditions which should be specified by the manufacturer. (If recommended as per application)
- Contractor should have to provide and apply installation condition to achieving the maximum life period and Device function with certificate

- Instrument Life cycle has to be approved. (Suppliers to confirm support for spares, Technical services for Precision Instruments for 10 years after commissioning even after these models become obsolete or discontinued by the suppliers.
- General details of model and connection should mention on the Sensor or Transmitter in (Name plate, Scanner, etc.)
- The measuring device complies with the general safety requirements in accordance with EN 61010-1, the EMC requirements of IEC/EN 61326 and NAMUR Recommendations NE 21 and NE 43

4.2 Flow meters

Supplier have to review the General Instrument Specification Prior checking each individual Instrument Item

4.2.1 General Specification for All type of flow meter

1. Flow meters should be the latest "state-of-art" microprocessor based device with integral sensor, transmitter, processor & indicator suitable for measurement of water flow as per direction, also reverse flow condition should recorded separately and should able to calculate volume and send as separate signal.
2. Base accuracy of the combined system ex. sensor, Transmitter & Indicator should be better than ± 0.5% of the full scale reading and should have a temperature effect not greater than +0.5 % per 50 Deg.C of the full scale. The technical accuracy & acceptance requirements for the Flow meter should be based on the standards BS EN ISO 4064-1 & OIML R49
3. Flow at any value in the range, supplier to submit flow meter sizing print out for given minimum, Normal and Maximum flow data, also to submit typical actual calibration curve for offered model along with the offer.
4. The supplier should have their own facility for wet calibration in Saudi Arabia with master calibration meter accuracy of ± 0.05% or better which should be certified by NPL or TUV approved & National Laboratory of TUV approved or ISA certified International Laboratory. The copy of certification should be enclosed with the offer.
5. The offered instrument should be suitable for operation at atmospheric condition of 100% humidity and 0 to 60 deg. C Ambient temperature. The housing should be cast aluminum IP68 (NEMA 6) class. The meter should give 4 to 20 mA DC current output for SCADA

and should also have two nos. of relay outputs which should be programmable/Scalable for any given flow value., with contact rating of 0.2A, 250 VDC, 50 Watts, resistive. Relays should be integral part of the flow meters and should be built in to the meters only. Relays external to flowmeters are NOT acceptable. Relay output by any other method or mode is NOT acceptable.

6. Flowmeters should have HART protocol functional & Hardware requirements for slave port, device specific commands and all Universal which supported Common Practice commands supported by the HART interface
7. It should be possible to select the range of flow measurement on the flow meters at site as per requirement. Supplier should furnish the detailed procedure of range selection along with the offer. Supplier should also indicate the minimum and maximum selectable range in LPM/MPH and corresponding flow velocity along with the offer.
8. The flow meters should be suitable for a working water pressure of 10 Kg/cm2 (16 Bar) and a test pressure of 15 Kg/cm2 (20 Bar) for 30 minutes duration. Flow meters should pass this Pressure test successfully.
9. Suppliers Supply, delivery, Installation & Commissioning of the instrumentation should be as per the required Pipeline Diameter, Make and Application Area & Medium of Flow. Shall follow the Following Specification for the Supply & Installation.
    - External Power Flowmeter should have Multi line backlit LCD display with facility to show flow rate indication with Eng. Unit (LPM) and flow totalizer. The display should be programmed to show readings in LPM prior to dispatch.
    - The Installation requirements for Potable water & acceptance requirements for the Flow meter should be based on the standards BS EN ISO 4064-5 & OIML R49
    - The meter should be suitable for universal mounting i.e. horizontal or vertical, flow left to right, right to left, top to bottom and bottom to top. Supplier to specify the straight lengths of pipes required on upstream and downstream of flowmeter for reference. The display unit of the meter should be rotatable in steps of 45 deg. C to see from any angle after installation to suit site conditions.
    - Flowmeter should have minimum 16-character LCD display is provided with backlighting that can display alphanumeric characters as per requirement
    - All the menu of the flowmeter is clearly labeled for easy understanding of the menu with different languages (English and Arabic)

- The front cursor type keypad can be used to navigate through the menu system of the flowmeter
- Calibration of the flowmeter is done digitally through front keypad
- Flowmeter configuration should be user friendly.
- Programmability of the flowmeter offers flexibility in the usage of the flowmeter at different velocity and different pipe diameters
- The onsite digital calibration feature ensures high accuracy for a given flow condition
- The required rate conversion is done internally and displayed in a unit that is convenient to process application
- The programming of the meter should be possible through touch control operation without opening the meter cover.
- Suppliers should complete Instrument chamber including Provision for Easy access, laying of Instrument & Power cable, Provision for laying External antenna cable (if required)
- Supplier should complete installation, Termination of Cables, Erection, testing, trial run and commissioning of flow meter in line with actual transmission
- Supplier should follow the technical requirements Like Flow velocity, Ingress protection Class (IP 68), Selection of Electrodes and Shall Provide Calibration certificate
- Supplier should follow the requirement for Signal Output, Modbus TCPIP/DNP3 or other Communication protocol, 4-20mA, Pulse, passive/Active, Remote Display version, Sensor cable length, Power supply & Auxiliary Power Supply, Frequency etc.

- The meter should give 4 to 20 mA current output for SCADA and should also have two nos. of relay outputs which should be programmable/Scalable for any given measured value.
- Safe operation – display provides easily readable process information, Fully industry compliant – IEC/EN/NAMUR

- Maintenance-free – no moving parts, Calibration lab as per ISO 17025 as directed with all lead and lift complete including all the required materials for commissioning.

10. Based on Site condition and Application supplier should provide different Provisions for Power Supply (Direct AC Power/ Battery/ Solar Cell/ Wind Generator etc.) solutions as Follows,
    - Flowmeter should be suitable for operation with 85 to 260 VAC, 45 to 65 Hz, and Single phase AC supply if direct power required and supplier has to arrange the required Power as per contract and agreement.
    - Supplier should confirm the Battery Life Minimum 5 or 10 years as directed with all lead and lift complete where approved to work on Auxiliary Power.
    - Supplier should confirm the Battery life according to the Frequency of Transmission as per requirement, which should be user configurable.
    - Device should able to send information about the Battery life to monitor remotely as per different application
    - Selection of Brand and Type of Battery are subjected to approval, Supplier should have to provide complete information with datasheet and Certificate for the approval as per contract and application.
    - Contractor should supply and install Solar or wind power source from which device Utilizes a DC Voltage in the range 6 to 24 V as per the requirement of Application or site condition as approved solutions.
    - Supplier should confirm with document the Charge/Discharge period for the Solar supply and maximum backup time can get with Internal or External batteries attached with Solar System.
11. Supplier should follow the following Technical Details for the Selection & Supply for the Insertion type flow meters
    - Measurement range- Bidirectional from 0.02 m/s to 5 m/s (0.06 ft/s to 16.40 ft/s), limited only by the stability of the probe in the flow. Fluid conductivity needs to be minimum of 20 µs/cm.
    - Accuracy- Point velocity: in average or smoothed flow: ± 2% if V =10 cm/s and ±2 mm/s (0.33 ft/s and ± 0.006 ft/s) of reading value for V< 10 cm/s (0.33 ft./s), Average velocity and volume: refer to the standard ISO 7145-1982

- Units- Selectable: mm, meters, feet, liters, Mega liters, m3, ft3, Imp Gal, US Gal, MegaImpGal, MegaUSGal, seconds, minutes, hours, days, KiloUSGal, KiloUKGal, KiloFt3, Kilom3
- Sensor- Information Calibration, serial N°, date of factory calibration, settings and user notes.
- Calibration- Factory calibration against traceable standards; internal checking in accordance with OIML R49 Type P (Permanent) requirements.
- Internal logging- Negative Totalizer / Positive Totalizer / Net Totalizer.
- Outputs- RS 232 programmable point velocity, average velocity, instantaneous flow, totalized volume, signal quality; 2 pulse outputs, isolated open collector. Can be 1 channel positive flow and 1 channel negative flow or 1 channel flow and 1 direction. Maximum frequency 50 Hz.
- Connector- IP68/NEMA 6 Watertight 10-way mil-spec connector for 72 hours
- Software- Supplier should provide manufacturer software for communication with Flowmeters
- Temperature Range-Electronics -20°C to +60°C (-4°F to 140° F).
- Insertion element: Non-frozen water up to +60 °C (140°F).
- Max Pressure- 20 bars (290 PSI). Integral BSP quick fit pressure connector.
- Ingress Rating - IP 68/ NEMA6 (immersed in 10 meters of water for up to 72 hours) with connectors secured.
- Construction-All materials in contact with the water are WRAS and ACS approved, Insertion components: Stainless Steel 316. PVC WRAS approved n°1207559 / ACS approved. N°13ACCLY528 / NSF/ANSI61 approved N°C0286058, Nitrile joints WRAS approved N° 1410504 / 1301500.External components: Stainless Steel 316. Bronze C2121- Probe head: Strengthened ABS.
- Certification-Calibrated to reference meters to Standard procedures and traceability.

4.2.2 Open Channel Flow meters

- Contractor should Supply, Install and commission Open Channel Flow Microwave Radar to be installed in proper location of Parshould Flume for the measurement of raw water flow

in open channel as per manufacturers instruction. The design of the Parshould flume is standardized under ASTM D1941, ISO 9826:1992, and JIS B7553-1993.

- The meter should have flanged connections to IS-6392 table 17 or equivalent, else supplier should supply 2 Nos. of matching flanges with each flow meter.
- Supplier should Provide measuring Tube / Sensor with extra thick PTFE (Polytetrafluoroethylene) lining for optimum functioning Water contains silt and sand particles at the Wastewater Application

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Flow meters:

1. Open Channel Flow, radar, contactless and maintenance-free.
2. Application: Raw water Flow Measurement at Parshould Flume
3. Reliable measuring: for changing media, pressure, temperatures, gas phases.
4. Easy wireless setup via free downloadable APP and Bluetooth.
5. Measuring Range: (e.g. 0- 10m liquid), -40 to 60 deg. C (as per the application)
6. Accuracy: Shall mention depending application and sensor used
7. Protection: IP68,
8. Cable Length: Supplier should mention the cable length required for the application and as per sensor used
9. Output: Flow Proportional to 4-20mA or 0-20mA up to 500ohm Resistance which is user programmable and adjustable, MODBUS, Full duplex RS-232 Digital Output; Voltage Free Contacts/Pulse outputs as required
10. Power Supply: Direct Single Phase AC Supply or Auxiliary 24VDC By Solar & battery combined System as directed with all lead and lift complete including all the required materials for commissioning.

4.3 Pressure Transmitters

4.3.1 External Powered Pressure Transmitters

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Pressure Transmitter, Piezoresistive Battery Powered, Inductance/capacitance based on application requirements

1. Application: Pump Delivery Pressure monitoring, DMZ/DMA Pressure Monitoring.
2. Membrane: 316L, welded.
3. Sensor Range: Shall supply as per different application 0-20 Bar, 0-16 Bar, 0-10 Bar overload: 40bar.
4. Accuracy +/-0.3%.
5. Process Connection: Thread ISO 228 G1/2 EN837, 316L .
6. Output: 4-20mA
7. Power Supply: 24V DC/230VAC.
8. Protection: IP68/IP66 as directed with all lead and lift complete including all the required materials for commissioning

4.3.2 Battery Powered Piezoresistive Pressure Transmitters

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Pressure Transmitter,

1. Pressure Transmitter Selection: Piezoresistive Battery Powered based on application requirements
2. Sensor Range: 0-10bar/16- bar/20 bar
3. Accuracy +/-0.3%.; Shall mention depending on the application and sensor used
4. Process Connection: Thread ISO228 G1/2 EN837, 316L
5. Type/Output: Smart two wire/4-20mADC/HART/Profibus/FF BUS
6. Body: Plated carbon steel/316 SS
7. Frequency: Every 30min, 1hr, 1day user selectable
8. Protection: IP68, Battery Life: Minimum 10-15 years as directed with all lead and lift complete including all the required materials for commissioning.

4.4 Level Transmitters

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Level Transmitters

1. Level, radar, contactless and maintenance-free.
2. Application: water Level / Open Channel Flow
3. Reliable measuring: for changing medias, pressure, temperatures, gas phases.
4. Easy wireless setup via free downloadable APP and Bluetooth.
5. Measuring Range: 0- 5m/10m liquid, -40 to 60 deg C as required for application

6. Accuracy: +/- 2mm, Shall mention depending on the application and sensor used
7. Protection: IP68, Cable Length: 10m
8. Output: 4-20mA, MODBUS
9. Power Supply: 24V DC/230VAC as directed with all lead and lift complete including all the required materials for commissioning.

4.5 Water Quality Analyzers

4.5.1 pH Analyzers

Supplier should confirm the following Technical Details for the Selection, Supply and Installation of pH Sensors

1. Memosens, pH comb. Glass Electrode, Memosens functionality
   Application: Standard process pH Measurement
   Diaphragm: PTFE, Signal transmission: Digital. Reference system: Gel. Conductivity: min 50uS/cm Pt100 Temperature sensor integrated. Range: 1-12pH
2. Immersion Pipe, Diameter, Length: PVC, 40mm, 1800mm as directed with all lead and lift complete including all the required materials for commissioning
3. Suppliers should follow the Calibration of sensors, Sampling methods during specified period after installation and should provide proper training for the routine maintenance.

4.5.2 Turbidity Analyzer

Supply, fitting, installation and calibration of memosens Turbidity sensor with flow assembly and transmitter as per approved drawing and instruction of EIC as directed with all lead and lift complete including all the required materials for commissioning

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Turbidity Sensors

1. Turbidity sensor according for low turbidity in clear water applications In accordance to ISO 7027 For all applications in the water plant
2. inline and immersions
3. based on Memosens-technology
4. compatible with Liquiline CM444R
5. Process Connection: Immersion sensor, thread G1, NPT3/4
6. Adaption Cable: Fixed cable, crimp sleeves as directed with all lead and lift complete including all the required materials for commissioning.

7. Suppliers should follow the Calibration of sensors, sampling methods during specified period after installation and should provide proper training for the routine maintenance.

4.5.3 Residual Chlorine Analyzer

Supply, fitting and fixing of Flow fit assembly with RCL2 Memosens sensor with other accessories and plumbing work to measure Residual chlorine at clear water as manufacturer's instruction with all lead and lift complete including all the required materials for commissioning.

Supplier should follow the following Technical Details for the Selection, Supply and Installation of Chlorine Sensors

1. Sample Water Flow Fit Assembly for Clear Water RCL2
2. Residual Chlorine, pH Flow assembly, CCS sensors Sensor slots: 1x disinfection sensor, 2xpH/ORP
3. Body: plexiglass PMMA, Flow indication, Flow control
4. Pressure max: 4bar, Temperature 0-45deg C, non-freezing
5. Application: water, water works, Disinfection, water quality control Chlorine Sensor, Inbuilt Proximity switch for no Flow as directed with all lead and lift complete including all the required materials for commissioning.
6. Suppliers should follow the Calibration of sensors, sampling methods during specified period after installation and should provide proper training for the routine maintenance.
7. Online instruments/analyzers should be installed with sampling lines with booster pump if needed

4.6 Preferred Instrument Applications

The following table identifies the preferred instrument applications for reliable operation.

Application	Preferred Technology	Acceptable Alternatives
Pressure reducing	Electromechanical (Valtek)	
Valve position	Pneumatic positioner (Auma AWG positioner)	
Differential pressure for micro filters	Differential pressure gauge with switch contact (Delta Comb)	Differential pressure Electronics Transmitter
Motor Speed Controller	Electronics speed controllers (Siemens) (Schneider electric)	
Acid dosing control	Rotameter with magnetic link	Electronics Flowmeter
Chlorination System	Automatically controlled by flow and residual chlorine, automatic leak detection, Automatic changeover units for the gas cylinders and back up control units.	
Silt Density Index	Automatic (PLC controlled)	
Online Process & analyzer measurements (pH, Conductivity/TDS, ORP, level_RADAR_ultrasonic, Turbidity, Temperature_PT100, Dissolve Oxygen, Residual Chlorine, differential pressure)	Electronics sensor and transmitter with built in relays for alarm and control	
Pressure controllers and transducers	Passive Pressure regulator and Active/electrical Pressure switch, I/P converters	electromechanical
Pressure switch	Electrically operated with relay contact	mechanical
Control valves for dosing application	Solenoid valves, pneumatic actuators	
Motor/Pump protection	RTD (temperature) for bearings and winding, piezoelectric for vibration, diaphragm type pressure switch with relay, electrical flow switches Built-in protections with soft-starts & VFDs, or separate protection smart-relays for larger pumps	
For Output/Reading Indicators	Electronics/digital Indicators/recorders	
Pressure Measurements	Electronics /diaphragm type Pressure sensor/transmitter	Bourdon Tube, manometer
Level measurement for water reservoirs, water filters	RADAR, Ultrasonic, hydrostatic	Differential, floats
Level measurement for raw sewage wells, sludge tanks, chemical tanks	Ultrasonic, RADAR	Glass/Plastic level gauge

Level switches in water applications, building flood alarms	Limit switch, RADAR_ultrasonic_hydrostatic transmitter built in relay for control	Float (back-up only)
Level switches in sewage applications, chemical tanks	Level switch, RADAR_ultrasonic_hydrostatic transmitter built in relay for control	Float (back-up only) , Glass/Plastic level gauge with magnetic link as a switch
Sludge blanket level	Ultrasonic, RADAR	Series of light transmission rods
Level switches in sewage applications, chemical tanks	Laser Level Transmitter (ABB LLT)	Water and waste water processing plants. Oils and hydrocarbons Liquids in food and beverages. Chemical tanks Liquids in any industry, including metals, mining, power, pulp and paper, and pharmaceuticals
Pressurized pipe flow measurement in potable water, sewage, sludge, chemical	Full Bore Electromagnetic	Clamp on ultrasonic, Insertion type electromagnetic, differential pressure orifice (for water application)
Open channel flow measurement	Parshould flume/Ultrasonic	Transit time
Gas flow measurement for air, digester gas	Thermal Mass Flowmeter	Orifice Plate/Differential Pressure
Potable water turbidity	Light Adsorption	
In-line sludge density	Light Adsorption	
Sludge Density in Aeration tanks, sludge tanks	Light Adsorption	
Aeration tank dissolved oxygen	Membrane type sensors	
Potable water chlorine residual	Amperometric	
Full pipe line flow-meter	Electromagnetic	Transit time
Partially full pipe flow-meter	Transit time	

4.7 Preferred Instrument Vendor List

It is intended that all sources of instrumentation purchase come from the technically acceptable instrument manufacturers. All technically acceptable manufacturers' facilities should be surveyed and approved by Vendor Inspection.

The following table identifies the preferred instrument vendors.

Company	Relevant Equipment	Web Site
Siemens	Chlorination System, motor speed controller	*www.siemens.com*
Wallace & Tiernan	Chlorination System (gas feeder, chlorinator, automatic positioner, process control unit, PCU, vacuum regulator, injector, MS plus leak detector, chemical changeover unit, chlorine residual analyzer, depolox-4x residual chlorine sensor, PID controller, valve fitted with electrical actuator	*www.wallaceandtiernan-usa.com*
Severn Trent	Chlorination System (high & low vacuum switch, chlorine residual analyzer, heater, ejector, automatic change over	*www.stwater.co.uk*
Brook	Rotameter	*www.brook.org.uk*
KDG	Rotameter	www.kdg.com
MABAT	Automatic Silt Density Index Meter	*www.mabat-systems.com*
Endress and Hauser	Sensors and transmitters for pH, Conductivity/TDS, ORP, level _RADAR_ ultrasonic, Turbidity, Temperature_PT100, Dissolve Oxygen, Residual Chlorine, differential pressure, flowmeter, recorders, pressure, power supply	www.endress.com
ABB	Sensors and transmitters for pH, Conductivity/TDS, ORP, level_RADAR_ ultrasonic, Turbidity, Temperature_PT100, Dissolve Oxygen, differential pressure, Full bore & insertion type electromagnetic flowmeter, recorders, indicators, pressure sensor/transmitter, power supply, PID controller, Laser Level Transmitter /LLT100	http://www.abb.com
Norgren	Pressure regulator	
Fisher	I/P converter	www.fisher.com
Parker	Solenoid valve	
ASCO	Solenoid valve	
NORBRO	Pneumatic actuators with ball valve mounted	www.worcestercontrol.co.uk
Metra Mess	Vibration velocity sensor	www.MMF.de
McDonnell & Miller	Flow switch	www.mcdonnelmiller.com

VEGA	Hydrostatic level sensor, level switch, level transmitter, overvoltage arrestor	www.vega.com
Precision Digital	Indicators	www.predig.com
Wika	Bourdon tube Gauges, differential pressure gauge with switch contacts	www.wika.com
Square D	Oil pressure switch	www.squared.com
Sirco Controls LTD.	Water pressure switch	*www.sirco-controls.co.uk*
UNIVAR	Water pressure switch	www.univar.com
Coulton Instrumentation LTD	Pressure switch-Ettore Cella SPA	www.coulton.com
Foxboro Eckardt	Pneumatic positioner	www.foxboro-eckardt.com
Flowserve	Pressure reducing valve	www.flowserve.com
Danfoss	Pressure switch	www.danfoss.com
M System	Signal Converter	*www.a-msystems.com*
Bailey and Mackey LTD	Pressure switch	*www.baileymackey.com*
NIBCO	Motorize valve actuator	*www.nibco.com*
Honeywell	Pressure regulator	http://honeywell.com
Krohne	Flowmeter & transmitter, signal converter	*krohne.com*
Emerson	Online analyzers flowmeter, level meter, chlorine analyzer	*www.emerson.com*
Yokogawa	Online analyzer	*www.yokogawa.com*
Airtac	Pressure regulator with filter, solenoid valves	http://en.airtac.com/
Schneider Electric	Selector Switches, Pushbuttons and Indicating Lights Controls & Timing Relays PLC	
Allen Bradley (Rockwell Automation)	Selector Switches, Pushbuttons and Indicating Lights Controls & Timing Relays PLC; and I/O Cards	http://ab.rockwellautomation.com/
Ashcroft	Pressure Switch	http://www.dresserinstruments.com
Capital Controls	Chlorine Residual Analyzer	http://www.capitalcontrols.com
Control Concepts	Power Line Transient Protection	http://www.control-concepts.com
Cisco	Switches, Hubs, Routers	http://www.cisco.com
Entrelec	Signal Line Transient Protection DC Loop Power Supplies (24 Volt)	http://www.entrelec.com
Fluid Components International	Gas Flow meter	http://wwwfluidcomponents.com
Flygt	Level Float Switches, Flow meter,Pumps	http://www.ittflygt.ca
General Monitors	Gas Monitoring	http://www.generalmonitors.com
Hach	Turbidity Meter; Residual Chlorine; Online analyzer Parshould flume flow meter	http://www.hach.com
Krohne	Magnetic Flow meter	http://www.krohne.com

Kurz	Cost	http://wwwkurz-instruments.com
Nortel Networks	Switches, Hubs, Routers	http://www.nortelnetworks.com
Pepperl+ Fuchs	Safety Barriers	http://www.pepperl-fuchs.com
Phoenix	Signal Line Transient Protection DC Loop Power Supplies (24 Volt);Terminals,Switches-FIbreoptic & Ethernet	http://www.phoenixcontact.ca
Powerware	Motor Protection Relays Ups	http://www.powerware.com
ProMinent	Chlorine Analyzer pH Analyzer	http://www.prominent.ca
Rosemount	Pressure Transmitter Chlorine Residual Analyzers pH Analyzer Temperature Transmitter	http://www.rosemount.com
Royce	Sludge Blanket Level Dissolved Oxygen Analyzer; PH/ORP Transmitter	http://www.royceinst.com http://wwwblanketlevel.com
Milltronics	Ultrasonic Level Transmitter Open Channel Flow Motion Switch	http://www.miltronics.com
Nivus	Transit time flow meter Ultrasonic level meter, Data logger	http://www.nivus.com
Sofrel	Data Loggers, Pressure Sensors, Level Sensor, RTU	http://www.lacroix-sofrel.com/
Halma Water Management	Flow & Data Logger	https://www.hwmglobal.com/
Hydreka	Insertion type Flow meter, Data logger	http://hydreka.com/
Xylem	Insertion type Flow meter, Electromagnetic Flowmeter	https://www.xylem.com/en-sa/brands/flygt
Euromag	Ultrasonic Flowmeter	https://www.euromag.com/en/#miniera-euromag

CHAPTER-5

Typical Field Device I/O

5. Typical Field Device I/O

5.1 Typical Field Device I/O

The following typical device I/O should be specified in the device specifications.

Application	Function	I/O
Typical Motor (FVNR - Full Voltage, Non-reversing)	Mode Start/Stop Command Running Status Ready Status Fault Status	DI DO DI DI DO DI
Diesel Generator	Mode Start Cmd Stop Cmd Running Status Hi Temperature LO Oil LO Fuel Overcrank Overspeed	DI DO DO DI DI DI DI DI DI
VFD	Start/Stop Cmd Running Status Fault Status Mode Speed Setpoint Speed Feedback	DO DI DI DI AO AI
Air Actuated Valve, Spring Return	Open/Close Open Status Close Status	DO DI DI
Air Actuated Valve, maintain Last Position	Open Cmd Close Cmd Open Status Close Status	DO DO DI DI
Motorized Valve (Discrete)	Open Close Opened Closed Fault Mode	DO DO DI DI DI DI
Motorized Valve (Modulating)	Fault Mode Position Setpoint Position Feedback	DI DI AO AI
Smart Instruments	Analog Feedback Fault	AI DI

5.2 Field Indicating Lights

Field status and alarm lights should conform to the following color convention:

ITEM	COLOUR
Stopped, burner on, valve fully-CLOSED, breaker closed	Red
Running, safe, valve fully OPENED, breaker open	Green
Intermediate position for valve	OFF
Overload/Alarm/Warning FAULT	Yellow
Reset	No Color
Mode	Remote , Local

5.3 Control Wiring

Field Wiring Voltage Standards:

- The analog field wiring should be 24 VDC, using 4-20 mA signals. shielded (2 wire system)
- The DI and DO wiring should be 220 VAC . DO signals should be powered from the related field device circuit. The DI should be powered from the PLC panel so that they can be placed on UPS power if needed.

5.4 Analog Signals

- Analog signal wiring is to be twisted pair shielded (TPSH) wire. Individual signal conductors should be stranded copper wire. A "pair" is defined as two insulated conductors covered in a 100% electrostatic shield plus a shield drain wire. When multi-pair cabling is provided, each pair should be individually shielded and an over-all cable shield should be included.
- Each pair is to consist of one white and one black conductor. The convention is that the black conductor should be of a higher potential (voltage) than the white conductor.
- Each pair's shield drain wiring should be terminated to the Isolated DC Ground point in the PLC panel. This should be the only electrical connection to the shield. The shield should have its electrical isolation maintained through junction boxes, etc. by the use of insulating sleeves and dedicated terminal block assignments. The shield should be insulated and un-terminated at the field device.
- All analog I/O points within a PLC or SCADA controller cabinet should be terminated to uniquely numbered terminal blocks within the cabinet or to purpose-built remote

termination assemblies (such as the Phoenix Universal PLC Wiring System). Field device wiring should not be directly connected to I/O modules.

- Successful operation of the 4-20 mA analog signal transmission convention requires there is only one series pathway for the signal: there should not be any parallel current pathways. The desired loop pathway is from the "+" terminal of a 24 (nominally) Vdc power supply, to a transistor load (the field transmitter), to a sense resistor (250 Ohms), and finally to the "-" terminal of the power supply. The convention implemented in the SCADA system is that the low side of the (250 Ohms) resistor should be the only point of the loop connected to the SCADA Isolated DC Ground. Therefore it is critical that: (1) all elements in the loop are connected in a single series loop and (2) all elements in the loop should be isolated from ground. Refer to ISA S-50.1 for further discussion
- Field devices should include electrical isolation as necessary to ensure accurate signal transmission from/to field device to/from the controller. Note that this is a particular requirement for the popular Milltronics Multi Ranger ultrasonic level transmitters. Any analog signal connection to a VFD should be implemented with optical isolation.
- The power supply should be from the 24V power supply in the PLC panel. Connection for each individual field device circuit should be routed through either a fuse or a current limiting series resistor to ensure that a wiring fault of one field device does not impair operation of other devices sharing the same power supply.
- For 120V /220V field instruments, the power supply should be from the terminal blocks in the PLC panel. Connection for each individual field device circuit should be routed through either a fuse or a current limiting series resistor to ensure that a wiring fault of one field device does not impair operation of other devices sharing the same power supply.

5.5 24VDC Discrete Signals

- For all fields DI, the closed circuit should represent the normal state and an open circuit should indicate the process alarm state.
- Low voltage DC Field Device signals (24VDC) are to be installed with stranded copper wire #16 AWG. If cable color coding is black and white the convention should be consistent with analog wiring: the black conductor should be of a higher potential (voltage) than the white conductor.

- Conductor color for DC Discrete signal wiring which remains entirely within a single controller should be orange.
- Device change of state should be actuated by powering and un-powering the + (positive) side of the 24 Vdc circuit. All of the 0 Vdc (-, negative) connections of the circuit should be tied together. Switching elements on the return circuit is not permitted.
- Whenever DC digital signals are transmitted between two controller systems the topology of solid-state output to solid-state input should be avoided. Therefore either the controller output should be a "hard contact" (relay) type output or, if a solid state output is used, it should drive an interposing relay which in turn provides the hard contact for connection to the solid state input. The use of "pull down" load resistors in place of the interposing relay is not acceptable.

5.6 220VAC Discrete Signals

- For all fields DI, the closed circuit should represent the normal state and an open circuit should indicate the process alarm state.
- The 220VAC Discrete I/O field cabling is to be a minimum #14 AWG stranded copper wire.
- AC Discrete Input device field cables should use a minimum of three-conductor cable (with black, red and white conductors); two conductor cables should not be used. AC Discrete Output device field cables may use two conductor cables.
- The conductor colure designation is that green or bare conductors are always at ground.
- White conductors of field cables are for use as neutral or control signal wires. If a white wire is used for a control signal (as in cables with less than 3 conductors) it should be taped red or black for 50mm at its junction points.
- Red conductors of field cables are for use as control signal wires.
- Black conductors of field cables are for use as hot, or control signal wires. If a black wire is used for a neutral connection (as is common in cables with more than 3 conductors) it should be taped white for a length of 50mm at its junction points.
- Whenever AC digital signals are transmitted between two controller systems the topology of solid-state output to solid-state input should be avoided. The DO should drive an interposing relay which in turn provides the hard contact for connection to the solid state input. Use of "pull down" load resistors in place of the interposing relay is not acceptable.

- The connection to a 220VAC supply (typically a circuit breaker) for each individual field device circuit should be routed through a fuse to ensure that a wiring fault of one field device does not impair operation of other devices sharing the same 220VAC supply.
- Field devices, which require a 220VAC supply for operation should use the same 220VAC, **fused** supply for status sensing.

5.7 SCADA Signal Grounding Practice

- Isolated DC Ground
    - The analog DC and digital DC power supply "-" connection (0 Vdc) should be connected to a single star ground point referred to as the "SCADA Isolated DC Ground Point" located within the PLC panel. This is typically implemented using a copper bus bar on insulated stand-offs located near the bottom of the controller cabinet. This bus bar should be identified as the "Isolated DC Ground". This bus should be tied by one and only one ground wire which runs directly from the bus bar to the lowest potential building or system ground available (Typically the building frame or buried grounding grid. Simply tying this ground via the AC System Ground bus bar should be avoided. The grounding cable from the Isolated Ground DC bus bar to this ground point should not serve any other purpose.
    - Field device enclosures should not be connected to the Isolated DC Ground.
    - Wiring conductors connected to the Isolated DC ground should be labeled and colored in accordance with its loop function (i.e., with a "-" suffix as described below) or should be green/yellow in colored and labeled as "DC GND".

5.8 AC System Ground

- The AC System ground is the principle ground for the SCADA system. It originates from the supply transformer neutral.
- This is typically implemented using a copper bus bar on non-insulated stand-offs located near the bottom of the controller cabinet.
- All cabinets, bonding, AC powered field devices, AC digital field devices and AC field wiring should be grounded to the AC system ground.

- Wiring conductors connected to the AC System Ground should be labeled and colored in accordance with its loop function (i.e. with a "G" suffix as described below) or should be green/yellow in color and labeled as "AC GND".

5.9 AC Isolated Ground

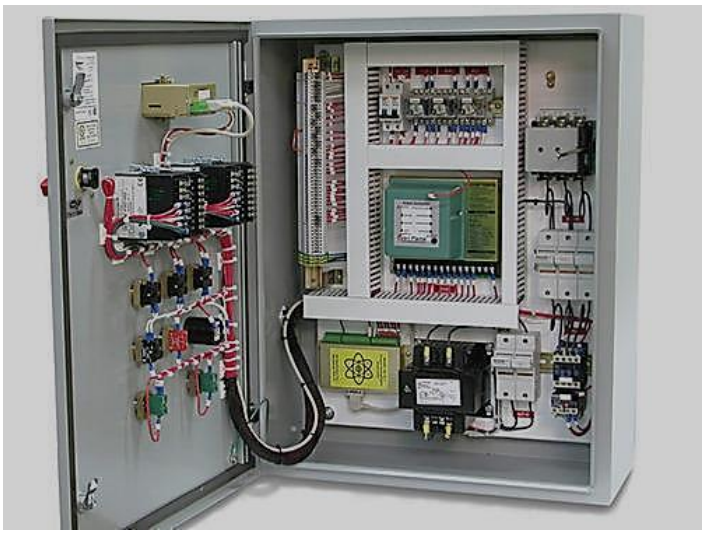
- The AC Isolated Ground is a short dedicated ground that only occurs with UPS and series topology power conditioners (i.e., Tycor) which have a supply side ground connection (which is tied to the AC System Ground) and a separate load side ground connection. The load side ground connection becomes the AC Isolated Ground. This ground should be connected to all loads from the device connection point and should not be connected to a bus bar.
- The AC Isolated Ground should be reserved for connection to data processing equipment (SCADA and PLC CPUs) in close physical proximity. Field device enclosures should not be tied to the AC Isolated Ground. If a field device is powered from a UPS (which requires an AC Isolated Ground) then the device should be bonded through its field wiring cable shielding to the AC Isolated Ground.
- Wiring conductors connected to the AC Isolated Ground should be labeled and colored in accordance with its loop function (i.e. with a "G" suffix as described below) or should be green/yellow in color and labeled as "AC ISO GND".
- Use of an AC Isolated Ground should be avoided unless the UPS or power conditioner manufacturer installation instructions require it.

5.10 Communication System Wiring Practice

- Network communication cables should be specified as required by the application. Whenever such cable is used it should be the of the premium model available and should include such features as individual shielding, stranded conductor construction, plenum rated fire jacketing, premium connector strain relief. Communication cables should be supplied as factory assembled whenever possible (factory made cables). Field assembled cables may be used where required to facilitate long cable run installations, however each and every such cable should be tested for DC insulation, DC conductivity and for representative data transmission using a recommended data test set.
- All elements of data network cabling system including cables, connectors, patch cords, termination methods and testing methods should be completed to a consistent standard. (should be labeled & numbered)
- Site communication wiring layout.

CHAPTER-6

Control Panels



6. Control Panels

6.1 General

Control panels house the control system at each of the basic levels of operator interface. In general, control panels at the PLC level are not used as hardwired operator control stations. With a few exceptions, operator interface is concentrated at the area or plant level and at the local hand stations.

6.2 Panel Fabrication

- Instruments to be installed in an open field should be characterize to sustain the weather condition of the environment and for additional protection it should be enclosed in a ventilated enclosure, viewing window on the enclosure door and easy to access for maintenance purposes.
- The cabling and placement of equipment should be agreed upon with the IT department.
- Cabinets should be placed in locked environmentally controlled IDF (intermediate distribution frame) rooms if existent.
- Newly purchased cabinets should be as per the standards, equipped with internal fans and take into consideration future expansions.
- Cabinets installed outdoors should have an access control system which utilizes a key and a password.
- Panel should carry applicable CSA/UL label and Ontario Hydro approval sticker.
- Use enclosures, which conform to the requirements of the EEMAC/NEMA type specified in the schedule or panel drawing.
- Provide structural reinforcements within enclosures to ensure a plane surface, to limit vibration, and to provide rigidity during shipment, installation, and operation without distortion or damage to the panel or to any instrument.
- Place knockouts for the wiring of freestanding panels either at bottom or sides of the panel. Cover holes for future devices with a plastic plate.
- Bonderize steel enclosures. Prime and finish with 2 coats of factory finished ANSI baked enamel. Paint the panel interior white. The exterior colure will be selected by the Owner.
- Provide steel stiffeners on the back of the panel face as may be required to prevent deflection due to instruments, operation of equipment, or opening/closing of doors. Use

0.64 cm high by 2.54 cm wide by 1.27 cm deep minimum stiffeners and tack welded to the panel.

- Provide internal condensation and freezing protection with thermostat controlled heater on outdoor enclosures.
- Provide a 25mm deep print pocket within enclosures.
- Fabricate panels, install instruments, plumb, and wire in the factory. Test wiring and plumbing prior to shipment. Use numbered terminal blocks for external connections.
- Use panel fabrication techniques that allow for removal and maintenance of all equipment after installation.
- Provide panels with switched full length fluorescent interior lights and mount near the top, where required by size of panel (larger than 24 x 24") or location (outstation) or equivalent area.
- Provide panels with a 15 A, 220VAC service outlet circuit with surge suppressor within the interior. Provide the circuit with 3 wire, duplex receptacles, one for every 1.0 m of width (one minimum per enclosure) and space evenly along the back-of-enclosure area. Provide ground fault interrupter type outlet in outdoor panels.
- Install panel lighting, service outlets and cooling fan on separate 220VAC breaker. Do not mix with internal panel circuits or loads.
- Provide louvers, forced ventilation, or shading, or air conditioners as required to prevent temperature build-up to make sure temperature inside the cabinet not exceed 40 degrees centigrade.
- Provide clean instrument air purging arrangement with filter regulator and shut-off valve, where required (review if required)

6.3 Signals and Interfaces

- Analog signals are 4 to 20 mA DC and conform to the compatibility requirements of ISA Standard 50.1. Provide the signal conversion necessary for compatibility with panel mounted instruments and the interface to the digital controllers.
- Provide interposing relays or opto-isolators, if required, for retransmission of isolated discrete (digital) signals to digital controllers. Relays should be 10 Amp, 220VAC, SPDT or DPDT, pin-base, plug-in style with neon indicator.

- Furnish, mount, and wire control components such as relays, timers, and other equipment to provide the interfacing and interlocking between the motor starters and associated protective circuits, or other type of control circuit function applicable to a particular final control element. Use sealed and plug-in type components.

6.4 Panel Wiring and Terminations

Wiring:

- Use flexible, stranded, copper TEW wiring. Run wires in continuous lengths from terminal to terminal. Do not splice wires.
- For analog signal wiring, use uniformly twisted shielded pairs not smaller than 18 AWG with a minimum of six twists per foot. Separate analog signal wiring at least six inches from power wiring. Provide continuous foil or metalized plastic shields with 100 percent coverage. Include a drain wire in continuous contact with the shield. Multiple cables should have an overall shield and individual shields for each signal cable.
- Use 16 AWG if approved under the local electrical authority or larger for control signal wiring.
- Use power wiring with insulation rated at 600 V. Use 12 AWG or larger for power wiring.
- Segregate signal wiring from control power wiring, group functionally, and arrange neatly to facilitate tracing of circuits.
- Use plastic wiring wraps to bundle wires, outside of wiring ducts. Securely fasten the bundles to the steel structure at intervals not exceeding 12 inches. Each bundle contains 30 conductors maximum. Use Panduit, or equal wiring ducts and size to provide a minimum of 20 percent spare space.
- Do not intermix signals within the same bundle or duct.
- Use twisted unshielded wire for other DC signals and segregate from wire conducting AC signals.
- Use PVC crimped sleeve type wire tag identifications.
- Printed labels for panel parts (relays, push buttons, PLCs … etc.) should be attached to a fixed surface under the part, not on the part itself.

6.5 Terminal Blocks

- Provide DIN style terminal blocks mounted on DIN rails, such as Entrelac or Phoenix. Space terminal block strips no closer than 15 cm center to center.
- Provide a continuous marking strip with the terminals. Provide a separate terminal for terminating each shield wire.
- Reserve one side of each terminal strip for field incoming conductors. Do not make common connections and jumpers required for internal wiring on the field side of the terminal. Terminate no more than two wires at any one terminal.
- Provide a minimum of 25 percent spare terminals, mounted separately.
- Provide analog loops positive side metering circuits plug in type terminals.

6.6 Grounding

- Provide 2 ground buses in each cabinet or panel, one for shield and cabinet grounding and one for signal grounding.
- Provide grounding lugs for connection to the external grounding system.
- Provide # 6 AWG stranded copper grounding conductor for DC signals.

6.7 Wire Color Standard

The purpose of defining field wiring standards for SCADA systems is to assist the Operations and Maintenance staff to easily identify and troubleshoot wiring issues and to ensure a safe and compliant SCADA system installation consistent with good workmanship practices.

- Control Panel Wire Colors:

Wire Usage	Color	
220VAC panel feeders and internal power wiring	Power (1) Power (2) Neutral	-Blue -Red -White
220VAC DO or DI power from outside panel	Power Neutral	-Yellow -Yellow/white stripes
24 VAC DO powered from outside panel	Power (+) Power (-)	-Blue -Blue/white stripes
220VAC DO or DI powered from within the control panel	Power Power (Return)	-Orange -Orange/white stripes
24 VDC AI or AO powered from outside the control panel	Cable Power Strand (+) Power Strand (-)	-Black with 6” of yellow tape at each end -Black -White
24 VDC AI or AO power from within the control panel	Cable Power Strand (+) Power Strand (-)	-Black -Black -White
Ground wires		Green/ Yellow

6.8 Power Distribution

- Provide a main circuit breaker and branch circuit breakers for each individual circuit distributed from the panel. Group the circuit breakers on a single subpanel. Place subpanel so that there is a clear view of and access to the breakers when the door is open. Use branch circuit breakers rated as required.
- Place no more than 16 devices on any single circuit breaker, as required. Avoid common mode power loss; Subject to operational impact review.
- Where multiple units perform parallel operations, do not group all devices on the same branch circuit.
- Do not exceed 12 amperes on a 15A branch circuit.
- Provide DIN-style fuse with LED failure indicator, Entrelac or Phoenix, for each control loop.

6.9 DC Loop Power Supplies

- Enclose each power supply in an EEMAC type 1 enclosure, vertical surface mounting type, with surface barrier screw terminals for load connection. Equip each power supply with a power on/off circuit breaker.
- Meet the following:
    - Input Power: 220VAC + /-10 percent, 60 Hz.
    - Output Voltage: 24 VDC regulated.
    - Output Voltage Adjustment: 5 percent.
    - Line Regulation: 0.05 percent for 10 volt line change.
    - Load Regulation: 0.15 percent no load to full load.
    - Ripple: 3 mV RMS.
    - Operating Temperature: 0 to 50 degrees centigrade

- DIN rail mounted.
- In general, use single or dual loop power supply.
- Mount power supplies such that dissipated heat does not adversely affect other components. Install output fused terminal blocks, mounted alongside terminal blocks.

6.10 Panel Mounted Devices

- Use face-of-panel mounted devices which are semi-flush mounting and which present a uniform appearance.
- For EEMAC type 3R and type 4 panels, mount face-of-panel mounted devices such as indicating meters, controllers, etc. that are not weatherproof on a hinged inner door. Provide an EEMAC/NEMA rated viewing window on the enclosure door.
- Locate face-of-panel mounted device higher than 0.8 m and lower than 2.0 m from the floor.
- Arrange back-of-panel devices in a neat and orderly fashion. Allow 20% continuous space for future additions. Use mounting plant for mounting all components.
- Furnish face-of-panel mounted nameplates to identify systems and equipment. Use engraved gravoply laminate nameplates having white letters on black background. Include device identification number as well as a descriptive name. Centre lettering on each line.

Use minimum 3 mm high characters. Mount nameplates with quantity 2 stainless steel machine screws.

- Use engraved gravoply laminated nameplates with white letters on a black background in the panel interior to identify each device mounted on the panel exterior and interior. Place the tags above, but not on, the device. Do not obstruct visibility by wire bundles or other equipment. Include device identification number as well as a descriptive name to match identification shown on drawings. Mount nameplates with quantity 2 stainless steel machine screws.
- Follow ISA-RP60.6-1984, Recommended Practice for Nameplates, Labels and Tags for Control Centers.
- Use SCADA color convention, unless otherwise noted.

6.11 Selector Switches, Pushbuttons and Indicating Lights

- Provide EEMAC oil-tight selector switches, pushbuttons, mushroom head pushbuttons for emergency stop, and indicating lights (LED). Provide units that will accommodate panel thicknesses from .423 cm to .476 cm. Provide units that occupy approximately 6.5 cm to 10 cm square face-of-panel space.
- Include operator mechanisms and contact blocks on selector switches and pushbuttons. Label contact block terminals for identification purposes and provide at least 1 single pole, double throw contact. Use heavy duty type contact blocks rated 10 A at 220VAC breaking current.
- Where the contact blocks handle analog (4 to 20 mA) and 24 VDC or less contact closure signals, provide contact material of gold or gold flashing over silver and rated 0.5 A at 120VAC 220VAC
- Provide flush head type pushbuttons with momentary operation.
- Provide 2, 3, and 4 position maintained contact selector switches. Provide springs return selector switches as indicated on the drawings.
- Provide LED indicating light units, which allow light removal and replacement through the front of the unit, such as Enteral.
- Provide a pushbutton with suitable diodes to test all indicating LED light units.
- For key-operated selector switch, use standard Allen Bradley DO-18 key or equivalent.

6.12 Enclosures

6.12.1 Free-standing Enclosures— Steel

- Fabricate enclosures from sheet steel.
    - Provide single door EEMAC type 4 and 12 enclosures with 12 gauge sides, top, and back.
    - Provide double door enclosure with a 10 gauge back with 12 gauge top and sides.
    - Provide multi-door enclosures with 10 gauge sides, top, and back.
- Internally, supply the enclosures with a structural steel framework or bracing for equipment support and enclosure bracing. Permit lifting without racking or distortion. Provide removable lifting rings designed to facilitate rigging and lifting of the enclosure during installation. Provide plugs, which fill the lifting ring holes after installation is complete. Where two or more enclosures are shown mounted immediately adjacent to one another, bolt them securely together with their front faces parallel.
- Provide each enclosure with full height, fully gasketed access doors where shown. Provide doors with three- point latches. Provide for padlocking.
- Arrange rear access doors and size such that they extend no further than 60.0 cm beyond the enclosure when opened to the 90-degree position. Provide access doors with full length, continuous, piano type, steel hinges with stainless steel pins. Provide for padlocking.
- Provide enclosures with louvers, forced ventilation, or air conditioners as required to prevent temperature build-up. Except for enclosures mounted with their backs directly adjacent to a wall, place louvres in the rear of the enclosure, top and bottom. For enclosures mounted with their backs directly adjacent to a wall, place louvers on the sides.

6.12.2 Free-standing Enclosures— Fiberglass

Use EEMAC type 4X fiberglass reinforced polyester enclosures. Construct the enclosures so that no metal parts are exposed.

Provide steel reinforced tops, bottoms, and sides. Provide an internal steel framework to support equipment, brace the enclosure, and permit lifting.

Provide removable lifting rings, interior lights, and receptacles as for steel enclosures.

6.12.3 Wall Mounted Enclosures— Steel

In addition to the EEMAC standards, meet the following requirements:

- 14-gauge minimum metal thickness.
- Doors should be rubber-gasketed with continuous hinge.

Where enclosures are mounted outside or in unheated areas, provide them with thermostatically controlled heaters that will maintain the inside temperature above 40 C.

6.12.4 Wall Mounted Enclosures— Fiberglass

In addition to the EEMAC standards, meet the following requirements:

- Hinge doors on the left side and equip with quick release latches. Provide fiberglass reinforced polyester latches and hinges.
- Provide heaters as for wall mounted steel enclosures.

6.12.5 Enclosure Options— If Required

Window Kits:

- Provide window kits suitable for EEMAC type 4 and type 12 enclosures as specified in the schedule or panel drawing.
- Provide windows with 0.6 cm clear acrylic with steel frames. Use stainless steel frames and polycarbonate window for EEMAC type 4X enclosures.
- Provide an oil resistant gasket to ensure a watertight seal around the window and window frame.
- Provide window kits in a variety of sizes ranging from 7.5 cm by 12.5 cm, to 60 cm by 91 cm.

Louvers:

Include washable aluminum air filters with louvers used for ventilation.

Fans:

- Provide forced ventilation fans, where used, with washable, aluminum air filters and finger guards.
- Operate fan motors on 220VAC, 60 Hz power. Include thermal protection. Use motors rated for 20,000 hours of continuous operations without lubrication or service.

- Provide exhaust grilles with filters.

6.12.6 Closed Loop Air Conditioners:

- Provide closed loop cabinet air conditioners as specified in the schedule or panel drawing.
- Meet the following requirements:

a.	Power:	220VAC, 60 Hz.
b.	Mounting:	Vertical on side or back.
c.	Capacity:	1,200 to 10,000 BTU per hour as required by the cabinet equipment.

- Provide special coatings on coils and copper lines to reduce corrosion damage.

CHAPTER-7

Process Solutions' Standards

7. Process Controller Solutions' Standards:

7.1 Vendor List

The following table identifies the standard PLC hardware & software for use in any installation (Showing Accepted and preferred Vender):

PLC Accepted Brand	PLC Preferred Brand
Schneider	https://www.schneider-electric.com/en/work/products/automation-and-control.jsp
Allen Bradley	https://ab.rockwellautomation.com/Programmable-Controllers
Siemens	https://www.industry.usa.siemens.com/automation/us/en/automation-systems/industrial-automation/plc/pages/plc.aspx
Mitsubishi	http://www.mitsubishielectric.com/fa/products/cnt/plc/index.html

7.2 PLC Standards:

7.2.1 Main PLC:

- A Plant should be equipped with minimum of one PLC.
- All Main PLC's should be redundant (Power supply, CPU and Communication Modules) with Hot Stand by PLC
- All Sub-PLC's should be connected to the main PLC through Fiber Optic Network; with Ring Topology.
- All Fiber Switches should be managed to control the Ring Redundancy.
- Main PLC should be connected to the Wells RTU's through the applicable FIU. This is to complete the compatibility and the need of the process like controlling the wells according to the production needs.
- Main PLC should be connected to the Primary Cloud of the Plants Central SCADA network. Accordingly an RTU should be installed for this purpose.
- A UPS should be provided to ensure the continuity of the PLC service for 120 minutes in case of power failure.
- Isolation transformer to protect the Sub-PLC from external power

7.2.2 SUB-PLC:

- To control and monitor the plant different process functions
- Minimum one Sub-PLC should be provided for each process function and for each location.
- Redundant Sub-PLC (Power, CPU and Communication Module) with Hot Stand By is a should for Critical Process Function as per the table below:

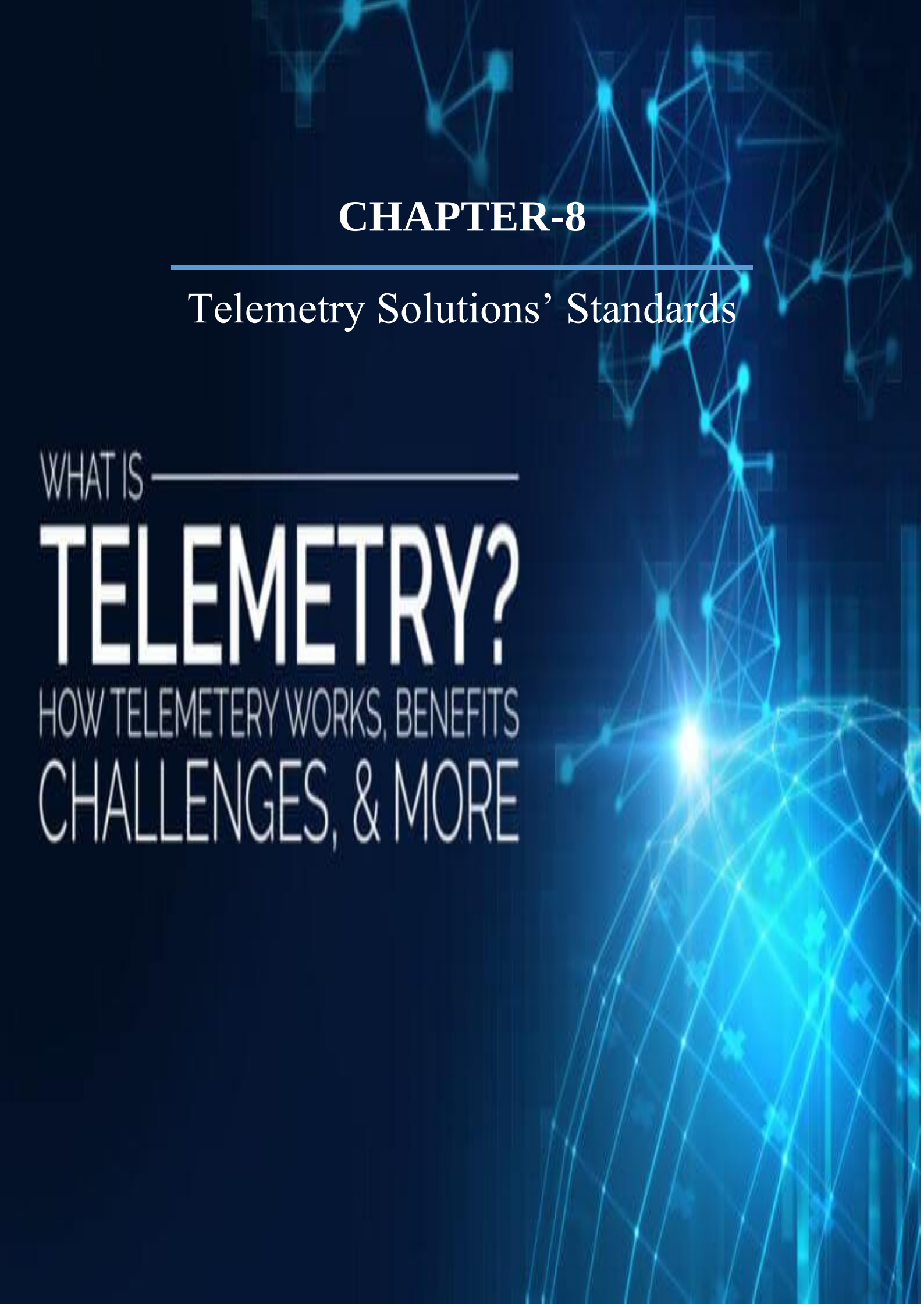
Process Function	Criticality	Redundancy
Cooling Tower		As design
Filters	High	Required
Softener		
Chemicals	High	Required
Reverse Osmoses	High	Required
Chlorination	High	Required
Pump Station		As design
Booster Station	High	Required
Electrical Building		

- All Sub-PLC's should be connected to each other through Fiber Optic Network; with Ring Topology.
- Local HMI should be provided for each Sub-PLC to monitor the process locally. Local HMI should be capable to control the process locally If and only If the Main PLC Logic permits the action.
- To bypass the previous Main PLC vs Sub-PLC control mode, an Authentication by a plant manager is needed using a very strong password.
- HMI Shall be connected to the Ring Network through Ethernet
- Input / Output Modules:
- Built-in Communication Ports: 1 Serial
- Communication Options: Ethernet TCP/IP, ControlNet, DeviceNet, DH+ (Ethernet TCP/IP recommended)

- A UPS should be provided to ensure the continuity of the Sub-PLC service for 60 minutes in case of power failure.
- Isolation transformer to protect the Sub-PLC from external power
- All the digital inputs & outputs should be interfaced by isolation relays
- All analog input & outputs should be protected by surge arrestors.
- Panel should be indoor IP55 with standard size of (H:2000 mm x W:800 mm x D:400 mm) with metal plinth of 100mm.
- In case of more space is needed; multiple Panels with the same standard size should be used.
- Marshaling and System Cabinets should be segregated.
- Connection between Marshaling and System Cabinets should be through pre-fabricated cables.
- Analog and Digital signals should be segregated in the panel on the level of location, cables and ducts.
- Splitter Analog signals sometimes is required.

CHAPTER-8

Telemetry Solutions' Standards



8. Telemetry Solutions' Standards:

8.1 Vendor List

The following table identifies the standard RTU hardware for use in any installation. Showing Accepted and preferred Vender:

RTU Accepted Brand	RTU Preferred Brand
Sofrel Lacroix	http://www.lacroix-sofrel.com/
Schneider	https://www.schneider-electric.com/en/work/solutions/for-business/s4/electric-utilities-remote-terminal-units-and-controllers/
Siemens	https://w3.siemens.com/mcms/industrial-communication/en/industrial-remote-communication/telecontrol/remote-terminal-unit/pages/rtu-3030c.aspx

Parts	Comments	Acceptable Manufacturers/Products
Ethernet Switch	16/24port	Cisco 2900 series
Industrial Ethernet Switch	4/8/16/24port	Cisco Industrial Ethernet 1000 Series Switches. Cisco Industrial Ethernet 2000 Series Switches. Schneider ConneXium TCSESB083F23F0. Schneider ConneXium TCSESB083F2CU0. Siemens SCALANCE 200 series. Siemens SCALANCE 200IRT series. Siemens SCALANCE 300 series.
Ethernet Routers & Firewalls	Cisco routers / UTM	Cisco / FortiGate
Ethernet Media Converter	When required, provide Ethernet media converter from 100baset to duplex multimode optic fibremedia. Converter should have RJ-45 and ST connectors and should include rack-mounting accessories.	Allen Bradley (Rockwell Automation) Ethercom – EFM-12T Blackbox – LHC001A Siemens RUGGEDCOM RMC30 (support DNP3). Siemens RUGGEDCOM RS910 (support DNP3).
Network Connection Modems	When required, provide network interconnection modems for use on dial-up services.	3COM (quickest available speed)
Ethernet Jacks	When required, provide Ethernet jacks to CAT 5E and 6 standards complete with mounting plates. Jacks should be non-keyed RJ-45 style and connections should be by "110 Style" punch down connectors.	Hubbell Thomas & Betts Panduit
Ethernet Patch Panel	When required, provide Ethernet patch panel to CAT6 or more standards in 19" rack mounting configuration and with not less than 16 ports. Rear mounted punch down	Hubbell Thomas & Betts Panduit

	connectors should be “110 Style”. Front mounted connections should be RJ-45 jacks.	
Network Equipment Rack	When required, provide network equipment rack.	Rack should have the following features: 19” rack standard (EIA 310). Minimum rack height of 17.5” (10 units). Minimum rack depth of 10” EEMAC 1 construction
GSM Module	Provides wireless monitoring and control of field devices via cellular network from a central site or control center	Cisco IR910 3G Industrial Router ABB Wireless Gateway ARG600. Siemens SCALANCE M876-3 Multinet PROD0302 / 0303 TAINY HMOD-V3

8.2 RTU Technical Specification

8.2.1 General

- The SCADA controller should be an intelligent, modular unit, capable of both data acquisition and local data processing. It should monitor and control local equipment in a standalone mode as well as being an intelligent node in a distributed system. It should be based on multiprocessor architecture, in which a co-processor is used for handling on-board input/output channels. To facilitate initial installation, maintenance and future expansion, all external input/output modules should connect to the basic controller using a high-speed bus.
- The SCADA controller should be configured with a modern Windows application and programmed with open standard IEC 61131-3 programming languages. Programs should be developed and downloaded either directly to the controller using a standard RS-232 interface cable, USB, Ethernet, or remotely through the communication network media such as phone lines, dedicated lines, mobile IP systems or wireless radios.
- The controller should be supplied with the number and type of input/output modules and communication ports as indicated elsewhere in the specifications. Expansion should be by plugging in additional input/output modules to the I/O bus.

8.2.2 Controller hardware specifications

The controller should include the following:

8.2.2.1 Central Processing Unit (CPU):

- The central processing unit should consist of a high speed 32-bit microprocessor or more with 32-bit internal and external bus.
- The CPU should include a real time clock/calendar, accurate to within one minute per month, with lithium battery backup. The battery will maintain the memory and clock/calendar in case of power off time. The controller should provide an adjustable period for updating time from SCADA protocols in order to achieve accurate clock time.
- The CPU should include an internal clock with at least 10mS resolution and be capable of applying timestamps at this resolution to internal and externally obtained data.
- Diagnostic LEDs should be included for the following:
- Controller Status
- Wide area communication link activity such as transmit, receive
- Local peripheral communication link activity
- I/O point indication for all DI & DO points (as a minimum)
- The controller should include a built-in power supply with wide range input, at least 10VDC - 30VDC. The power supply should be capable of providing 24VDC output to power field transmitters.

8.2.2.2 Mixed process input/output:

- All inputs should be provided with 11 – 24 VDC range and should tolerate 150% over-voltage. Digital inputs should be configurable for reporting of time-stamped events (including unsolicited reporting of state changes), and alarm time dead bands.
- Digital input changes on the controller's local I/O should be time-stamped to at least 200mS accuracy of actual input change, with an internal resolution of 10mS between detectable events. State change and timestamp should be reported through DNP3 SCADA protocols.
- Digital input points should include point quality such that an I/O module or other failure will indicate bad point quality if the point values cannot be updated. User logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in DNP3 protocol.
- The controller should include high speed counters (up to 5 Khz) rated at 12/24 VDC. Counter input points should include point quality such that an I/O module or other failure

will indicate bad point quality if the point values cannot be updated. User logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in DNP3 protocol.

- Digital Output points should include point quality such that I/O module or other failure will indicate bad point quality. User logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in DNP3 SCADA protocol.
- Analog inputs should be 4-20mA on any channel, 14 bit resolution, ± 0.2% accuracy over the operating temperature range, ± 0.1% accuracy at 77 °F (25 °C). Analog Inputs should be single ended. (Modify per application).
- Analog inputs should be configurable for reporting of time-stamped events including unsolicited reporting, event filtering with selection for absolute, percentage and integrated deviations, alarm limits, no-change alarm reporting, exceed rate of rise or fall, and alarm time dead bands. These reporting facilities should be available by parameter configuration and not require any user programming.
- Analog input changes on the controller's local I/O should be time-stamped to at least 200mS resolution, with an internal resolution of 10mS between detectable events. Value and timestamp change should be accessible by a user application and reported through DNP3 protocol.
- Analog Input points should include point quality such that I/O module or other failure will indicate bad point quality. User logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in DNP3 protocol.
- The controller should include one internal temperature measurement channel, scalable in oC or oF to indicate the operating temperature, for remote monitoring via the communication network, or use within the application software. Incase this sensor doesn't exists; the vendor has to supply temperature analog sensor in the panel to send to panel temperature.
- The controller should include a measurement channel for the controller input voltage. It should indicate the value of the input power supply in Volts; include a configurable low

voltage threshold and a low voltage alarm indication capable of configuration as a SCADA protocol event.

- The controller should include monitoring of the RAM battery which can be monitored and alarmed remotely via the communication network.
- Analog outputs should support 12 bit resolution, 0-20mA and 4-20mA selection on any channel, +/- 0.25% accuracy over the operating temperature range, ± 0.15% accuracy at 77° F (25 °C).
- Analog Output points should include point quality such that I/O module failure or other failure will indicate bad point quality. User logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in DNP3 protocol.
- The state of digital and analog outputs should be configurable to hold their last output value or go to the OFF condition when the application program is stopped (Recommended as per application).
- Terminal blocks should be removable and can accommodate solid or standard wires. This allows module replacement without disturbing the field wring.
- The controller I/O should be capable of expansion through local or Remote IO cards. Digital input and digital output points should include visual indication of point status (on & off).

8.2.2.3 Communication

- The controller should possess a minimum of 4 built-in communication ports with the following characteristics:
- Ethernet port 10BaseT / 100BaseT
- GSM Module
- RS-232, software controlled to 115200 baud
- At least one of these ports should be software selectable for RS-232, and RS-485 2-wire operation
- Serial ports speeds should be configurable
- The controller should support asynchronous operating mode, half and full duplex transmission including use of RS232 signals for controlling external communication

devices. All RS232 serial ports should include as a minimum: one output control line (e.g. RTS: Request To Send) and one input control line (e.g. CTS: Clear To Send)

- The controller should support software collision avoidance on all its communication channels. As a minimum this should include collision avoidance on ports configured for RS-485 2-wire operation and collision avoidance on RS-232 ports provided with DCD (Data Carrier Detect) indication from external communication equipment.

8.2.2.4 Communication Protocols

- Open Standard Protocols
- The controller should support the following industry standard protocols:
- DNP3 Level 3 or higher conformant Slave* serial and DNP3 over IP
- DNP3 Level 3 or higher conformant Master* serial and DNP3 over IP
- DNP3 Slave is required to have the ability to send DNP3 Master Read and Control requests to a peer Slave controller
- Modbus RTU Master
- Modbus RTU Slave
- Open Modbus/TCP Client +
- Open Modbus/TCP Server +
- + The Open Modbus/TCP class conformance should be stated for these protocols.
- Interoperability profiles should be provided for these protocols and the device should be certified to at least the DNP3-2009 Level 2 Slave conformance test procedures.
- DNP3 interoperability profiles should be provided in DNP3-2010 standard XML format.
- TCP/IP communications should be supported over Ethernet, asynchronous serial PPP, GPRS, 1xRTT and 3G cellular IP networks.
- Protocol Capabilities
- The controller should provide the following capabilities:
- Allow up to 65500 stations to be addressed in one system.
- Ability to transfer complete configurations and IEC61131-3 application programs and data over the communication network to the controller using DNP3 protocol. The controller should support these facilities via RS232, RS485, TCP/IP PPP serial links, TCP/IP Ethernet, PSTN, radio, cellular IP, etc.
- Support high data integrity techniques such as Cyclic Redundancy Check CRC16.

- Support for multiple master's capability for all Slave protocols. I.e. fully support simultaneous connection from at least two master systems of the same protocol, simultaneously. Time-stamped event data should be independently provided to all masters. The controller should also support simultaneous connection from Masters using multiple open standard protocols from the above list.
- Support high integrity cryptographic techniques such as AES-128 and SHA-256 for security features.
- Proprietary protocols should not be used for remote communication with the device.
- Flexible Communications

8.2.2.5 Routing

The controller should be able to intelligently route DNP3 messages across all its communication ports and interfaces. This should include the ability to filter messages based on source port, source and destination addressing, and include connection information for the destination device such as communications port, PSTN telephone number, IP address, UDP port number, etc.

8.2.2.6 Store and Forward

- The controller should be able to receive information from other sites and retransmit the message to another site, using the same communication port. This should be integrated with the controller's routing configurations.
- The controller should allow flexible communications on all communication ports. All ports should be able to act as Master, Slave or Store-and Forward. DNP3 serial ports should be capable of Master and Slave communications, including Peer controller communications, simultaneously. TCP/IP ports (Ethernet and Serial) should be capable of multiple protocols including master and slave operation, simultaneously.
- All communications parameters should be set by configuration and not require logic or user programs. Communication parameters should be adjustable by user programs but user logic should not be required to initially setup communication.
- The controller should be able to function as an interconnection point between different communication systems such as radio, leased lines, and radios with different frequencies.
- The controller should be able to perform report-by-exception (event driven communications) and unsolicited messaging without requiring the use of a user

application program. Time-stamped data should be provided using native event data objects supported for the open standard protocol

- The controller should provide integrated communications capability for DNP3 peer to peer communications between controllers across the wide area communication link. This facility should allow data to be transferred between devices for purposes such as control coordination between IEC61131-3 applications. Each controller participating in peer communications should be capable of requesting data, or sending data to other peer controllers.
- Communications between the controller and a SCADA host system (master station) should support redundancy as follows:
- Specifically, the controller should support a master changing to an alternate communication interface. This should be supported for DNP3 communications at a minimum and support both serial-serial port and Ethernet-serial port redundancy.
- In addition, the controller should detect and change its operation dynamically, as required, if a master station changes its IP address (e.g. master station changes to a different server with a different IP address). This should be supported for DNP3 communication and be able to occur automatically without user configuration changes or other user intervention.
- The controller should support other protocols, in particular Modbus RTU master, Modbus RTU slave on any of the serial communication ports. Open Modbus/TCP should also be supported on Ethernet, PPP, and cellular IP wide area communication links.
- The controller should be configurable with a unique station number for each communication protocol.
- Configuration capabilities, as described elsewhere in this specification, should be provided via local or remote communications.

8.3 Data concentrator capability

- When acting as a master for its open protocols, the controller should be able to instigate communications with remote devices and concentrate data from the multiple remote devices in to the controller database. This should include processing, integration and storage of current value data, point quality flags and historic data by means of time-stamped events. I.e. sequence of events with timestamps and point quality received from a remote device should be preserved for each individual event and incorporated in to the

controller database for later extraction, including via a different protocol. Further the controller should provide for the mapping of controls to multiple remote devices including transparent mapping of controls from a slave protocol to a master protocol without requiring user programming.

- Data concentration should include as a minimum:
- DNP3 serial protocol as a master
- DNP3 over IP (TCP and UDP) as a master
- Ability to put remote device communications in service and out of service on an individual device basis
- Ability to enable and disable setting remote device time (on a per device basis)
- A variety of polling algorithms for requesting event and static data
- Accept Unsolicited message reports from remote devices
- Full support for integrating point quality and event timestamps from remote device in to the controller's database without loss of information
- Independent polling strategy to minimize delays and recover from loss of communication with a remote device
- Ability to select data concentrator to stop collecting data when event buffers are full
- Communication status for each remote device available in the controller's point database
- Communication statistics for polling and unsolicited messages available in the controller's point database
- Provision for user program or protocol commands to the controller to force an event poll, integrity poll, or remote device restart.

8.4 Time synchronization

- When operating as a slave the controller should be capable of updating its time from the following time sources:
- DNP3 protocol serial time sync method
- DNP3 protocol serial time sync method over IP communications (TCP and UDP)
- DNP3 LAN Ethernet method
- NTP over IP communications
- When operating as a master the controller should be capable of providing time synchronization to remote devices via the following protocols:

- DNP3 serial time sync
- DNP3 serial time sync over IP (TCP and UDP)
- NTP
- Modbus register writes to remote devices
- The SCADA system clock should be synchronized with the network clock and all devices on the network, to ensure synchronous communications in the transmission and reception of data and control characters.

8.5 Mechanical Design

- The controller should be DIN rail mount. Front access to all controls, indicators, communication ports and power supply connection should be provided. RS-232 and Ethernet communication ports should use standard RJ style connectors to allow easy access using standard cables.
- All boards should be coated with conformal coating, for protection against humidity and corrosion.
- All system components should be constructed of corrosion resistant zinc plated steel with removable metal covers.

8.6 Environment

- The controller should operate over an ambient temperature range of -40°C to 70°C (-40°F to 158°F) with a relative humidity 5% to 95%, non-condensing.
- The controller should operate from nominal power supplies 12-24 VDC, but should tolerate a wider range than this. 115/240 VAC operation should be provided through the use of an optional power supply.

8.7 Certifications and Standards:

- The controller should be certified with CE Mark
- All inputs and outputs (except the serial communication ports) should survive ANSI/IEEE C37.90 surge withstand capability (SWC) tests without damage.
- The controller should be certified for electrical safety or applicable low voltage directive.
- Controller serial ports should be static protected to +/- 15kV as conforming to IEC 801-2 and 2.5kV surge withstand capability as per ANSI/IEEE C37.90.1-1989.

- The controller should be certified to meet or exceed the following standards:
- RF emission compatibility: FCC title 13 part 15, Subpart B, Class A
    - CISPR22 Class A
    - Electrical safety classification: c(CSA)us, CAN/CSA-C22.2 No. 61010-1
    - Hazardous area classification: CSA Class 1, Division 2, Group A,B,C,D
    - Discharge Immunity: EN61000-4-2
    - Radiated immunity: EN61000-4-3
    - Fast transient immunity: EN61000-4-4
    - Surge immunity: EN61000-4-5

8.8 Operating System:

8.8.1 Multitasking

- The software should be based on a multi-tasking executive system optimized for real-time environment. This should include:
- Controller Hardware watchdog management
- Individual software task watchdog management

8.8.2 File System

The operating system should include a file system for controller facilities such as configuration, application loading, firmware patching, data logging.

- File transfer to and from the file system should be provided by:
    - SCADA protocol (DNP3)
    - FTP via Ethernet, PPP or GPRS/1xRTT connections
    - Through local connection from configuration and maintenance software.

8.8.3 Firmware Upgrades

The operating system firmware should be capable of being upgraded locally and remotely, utilizing compression techniques to minimize the communications transaction size for loading of firmware patches or a new firmware image. The firmware upgrade should not commence until complete reception of the firmware image. Controller operation should not be interrupted during the communications transfer of the firmware image.

8.8.4 TCP/IP Communications

The operating system should include TCP/IP services that encompass, but are not limited, to the following:

- TCP socket interface for open protocols (Open Modbus/TCP)
- Both TCP and UDP socket interfaces for DNP3 open protocol
- TCP socket interface for IEC61131-3 programming interface
- ICMP (ping) management as a client and server
- Telnet to controller diagnostics stream
- FTP file transfer to controller file system
- NTP network time synchronization protocol
- BOOTP IP address serving for Ethernet I/O modules
- IP network table supporting Gateway, Host, Sub-network entries

8.8.5 Diagnostics

Detailed diagnostics should be available from the controller including the following features:

- Command line interface for interacting with the controller's file system and diagnostics.
- Command line via serial port connection using a generic terminal application. (The serial port should also be selectable for purposes other than dedicated command line)
- Command line from configuration application via local cable
- Command line via telnet
- Command line via DNP3 Protocol Virtual Terminal
- Protocol diagnostics - summary and detailed diagnostics filtered by protocol layer, communication port, protocol address for each of the protocols supported by the controller
- Operational statistics including communication port statistics, controller memory usage statistics, application execution statistics
- Protocol diagnostics and operational message should be able to be logged to an ASCII terminal via serial port, via Telnet, or recorded to a file on the controller's file system for later retrieval

8.8.6 Terminal Serving

Controller serial ports should have the ability to act as TCP socket end-points so that controller serial ports can be configured to operate as Terminal Server ports. This functionality should be available simultaneously with all other controller functions and not require additional hardware.

8.8.7 User Programming Software

The controller should support the following IEC 61131-3 programming languages:

- Sequential Function Chart (SFC)
- Functional Block Diagram (FBD)
- Ladder Diagram (LD)
- Structured Text (ST)
- Instruction List (IL)
- And may include simplified Flow Chart or Quick Ladder languages.
- The controller configuration and programming software should be accessible from a single user interface. The software should allow the user to develop and then download the application and system configuration locally via USB, serial port or Ethernet interface, and over the communication network via TCP/IP, DNP3 and IEC60870-5 protocols.

8.8.7.1 Features for programming language:

- PID feedback control
- Controller data logging functions
- Timers, counters, mathematical functions, memory functions
- Standard Ladder Logic functions such as coils and contacts
- Boolean logic functions
- Bit transfer functions
- Block transfer functions
- Scaling function
- Totaling function
- Flow function
- File manipulation functions
- Alarm grouping functions
- Database manipulation functions
- Communication manipulation functions

- On-line monitoring of user application data including function block and ladder logic application code should be included to facilitate debugging of programs.
- On-line remote monitoring and modification of application code should be supported via DNP3 protocol, and over all communication media supported for DNP3. The software should allow the user to debug applications via TCP/IP and DNP3 communication networks. DNP3 support should include the ability to download and debug over radio, mobile IP, leased and dial-up communication circuits.
- The programming software should support on-line monitoring and forcing of any variable in the application database. Forcing should write a value to the register and prevent modification of the variable content by the application software. A global command to remove all forcing should be included. There should be a physical indication LED on the controller when any application variable values are forced.
- In addition to forcing, the software should be capable of writing a value to any object in the controller database but continue to allow communication protocols or application software to modify the contents of the object.
- The software communication settings should allow a configurable number of retries in addition to message time-out of up to 99 seconds.
- The IEC61131-3 interfaces should provide coupling to the following controller facilities:
- Database functions: read/write attributes of the controller objects
- System command functions
- Protocol functions including routing manipulation
- DNP3 Peer Communications
- Pulse trains with 200mS accuracy

8.8.7.2 Event Capability

The controller should natively support event facilities without the need for user programming

- Open protocol event capabilities for DNP3 should be fully integrated with the controller's event facilities. The number of events stored by the controller should be configurable, with at least 20,000 events.
- The event facilities should be fully integrated with controller support for multiple master connections. I.e. report events and individually track event deletion when confirmed from individual master stations.

- The controller should provide the following capabilities:
- Generate events from physical or derived data objects
- Accept, process and chronologically sort events from external devices
- Merge external events using the original timestamp information provided by an external device
- Where a timestamp is not supplied externally, the controller should add a timestamp to all event data
- Utilize the original point quality supplied from external devices
- Where point quality is not supplied externally, the controller should natively add point quality to all event data
- Accept and merge events from multiple open protocols
- Report consolidated event data through multiple open protocols
- Prioritize reporting of event data
- Report Binary, Counter, Integer analog and Floating point analog events as a minimum
- Configuration should be provided to allow events to be generated locally by the controller for any controller data. This is required for both internally and externally derived data. Configuration should provide for events to be generated through:
- Changed state
- Significant changed value (deviation) expressed in floating point engineering units or percentage of full scale
- Significant changed integrated value expressed in floating point unit-seconds
- Over-range and under-range detection
- Exceeded analog alarm threshold – as a minimum 4 separate “low” alarm limits and 4 separate “high” alarm limits are required per analog object, in addition to over-range and under-range limits
- Report events for analog points on rate of rise exceeded, rate of fall exceeded and no change after a period of time. This functionality should be provided natively without the need for user programming.
- Event configuration for each data object should include an event priority
- Individual event configurations (e.g. each alarm limit) should provide a selection for enabling an unsolicited communication transaction when the event is generated

- To facilitate event integration from third party protocols and other user defined data sources, a programming interface should be provided to enable time-stamped events to be inserted in the controller's event lists by a user application.

8.8.7.3 Data Logging functionality:

The controller is required to have the following data logging functionality in addition to its event capabilities. The controller should support both event and data log operation simultaneously, including both event generation and logging on the same controller data objects.

- The software and hardware should provide time stamped data logging supporting, as a minimum, 16 separate logging trends.
- Logging should be selectable on digital input, digital output, analog input and analog output data objects.
- Analog logging should be by 32-bit floating point engineering values.
- Analog logging should also include data compression through a deviation configuration for each log trend, i.e. prevent storage of a log sample at the prescribed time if the value has not sufficiently changed.
- Logging should be configurable to include current value and summary statistics at a defined interval, including average, maximum and minimum logging trends.
- Logging frequency should be selectable by the user for each logging trend and vary from 1 second to 1 year.
- The controller should support at least 1MB storage for logged data.
- Configuration of the data log function should be made through the controller configuration without need for specific IEC61131-3 user programming.
- Logs should be enabled or triggered by timers or process events. As a minimum, each data log state should be enabled by a digital point state without requiring user programming. In addition, IEC61131-3 user programming can also enable or trigger individual data logs.
- Variable rate logging should be supported for "incident trending" whereby a process event can force faster trending for the duration of an "incident".
- It is recommended that all data should be able to be retrieved and made available as a .csv file for use in Excel, Access, or HMI software. Data uploaded to a PC should be

supported using direct serial connection, leased telephone lines, radio, dial-up modem, external memory media and via the SCADA communication link.

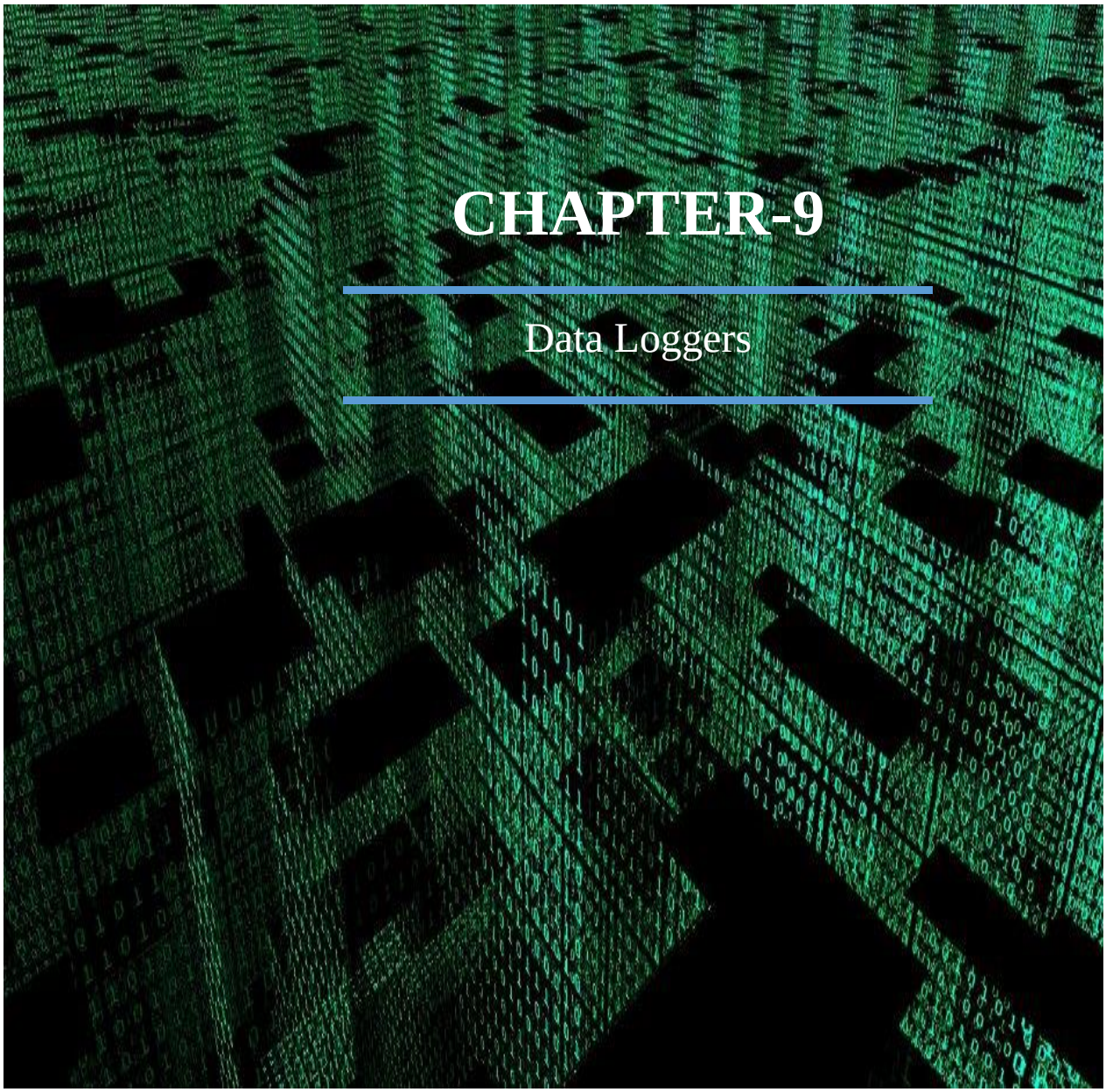
8.8.7.4 Security:

- The controller should provide communications security using recognized SCADA security open standards.
- Controller applications such as Telnet and FTP should be disabled by default. Enabling of these facilities for remote access should be through secured mechanisms only.
- Communication link security should be provided for the DNP3 open protocol as a minimum, supporting operation on serial and network links. This should include DNP3 Secure Authentication v2 with an option for data encryption. Security standards should be aligned to FIPS-120 standards and include AES-128 encryption and HMAC SHA-256 hash algorithms.
- A secure administration application should be provided for the Security Administrator to issue and track security keys, users and configuration computer nodes.
- The administrator application and the controller should provide a mechanism for securely loading encryption and hash keys without exposing the raw key values to the end user.
- The administrator application should provide the capability of specifying security configuration for groups of controllers, users (via username/password) and individual configuration computers.
- Controllers that are required to communicate with each other should be capable of being managed as a security group.
- Once security is enabled on a controller, communication link security should not be disabled unless a controller's configuration is completely erased.
- All communication ports on the controller should be capable of being secured. A single "local access" port free from encryption is permitted for use by the configuration application. Bridging of unprotected communication from this port to the secure communication ports is not permitted.
- All communication ports should be capable of being disabled through user programming on the controller to provide custom communication security solutions for peripheral devices.

- Access to controllers from configuration computers should be capable of being secured at the computer node level through unique keys.
- Access to controllers from configuration computers should also be capable of being secured through username / password access, validated by security configurations in the controllers. It is not acceptable for username/password information to be stored on configuration computers.

8.8.7.5 Warranty:

The manufacturer should warrant the hardware specified above against all defects in material and workmanship for a period of **three years.**



CHAPTER-9

Data Loggers

9. Data Loggers Technical Specification

9.1 General

- The Controller should be an intelligent, modular unit, capable of both data acquisition and local data processing. It should monitor and control local equipment in a standalone mode as well as being an intelligent node in a distributed system. It should be based on multiprocessor architecture, in which a co-processor is used for handling on-board input/output channels
- The Controller should be configured with a modern Windows application and programmed with open standard IEC 61131-3 programming languages. Programs should be developed and downloaded either directly to the controller using a standard RS-232 interface cable, Bluetooth, USB, Ethernet, or remotely through the communication network media such as phone lines, dedicated lines, mobile IP systems or wireless radios.
- The Controller should be supplied with the number and type of input/output modules monitoring combination of Digital and Analog signal and communication ports as indicated elsewhere in the specifications.
- The Controller should be supplied with Water tight MIL Spec connector which can comply IP68 or NEMA 6P Submersible requirement, it should be robust construction with sophisticated electronics and Long battery life have been proven deliver consistent and reliable data in some of the harshest environment.
- The controller should satisfy the operating temperature which is -20 to +70deg Celsius (-5 to +160 deg F)
- The Controller should be configured with user-friendly software for which firmware updates should be installed quickly and efficiently, Also upgrades should be possible through remotely other than direct connection with device.
- The controller should have the facility for select and configure different features as per Application specification.

9.1.1 Processor Unit (CPU):

- The CPU should include a real time clock/calendar, accurate to within one minute per month, with lithium battery backup. The battery will maintain the memory and clock/calendar in case of power off time. The controller should provide an adjustable period for updating time from SCADA protocols in order to achieve accurate clock time.

- The CPU should include an internal clock with at least 10mS resolution and be capable of applying timestamps at this resolution to internal and externally obtained data.
- Controller data logging functions
- Scaling function
- Totaling function
- Flow function
- Alarm grouping functions
- Communication Configuration functions

9.1.2 Configuration Settings:

- Controller Read/ Write configuration should be via Specific Software application which is licensed Permanently and Firmware updates should be available as per agreement
- Configuration Read/ Write operation should be done via universal medium such as Bluetooth, SMS, NFC, RS232, and RS485 or via remote server settings Etc.
- Channel configuration should be as standard for Digital and Analog Signals in the different formats like Pulse, 4-20mA, Standard meter etc. depending on the applications.
- Archive or Logging configuration should be available for different periods of time as per the requirements, also have the facility to extract or Update to the SCADA server as required.
- Threshold/ Alarm settings should be available for different period and the facility to immediate transmit data to the server as per the threshold criteria if required.

9.1.3 Process input/output:

- All inputs should be inputs should be configurable for reporting of time-stamped events (including unsolicited reporting of state changes), and alarm time dead bands.
- Digital input changes on the controller's local I/O should be time-stamped to at least 200mS accuracy of actual input change, with an internal resolution of 10mS between detectable events. State change and timestamp should be reported through TCP/IP, DNP3 or other SCADA protocols as required.
- All Digital and Analog input points should include point quality such that an I/O Channel or other failure will indicate bad point quality if the point values cannot be updated. User

logic should also be able to derive bad point quality on a per-point basis. Point quality should be indicated in the point database and through status flags on individual points in TCP/IP, DNP3, MODBUS, or other SCADA protocols as required.

- Analog inputs should be 4-20mA on any channel, 14 bit resolution, ± 0.2% accuracy over the operating temperature range, ± 0.1% accuracy at 77 °F (25 °C). Analog Inputs should be single ended. (Modify per application).
- Analog inputs should be configurable for reporting of time-stamped events including unsolicited reporting, event filtering with selection for absolute, percentage and integrated deviations, alarm limits, no-change alarm reporting, exceed rate of rise or fall, and alarm time dead bands. These reporting facilities should be available by parameter configuration and not require any user programming.
- The controller should include one internal temperature measurement channel, scalable in Deg C or Deg F to indicate the operating temperature, for remote monitoring via the communication network, or use within the application software.
- Spare channels should be available for reconfiguration and rewiring in case of failure of one channel

9.1.4 Diagnostics:

- Controller Diagnostic LEDs should be included Controller status, SIM Status and Network Status if required as per site conditions.
- Controller should be capable of communicating and sending latest updates with SCADA server
- Controller should be capable of checking the Signal Reception Level by different Network providers
- Controller should provide information of Battery level which is equivalent to the remaining days as per the current battery Voltage which can utilize for the power management
- Controller should capable of archiving data and extract all data as required like a for a period of time or All Logged data

9.1.5 Data Acquisition & Archiving:

- Controller should have minimum storage capacity that able to store 30,000 Value records.

- Controller should have the facility for periodical archiving of meter indices, average calculation and Analog measurements if required.
- Controller should have the facility to send reports daily based on the archived data and average calculation minimum once in a Day as required.
- Controller should log all data for the Particular period of time configured and should able to send all data together during the interval to the SCADA server.
- Controller should have the facility to Verify and update the Data Transmission completeness as per the recording.

9.1.6 Communication with SCADA Central Station

- Controller should be able to communicate with SCADA server as per the settings during particular interval
- Intermediate channel/Protocol for communication should be verified and compatible with the existing SCADA system and Approval should be based on the Pilot Test and configuration (Not recommended; Only if no have facility to connect directly with SCADA)
- Controller should be communicate with the Central SCADA system via GPRS Network by Secure and Standard recommended way as per client Network Policy.
- Controller should able to communicate with hand held devices or Mobile if required for threshold or Warning Messages
- Controller could be with an a built in antenna or outdoor external antenna depend of location (possibility installation & signal strong less)
- The controller should support asynchronous operating mode, half and full duplex transmission including use of RS232 signals for controlling external communication devices. All RS232 serial ports should include as a minimum: one output control line (e.g. RTS: Request To Send) and one input control line (e.g. CTS: Clear To Send)
- The controller should support software collision avoidance on all its communication channels. As a minimum this should include collision avoidance on ports configured for RS-485 2-wire operation and collision avoidance on RS-232 ports provided with DCD (Data Carrier Detect) indication from external communication equipment.

9.1.7 Communication Protocols

Open Standard Protocols, The controller should be supported one or more of the following industry standard protocols:

- DNP3 Level 3 or higher conformant Slave* serial and DNP3 over IP
- DNP3 Level 3 or higher conformant Master* serial and DNP3 over IP
- DNP3 Slave is required to have the ability to send DNP3 Master Read and Control requests to a peer Slave controller
- Modbus RTU Master
- Modbus RTU Slave
- Open Modbus/TCP Client +
- Open Modbus/TCP Server +
- WITS (Water Industry Telemetry Standard)/DNP3
- TCP/IP communications should be supported over Ethernet, asynchronous serial PPP, GPRS, 1xRTT and 3G cellular IP networks.
- Ability to transfer complete configurations and IEC61131-3 application programs and data over the communication network to the controller using approved Controller protocol. The controller should support these facilities via RS232, RS485, TCP/IP PPP serial links, TCP/IP Ethernet, Radio, etc.
- Support for multiple master's capability for all Slave protocols. I.e. fully support simultaneous connection from at least two master systems of the same protocol, simultaneously. Time-stamped event data should be independently provided to all masters. The controller should also support simultaneous connection from Masters using multiple open standard protocols from the above list.
- Support high integrity cryptographic techniques such as AES-128 and SHA-256 for security features.

9.1.8 Routing

The controller should be able to intelligently route DNP3, TCP/IP or other approved Protocol messages across all its communication ports and interfaces. This should include the ability to filter messages based on source port, source and destination addressing, and include connection information for the destination device such as communications port, IP address, UDP port number, etc.

9.2 Mechanical Design

- The controller should be suitable for mounting on DIN rail mount or should be come with proper bracket for Wall mounting purpose; Front access to all controls, indicators, communication ports and power supply connection should be provided. Communication Connector cable and connectors should available for easy access
- All Internal & Extension boards should be coated with conformal coating, for protection against humidity and corrosion.
- All system components should be constructed of corrosion resistant zinc plated steel with removable metal covers or High Grade Plastics with robust and durable design which has succeeded IP 68 requirements if application required.

9.2.1.1 Event Capability

The controller should natively support event facilities without the need for user programming

- The event facilities should be fully integrated with controller support for multiple master connections. I.e. report events and individually track event deletion when confirmed from individual master stations.
- The controller should provide the following capabilities:
    - Generate events from physical or derived data objects
    - Merge external events using the original timestamp information provided by an external device
    - Where a timestamp is not supplied externally, the controller should add a timestamp to all event data
    - Utilize the original point quality supplied from external devices
    - Where point quality is not supplied externally, the controller should natively add point quality to all event data
    - Accept and merge events from multiple open protocols
    - Report consolidated event data through multiple open protocols
    - Prioritize reporting of event data
- Configuration should be provided to allow events to be generated locally by the controller for any connected Signal data.. Configuration should provide for events to be generated through:
    - Changed state

- Significant changed value (deviation) expressed in floating point engineering units or percentage of full scale
- Over-range and under-range detection
- Exceeded analog alarm threshold – as a minimum 2 separate “low” alarm limits and 2 separate “high” alarm limits are required per analog object, in addition to over-range and under-range limits
- Report events for analog points on rate of rise exceeded, rate of fall exceeded and no change after a period of time. This functionality should be provided natively without the need for user programming.
- Individual event configurations (e.g. each alarm limit) should provide a selection for enabling an unsolicited communication transaction when the event is generated

9.2.1.2 Data Logging functionality:

The controller is required to have the following data logging functionality in addition to its event capabilities. The controller should support both event and data log operation simultaneously, including both event generation and logging on the same controller data objects.

- The software and hardware should provide time stamped data logging supporting, as a minimum, separate logging trends.
- Logging should be selectable on digital input, digital output, analog input and analog output data objects.
- Analog logging should be by 32-bit floating point engineering values.
- Analog logging should also include data compression through a deviation configuration for each log trend, i.e. prevent storage of a log sample at the prescribed time if the value has not sufficiently changed.
- Logging should be configurable to include current value and summary statistics at a defined interval, including average, maximum and minimum logging trends.
- Logging frequency should be selectable by the user for each logging trend and vary from 5 minute to 1 Day.
- The controller should be support at least 1MB/30,000 records of storage for logged data.
- Configuration of the data log function should be made through the controller configuration without need for specific IEC61131-3 user programming.

- Logs should be enabled or triggered by timers or process events. As a minimum, each data log state should be enabled by a digital point state without requiring user programming
- It is recommended that all data should be able to be retrieved and made available as a .csv file for use in Excel, Access, or HMI software. Data uploaded to a PC should be supported using direct serial connection, leased telephone lines, radio, external memory media and via the SCADA communication link.

9.2.1.3 Configuration:

- The device should be configured locally with a Windows-based PC application through a serial USB connection or wireless connection (Bluetooth)
- Remotely, with a SCADA host software platform that utilizes custom configuration objects and transmits configuration parameters to the device via the GPRS network.

9.2.1.4 Security

- The controller should provide communications security using recognized SCADA security open standards.
- A secure administration application should be provided for the Security Administrator to issue and track security keys, users and configuration computer nodes.
- The administrator application and the controller should provide a mechanism for securely loading encryption and hash keys without exposing the raw key values to the end user.
- The administrator application should provide the capability of specifying security configuration for groups of controllers, users (via username/password) and individual configuration computers.
- Controllers that are required to communicate with each other should be capable of being managed as a security group.
- All communication ports on the controller should be capable of being secured. A single “local access” port free from encryption is permitted for use by the configuration application. Bridging of unprotected communication from this port to the secure communication ports is not permitted.
- All communication ports should be capable of being disabled through user programming on the controller to provide custom communication security solutions for peripheral devices.

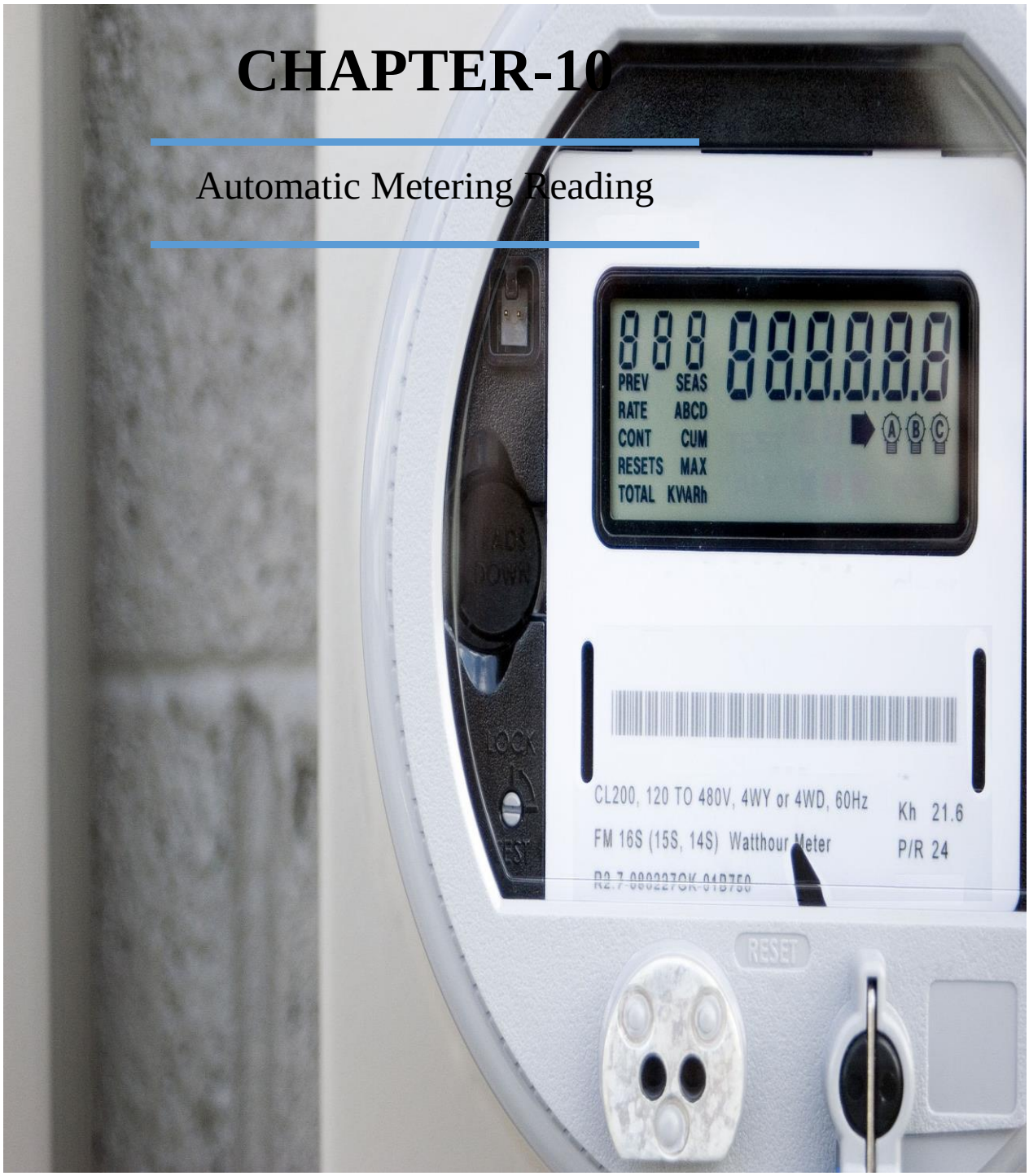
- Access to controllers from configuration computers should be capable of being secured at the computer node level through unique keys.

9.2.1.5 Warranty:

The manufacturer should warrant the hardware specified above against all defects in material and workmanship for a period of **three years.**

9.3 Vendor List for Data logger Controller

Data logger Accepted Brand	Description
Sofrel Lacroix	http://www.lacroix-sofrel.com/ (LS42, LS-Flow, LS-Pressure, LT-Level)
Halma Water	https://www.hwmglobal.com/ (Multilog)
ABB	https://new.abb.com/products/measurement-products/flow/electromagnetic-flowmeters/water-waste-water/aquamaster-few400-electromagnetic-flowmeter / (Aqua master 3, Aqua master -4 Flow meters with DL Solution)



CHAPTER-10

Automatic Metering Reading

10. AMR Technical Specification

10.1 General

- The Meter Device should be an intelligent, capable of both data acquisition and local data processing. It should be based on multiprocessor architecture, in which a co-processor is used for handling on-board input/output channels
- The Meter Device should be configured with a modern Windows application and Configuration should be developed and downloaded either directly to the Meter Device using a standard RS-232 interface cable, Bluetooth, USB, Ethernet, or remotely through the communication network media such wireless radios.
- The Meter Device should be supplied with MIL Spec connector/ Fittings which can comply IP68 or NEMA 6P Submersible requirement, it should be robust construction with sophisticated electronics and Long battery life have been proven deliver consistent and reliable data in some of the harshest environment.
- The Meter Device should satisfy the operating temperature which is +1 Deg to +70deg Celsius. The meter device should satisfy the Working temperature range for water medium in between °C +1 ... +50 (cold water) / +1 ... +90 (hot water)
- The Meter Device should satisfy different interfaces for Communication and Measurement minimum like Optical, Radio, M-Bus, Pulse etc if required and should be available with Display unit for basic information about Flow and device.
- The Meter Device should be configured with user-friendly software for which firmware updates should be installed quickly and efficiently, Also upgrades should be possible through remotely other than direct connection with device.

10.1.1 Processor Unit:

- The CPU should include a real time clock/calendar, accurate to within one minute per month, with lithium battery backup. The battery will maintain the memory and clock/calendar in case of power off time. The Meter Device should provide an adjustable period for updating time from the Application Server remotely in order to achieve accurate clock time.
- The CPU should include an internal clock with at least 10 ms resolution and be capable of applying timestamps at this resolution to internal and externally obtained data.

10.1.2 Configuration Settings:

- Meter Device Read/ Write configuration should be via Specific Software application which is licensed Permanently and Firmware updates should be available as per agreement
- Configuration Read/ Write operation should be done via universal medium such as Bluetooth, SMS, NFC, RS232, and RS485 or via remote server settings Etc.
- Channel configuration should be as standard for Digital and Analog Signals in the different formats like Pulse, 4-20mA, Standard meter etc. depending on the applications.
- Archive or Logging configuration should be available for different periods of time as per the requirements, also have the facility to extract or Update to the Application server as required.
- Threshold/ Alarm settings should be available for different period and the facility to immediate transmit data to the server as per the threshold criteria if required.
- Optical For configuration of display information and radio telegram, to switch to the various display loops.

10.1.3 Diagnostics:

- Meter Device Diagnostic LEDs should be included Meter Device status, Connection Status and Network Status if required as per site conditions.
- Meter Device should be capable of communicating and sending latest updates with Application server
- Meter Device should provide information of Battery level which is equivalent to the remaining days as per the current battery Voltage which can utilize for the power management

10.1.4 Data Acquisition & Archiving:

- Meter Device should have the facility for periodical archiving of meter indices, average calculation and Analog measurements if required.
- Meter Device should have the facility to send reports daily based on the archived data and average calculation minimum once in a Day as required.

10.1.5 Communication with Application Server

- Meter Device should be able to communicate with Application server as per the settings during particular interval
- Intermediate channel/Protocol for communication should be verified and compatible with the existing Application system and Approval should be based on the Pilot Test and configuration (Not recommended; Only if no have facility to connect directly with Application Server or Water management system)
- Meter Device should be communicate with the Central Application system with approved data transmission protocol via GPRS Network by Secure and Standard recommended way as per client Network Policy.
- Meter Device should able to communicate with hand held devices or Mobile if required for threshold or Warning Messages
- Meter Device Shall be with a built in antenna or Transmitter receiver for signal transmission according to the signal criteria for communication.
- Meter Device Shall be with Radio interface for which frequency as per approved from client like 434 or 868 MHz, Prios, Real data, Open Metering Standard (OMS-Generation 3, Profile A, or OMS-Generation 4, Profile B, selectable) M-Bus 2400 Baud (adjustable to 300 Baud), configurable telegram, cable length 1.5 m, power supply only via built-in battery Pulse (Open collector) 2 configurable pulse outputs, cable length 1.5 m
- Meter Device should comply the communication interfaces with the following specification which is IEC 870-5-1 corresponding to EN 1434-3 std. requirements. Meter should equipped with M-Bus communication which is over a two-wire line in addition to the other required as approval.

10.1.6 Communication Protocols

Open Standard Protocols, The Meter Device should be supported one or more of the following industry standard protocols:

- Modbus Master/Slave
- BACNet
- Narrow band
- OMS ; Open Metering Standard (OMS-Generation 3, Profile A, or OMS-Generation 4, Profile B, selectable

- MAC Layer communication protocol
- Open Modbus/TCP Client +
- Open Modbus/TCP Server +
- WITS (Water Industry Telemetry Standard)/DNP3
- TCP/IP communications should be supported over Ethernet, asynchronous serial PPP, GPRS, 1xRTT and 3G cellular IP networks.
- Ability to transfer complete configurations and IEC61131-3 application programs and data over the communication network to the Meter Device using approved Meter Device protocol. The Meter Device should support these facilities via RS232, RS485, TCP/IP PPP serial links, TCP/IP Ethernet, Radio, etc.
- Meter Device should Equipped with the following interface technology if required depends on Different application
- Telegram formats: Communication complies with IEC 870-5-1 Tele control equipment and systems; Transmission protocols; Section One-Transmission frame formats.
- UART (Universal Asynchronous receiver Transmitter): Selectable Baud Rates; M-Bus: 300 and 2400 bauds (300 bauds: transmission in Interrupt Mode),
- Protocol layer: IEC 870-5-1 corresponding to EN 1434-3, Data output (RSP_UD)

10.1.7 Data Concentrator/Interface Unit for AMR

When acting as a master for its open protocols, the controller should be able to instigate communications with remote devices and concentrate data from the multiple remote devices in to the controller database. This should include processing, integration and storage of current value data, point quality flags and historic data by means of time-stamped events. I.e. sequence of events with timestamps and point quality received from a remote device should be preserved for each individual event and incorporated in to the controller database for later extraction, including via a different protocol. Further the controller should provide for the mapping of controls to multiple remote devices including transparent mapping of controls from a slave protocol to a master protocol without requiring user programming.

Data concentration should include the following fully or maximum features as required or approval:

Data Concentrator should have the Communication interfaces and Protocol as mentioned below which can selectable to fulfill the requirement as per approval

- DNP3 serial protocol as a master
- DNP3 over IP (TCP and UDP) as a master
- Meter Bus (M-Bus),RS-232,GPRS
- Narrowband Internet of Things (NB-IoT) is a Low Power Wide Area Network (LPWAN) radio technology standard developed by 3GPP to enable a wide range of cellular devices and services
- A low-power wide-area network (LPWAN) or low-power wide-area (LPWA) network

- MAC Layer communication protocol
- FTP (File transfer Protocol)
- Ability to put remote device communications in service and out of service on an individual device basis
- Ability to enable and disable setting remote device time (on a per device basis)
- A variety of polling algorithms for requesting event and static data
- Accept Unsolicited message reports from remote devices
- Full support for integrating point quality and event timestamps from remote device in to the controller's database without loss of information
- Independent polling strategy to minimize delays and recover from loss of communication with a remote device
- Communication status for each remote device available in the controller's point database
- Communication statistics for polling and unsolicited messages available in the controller's point database
- Provision for user program or protocol commands to the controller to force an event poll, integrity poll, or remote device restart.
- The no.of Meters and length of total connectivity in a loop should be as per the approval and detailed design. Minimum Daily limit for data storage should satisfy 2000 records
- Meter Concentrator Device Diagnostic LEDs should be included Meter Device status, Connection Status and Network Status if required as per site conditions.

- Ability to select data concentrator to stop collecting data when event buffers are full also memory extension facility should provide
- Meter Concentrator Device should capable of archiving data and extract all data as required like for a period of time or All Logged data.
- Meter Device should log all data for the Particular period of time configured and should able to send all data together during the interval to the Application server.
- Meter Device should have the facility to Verify and update the Data Transmission completeness as per the recording.

10.2 Mechanical Design

- The controller should be suitable for mounting on DIN rail mount or should be come with proper bracket for Wall mounting purpose; Front access to all controls, indicators, communication ports and power supply connection should be provided. Communication Connector cable and connectors should available for easy access
- Mechanical Design should be coated with conformal coating, for protection against humidity and corrosion if required.
- All system components should be constructed of corrosion resistant zinc plated steel with removable metal covers or High Grade Plastics with robust and durable design which has succeeded Ingress Protection requirements if application required.

10.3 Environment

- The controller should operate over an ambient temperature range of -40°C to 70°C (-40°F to 158°F) with a relative humidity 5% to 95%, non-condensing.
- The controller should operate from nominal Battery power supplies,

10.4 Certifications and Standards:

- The controller should be certified for electrical safety or applicable low voltage directive.
- The controller should be certified to meet or exceed the following standards:
- RF emission compatibility: FCC title 13 part 15, Subpart B, Class A
    - CISPR22 Class A
    - Electrical safety classification: c(CSA)us, CAN/CSA-C22.2 No. 61010-1

- Hazardous area classification: CSA Class 1, Division 2, Group A,B,C,D
- Discharge Immunity: EN61000-4-2
- Radiated immunity: EN61000-4-3
- Fast transient immunity: EN61000-4-4
- Surge immunity: EN61000-4-5

10.4.1 Firmware Upgrades

The operating system firmware should be capable of being upgraded locally and remotely, utilizing compression techniques to minimize the communications transaction size for loading of firmware patches or a new firmware image. The firmware upgrade should not commence until complete reception of the firmware image. Controller operation should not be interrupted during the communications transfer of the firmware image.

10.4.1.1 Security

- The controller should provide communications security using recognized Application Server security open standards.
- A secure administration application should be provided for the Security Administrator to issue and track security keys, users and configuration computer nodes.
- The administrator application and the controller should provide a mechanism for securely loading encryption and hash keys without exposing the raw key values to the end user.
- The administrator application should provide the capability of specifying security configuration for groups of controllers, users (via username/password) and individual configuration computers.
- Controllers that are required to communicate with each other should be capable of being managed as a security group.
- Once security is enabled on a controller, communication link security should not be disabled unless a controller's configuration is completely erased.
- All communication ports should be capable of being disabled through user programming on the controller to provide custom communication security solutions for peripheral devices.
- Access to controllers from configuration computers should be capable of being secured at the computer node level through unique keys.

10.4.1.2 Warranty:

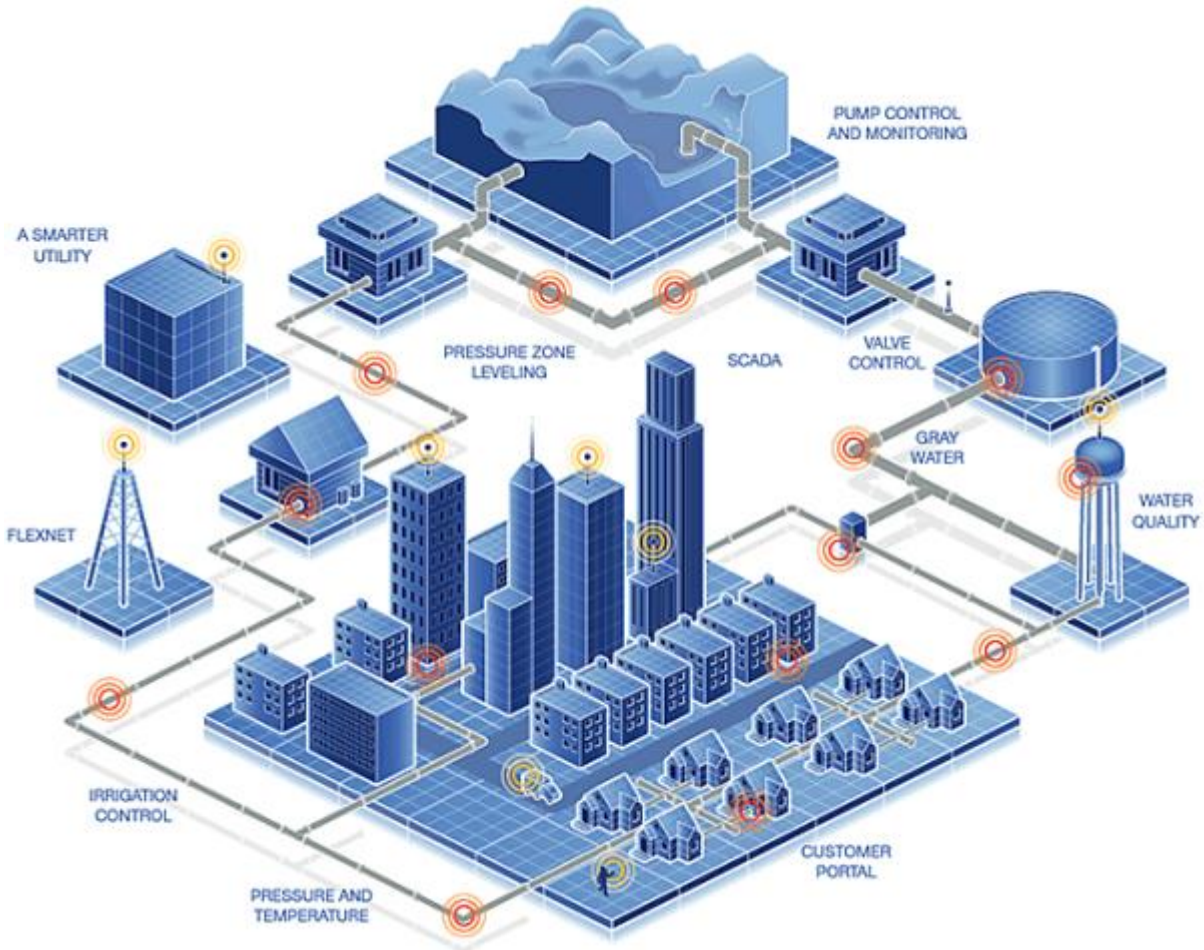
The manufacturer should warrant the hardware specified above against all defects in material and workmanship for a period of **Five years.**

10.5 Vendor List for AMR Controller Unit

AMR Accepted Brand	Description
DIEHL	https://www.diehl.com/metering/en/portfolio/water-metering/ (HYDRUS,ALTAIR,WESAN,AURIGA,IZAAR
SENSUS	https://sensus.com/solutions/automatic-meter-reading-amr/

CHAPTER-11

Communication Methodology



11. Communication Methodology:

11.1 Private Cloud Management (Private Network)

11.1.1 Booster Stations:

- A single cloud (BS Primary Cloud) to manage the Booster Stations network is implemented to minimize the administration and maintenance headache and to eliminate the single point of failures resulted from having different equipment's supporting different technologies.
- The BS Primary Cloud will allow the bi-directional communication between the different Booster Stations.
- All Booster Stations should be connected and consistent with the BS Primary Cloud requirements. New Booster Station should be added to the existing BS primary cloud using the same unified protocol, RTU specs.
- Booster Stations managed by a Water Treatment Plant is an exception to the above, and should be connected and consistent with the Plant Cloud infrastructure (will be out of the Booster Stations Primary Cloud).
- Exception to the above; other than "Booster Stations managed by a Water Treatment Plant", has to be justified by the necessity of building a new cloud (BS Secondary Cloud) and should be approved by the Operations Director and the IT Director.
- Minimum number of BS Secondary Clouds should be maintained as much as possible.

11.1.2 Lifting Stations:

- A single cloud (LS Primary Cloud) to manage the Lifting Stations network is implemented to minimize the administration and maintenance headache and to eliminate the single point of failures resulted from having different equipment's supporting different technologies.
- The LS Primary Cloud will allow the bi-directional communication between the different lifting Stations.
- All Lifting Stations should be connected and consistent with the LS Primary Cloud requirements. New Lifting Station should be added to the existing LS primary cloud using the same unified protocol, RTU specs.
- Exception to the above has to be justified by the necessity of building a new cloud (LS Secondary Cloud) and should be approved by the Operations Director and the IT Director.

- Minimum number of LS Secondary Clouds should be maintained as much as possible.

11.1.3 Water and Waste Water Treatment Plants

- In a Plant one single cloud should be implemented (Plant Internal Cloud); using same protocols and consistent SCADA equipment's, such as PLC's and RTU's. This is to minimize the administration and maintenance headache and to eliminate the single point of failures resulted from having different equipment's supporting different technologies.
- The Plant Internal Cloud should allow the bi-directional communication between the different Process Functions with the Main PLC, as well as with the Wells inside the same plant.
- If there is a need to have bi-directional communication between a Plant and any other plants, then the Plant Internal Cloud Specs should follow the same specs (Protocols and equipment) as the other Plants Internal Cloud specifications.
- Fiber Optic cables should laying in ring mode which apply the redundancy of communication

11.2 Ways of Communication:

11.2.1 Booster Stations:

- BS Primary cloud: RTU Connectivity to Central SCADA is Direct link through OPC to Central SCADA
- BS Secondary cloud: RTU Connectivity to Central SCADA is recommended to be direct through Driver or OPC to eliminate the existence of many different FIU's.
- Primary Communication Link between the RTU's and the Central SCADA in the Business Unit Control Room and/or the HQ Control Room - BS Primary Cloud and BS Secondary Clouds - is through 3G/GPRS (VPN-To-MPLS). (Industrial communication)
- Backup Communication Link between the RTU's and Central SCADA in the Business Unit Control Room and/or the HQ Control Room - BS Primary Cloud and BS Secondary Clouds - is through Radio using the defined frequencies by National Water Company if recommended.

11.2.2 Strategic Booster Stations (e.x. HPT):

- Main RTU should be connected to the Central SCADA system using VSAT or MPLS technology with sufficient bandwidth that will be decided during the design phase.

- Two redundant links are required with failover technique connecting the Main RTU and the Central SCADA system.

11.2.3 Lifting Stations:

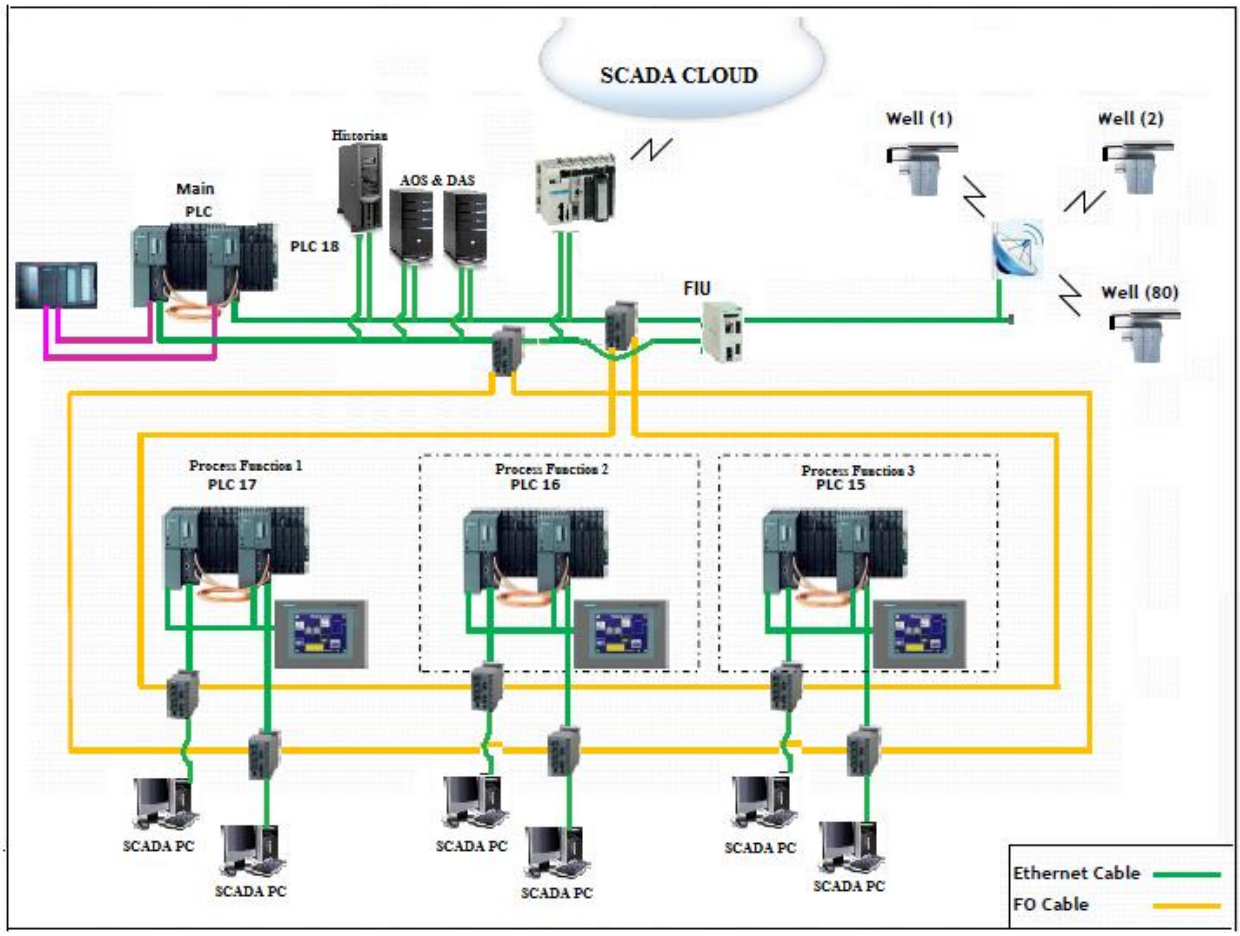
- LS Primary cloud: RTU Connectivity to Central SCADA is Direct link through OPC to Central SCADA
- LS Secondary cloud: RTU Connectivity to Central SCADA is recommended to be direct through Driver or OPC to eliminate the existence of additional FIU's.
- Communication Link between the RTU's and the SCADA for LS Primary and LS Secondary Clouds is through 3G/GPRS (VPN-To-MPLS).

11.2.4 Water and Waste Water Treatment Plants

- Main PLC's should be connected to all Sub-PLC's through Fiber Optics using SCADA protocol/Modbus/IP protocol or ProfiNet.
- Main PLC's and Sub-PLC's should be connected using Ring Topology to minimize the possible downtime as much as possible. When possible two redundant Rings should be implemented.
- Main PLC should be connected to the Local SCADA System using Ethernet / IP
- Main PLC should be connected to the Plant RTU's (Gateway & Sub) through one FIU using Modbus/IP, Ethernet/IP or Profinet.
- Main PLC should be connected to the Central SCADA System through one dedicated Gateway RTU.
- Sub RTU's should be connected to the FIU Receiver using GPRS when applicable or Radio when not applicable. Sub RTU's connectivity solution should be unified.
- Gateway RTU should be connected to the Central SCADA system using VSAT or MPLS technology with sufficient bandwidth that will be decided during the design phase.
- Two redundant links are required with failover technique connecting the Gateway RTU and the Central SCADA system in the Business Unit Control Room (Operations DMZ)and the HQ Control Room (Operations DMZ).
- Redundant FIU for High Availability should be provided.

11.2.5 Water Treatment Wells:

- LS Primary cloud: RTU Connectivity to Central SCADA is Direct link through OPC to Central SCADA
- LS Secondary cloud: RTU Connectivity to Central SCADA is recommended to be direct through Driver or OPC to eliminate the existence of additional FIU's.
- Communication Link between the RTU's and the SCADA for LS Primary and LS Secondary Clouds is through 3G/GPRS (VPN-To-MPLS) or through Radio using the defined frequencies by National Water Company - Riyadh Business Unit or WiFi communication within open & allowed frequency 5Ghz.



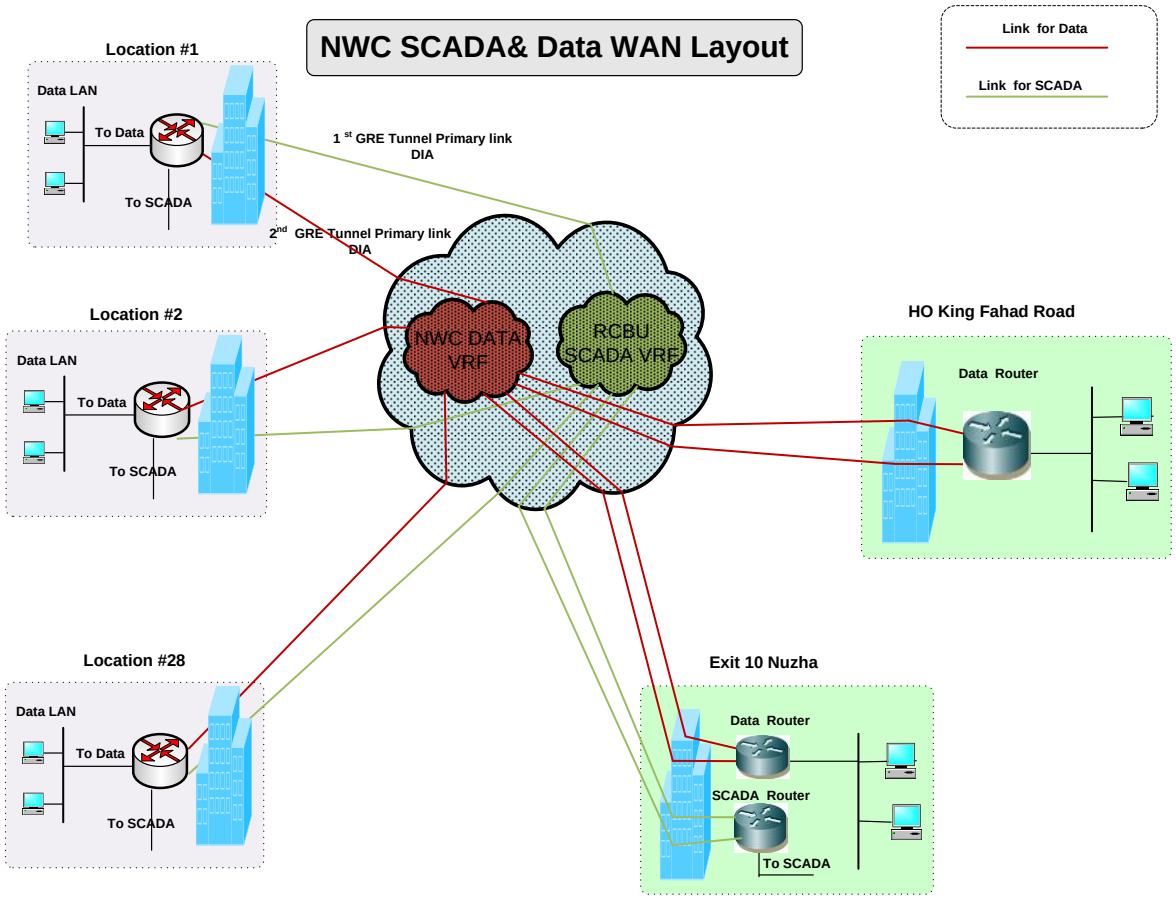
11.2.6 Network Data Loggers:

Communication with Central SCADA should be provided via GPRS

11.3 Network Architecture:

Two Service Providers with two different bathes and technologies are required to utilize their network infrastructure facility to provide high availability services & end-to-end managed WAN services. This is through:

- Providing true redundancy services for all locations using different local loops.
- There should be two different VRFs; one for Data and a separate one for SCADA, configured to separate totally the business data Traffic from the SCADA Traffic.
- A full mesh and star topology should be implemented for SCADA Network.
- Plants and Sites should only be allowed to communicate with The Business Unit Control Room (Operations DMZ) and HQ Control Room (Operations DMZ) for Historian database synchronization and engineering purposes when required.
- A dedicated Leased Line Circuit (MPLS) link should be provided to the Business Unit Control Room as a primary link, connecting the control room Operations DMZ to the SCADA VRF Cloud with Minimum of 4M Bandwidth.
- Another dedicated link should be provided to the Business Unit Control Room using different service provider and/or technology as a Secondary link, connecting the control room Operations DMZ to the SCADA VRF Cloud with Minimum of 2M Bandwidth.
- All Local site IPs provided only by IT department.

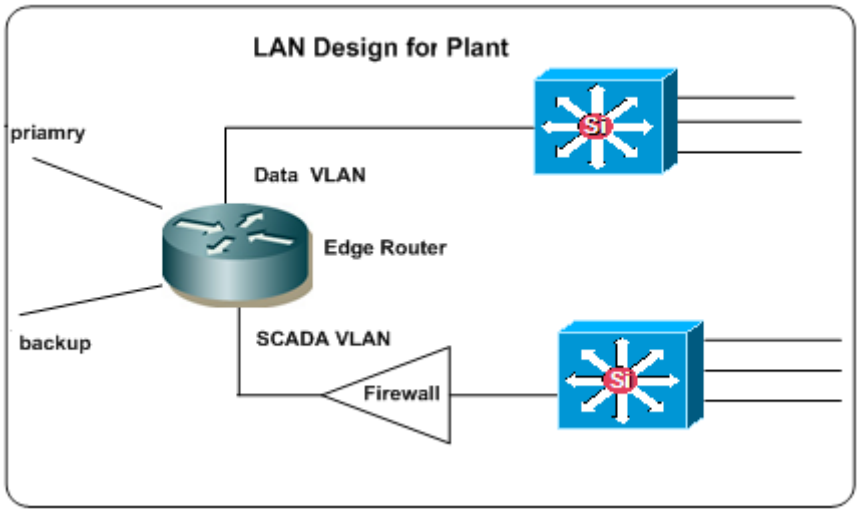


11.3.1 Treatment Plants and Strategic Booster Stations

Two Service Providers with two different bathes and technologies are required to utilize their network infrastructure facility to provide high availability services & end-to-end managed WAN services. This is through:

- Providing true redundancy services for all locations using different local loops.
- SCADA Traffic should be routed to SCADA dedicated and isolated VRF through dedicated and isolated Subnet.
- SCADA Traffic can only be routed with restricted rules to the Operations DMZ; protected zones established in the HQ and the Business Unit Control Rooms.
- Primary Link should be established on dedicated Leased Line Circuit (MPLS). If not available, it should be provided on VSAT technology.
- Cost effective solutions as backup for the remote locations by using 4G/GPRS (VPN-To MPLS) or existing Radio service (if available)as a backup link. Backup Link should be on VSAT technology if 4G/GPRS or existing Radio service cannot be implemented or can be unreliable.

- If the Primary and Backup Links are decided on VSAT technology then both should be provided by two different VSAT providers (Satellites).
- Service Provider should provide the required Hardware for both Primary and backup links as well as for any hardware needed to isolate SCADA VLAN in the Plant location. This is in order to provide end-to-end management solution.
- 24x7 monitoring system for all connectivity services should be provided (Availability, Utilization, and traffic analyzer).
- The planned design for LAN in each location should be as per the below drawing



- Below table contains all details Standards and Bandwidth:

Standard Priority (High = 1)	Primary Media type & B.W	Backup Media Type
1	Minimum of 2M MPLS	3G (VPN-to-MPLS)
2	512 Kbps thru VSAT	Radio Tech.
3		512 Kbps thru different VSAT provider

11.3.2 Booster/Filling Stations

- Primary links for all locations should be on 4G/GPRS (VPN-to-MPLS)
- Backup Link should be provided on radio Technology.
- Service Provider should provide the required Hardware for both Primary and backup links as well as for any hardware needed to isolate SCADA VLAN from DATAVLAN. This is in order to provide end-to-end management solution.

- 24x7 monitoring system for all connectivity services should be provided (Availability, Utilization, and traffic analyzer).

Standard Priority (High = 1)	Primary Media type & B.W	Backup Media Type
1	3G/GPRS (VPN-To-MPLS)	Radio Tech.
2	Radio	Not uses

11.4 Protocols Standards:

11.4.1 Server and Workstation Communication Protocols

11.4.1.1 TCP/IP:

The SCADA servers and client Computers communicate via TCP/IP protocol over Gigabit Ethernet twisted pair (LAN). Each device on the LAN is assigned a permanent fixed IP address. This LAN is completely separate from the HQ LAN, Business Unit LAN and other networks (Internet) for security reasons.

11.4.2 PLC and RTU Communication Protocols

The following communication protocols are used to communicate between the "AOS and DAS" servers and the plant PLC's, field RTU's and FIU's.

11.4.2.1 Modbus Ethernet

A protocol where Modbus is embedded within TCP frames. Ethernet is the primary communication path between the PLC's/RTU's and the SCADA System, as well as Field RTU's with the FIU unit. The PLC's have dedicated IP addresses..

11.4.2.2 Modbus Plus

An asynchronous protocol where embedded Modbus messages are transmitted over an RS485 link. This token passing protocol is supported by fiber to RS485 devices. This communication path is configured in a ring where the media converters generate an artificial break in the fiber ring whereas in the event of an actual fiber break the media converter will remove the virtual break while communication is maintained.

Modbus Plus is used as a backup communications path to the Modbus Ethernet. This method provides a redundant PLC communication protocol and path in the event that the Modbus Ethernet link fails.

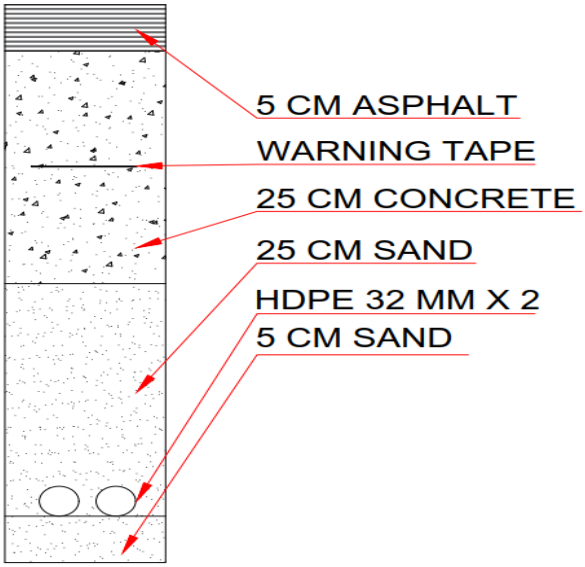
11.5 Local network

All site should be covered by local network to transmit the data between the devices to the local or remote automation systems

11.5.1 Fiber Optic Specs

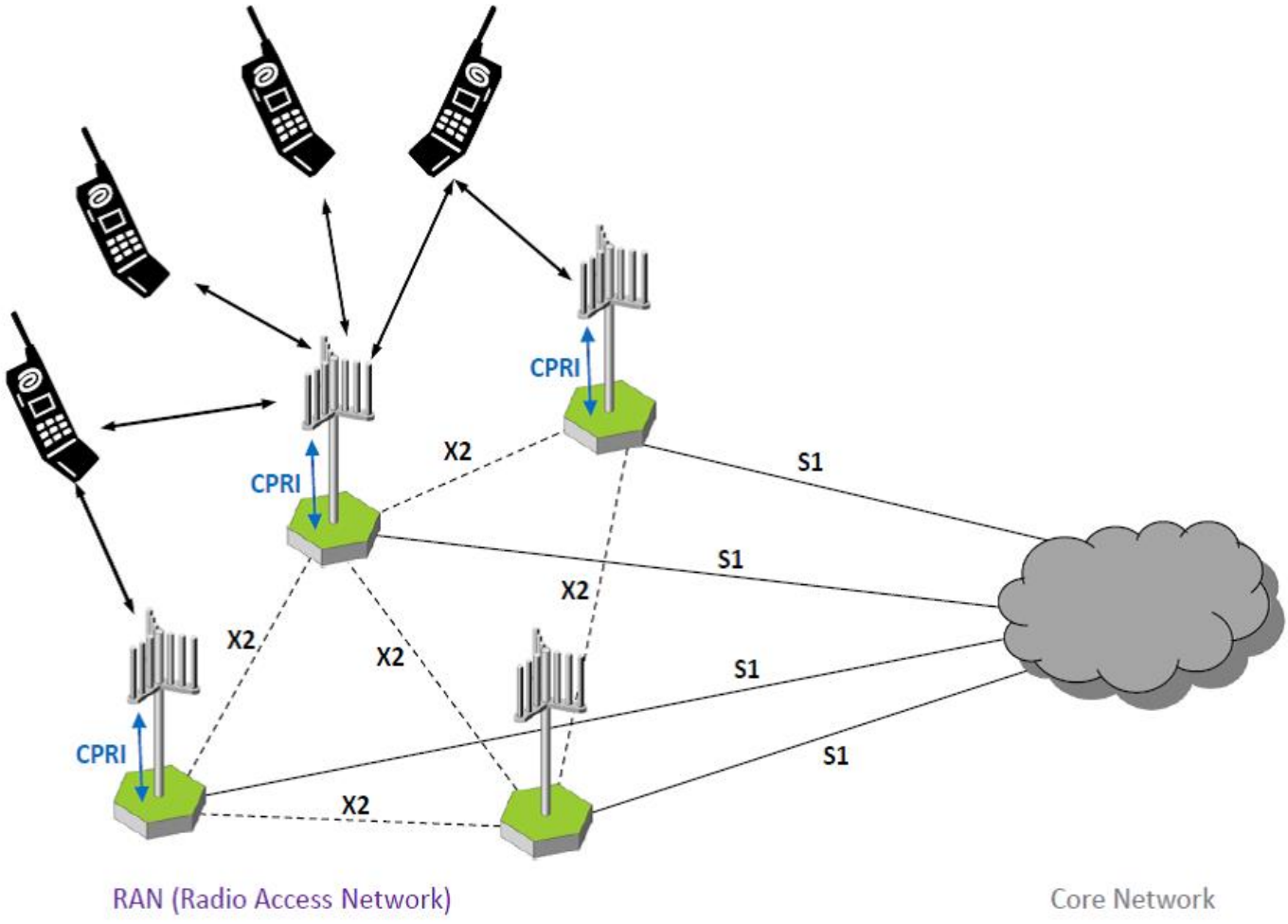
The contractor should follow the standard (OSP fiber optics civil works guide, The Fiber Optic Association, Inc) & Technical Standards for Outside Plant (OSP) Installations from CITC).

- Between cities follow (Technical Standards for Outside Plant (OSP) Installations from CITC)
- The drilling depth should be not less than 60 cm inside the city or site
- Excavate on the side of the roads and the manholes locations without blocking the roads or the main intersections inside the site.
- Clean up excavation wastes to the containers and remove the containers outside the station.
- Put a layer of fine red sand inside the excavation paths before lay the pipes inside them.
- Install manholes with iron covers with acceptable quality on main streets.
- Inside excavation path, should lay 2 pipes (size 32 mm) with splitter per 2 m to organize and insert into the manholes.
- Should Put 10 cm layer of sand on the pipes to protect it.
- Cover the excavation paths with approved concrete with a minimum thickness of 20 cm
- Inside excavation path, Lay a magnetic warning tape inside the concrete.
- All excavation paths must return to their pervious state whether it's asphalt, agricultural or tile.
- Every 200 m should have manhole
- Provide iron pipe with all required accessories inside each building to connect the fiber optic cables up to the patch panel.
- Provide patch cords between patch panels and fiber optic switches.


5 CM ASPHALT
WARNING TAPE
25 CM CONCRETE
25 CM SAND
HDPE 32 MM X 2
5 CM SAND

CHAPTER-12

Digital Radio Communication System Standards



12. Digital Radio Communication System Standards:

12.1 Radio Equipment Descriptions

12.1.1 Radio and Modem

Both Master and Remote Station equipment should contain a fully integrated all-digital data radio transceiver circuit, digital data modem and digital data multiplexer circuit inside the one unit. Combinations of radio transceivers from one supplier and modems from other suppliers should not be permitted.

The equipment should be capable of operating at full specification from –30ºC to + 60ºC and have a compact and rugged all metal alloy die cast housing for the Remote Station.

The transmitter power control circuit should feature an automatic power reduction circuit to prevent over-heating of the transmitter in the event that the ambient temperature exceeds the specified maximum. The reduction in transmitter power should be between 6 and 9 dB.

The receiver circuitry in the data radio should employ automatic frequency control that permits the receiver frequency to track the frequency of the received signal by up to +/- 3kHz.

Total power consumption should be minimized with sleep mode operation capability in the Remote Station.

Internal operational firmware in Remote Stations should be stored in Flash memory and be easily upgraded in the field using a portable computer.

Both Master and Remote Station equipment should have externally visible multi-function LED status indicators for DC Pwr, Tx, Rx, Sync, TxD and RxD for both data ports.

12.1.2 Data Ports

The Master and Remote Stations should feature two independently configurable user data ports. There should be a separate System Port for Configuration as well as (optional) Network Management and Diagnostics.

The data ports should be individually and separately user selectable for interfacing to asynchronous RS-3232 data circuits communicating at data rates from 300 bps up to 76,800 bps (38,400 bps max. when both ports enabled).

The over-the-air data transport should use an industry standard nonproprietary protocol, e.g., HDLC, and the modem should be compatible with most industry standard data protocols. eg: MODBUS, DNP-3, IEC 870 etc.

12.1.3 Auto Tx enable

Both Master and Remote Station equipment should provide automatic Tx enable so that in non-continuous transmit operation, the transmitter is only enabled when data needs to be transmitted. At other times it will automatically switch off. No intervention is required from externally connected equipment, e.g., the RTU.

12.1.4 Multiple Data Streams

The data radio system should be able to support simultaneous delivery of up to 255 multiple data streams and data protocols on a single radio channel allowing data streams from multiple different equipment vendors to be transported on the one radio system.
Both Master and Remote Stations should support flexible data stream routing providing optimum radio channel efficiency by allowing each data port to be separately configured to selectively route and repeat individual and grouped data streams through the modem as well as into and out of the user data ports.
Internal data message buffering should allow store and forward of selected data streams simultaneously with the transmitting and receiving of other data streams through the local user data ports.

12.1.5 Collision Avoidance

The equipment should feature a data collision avoidance mechanism to allow simultaneous polling of one Remote Station by the Master Station and spontaneous, unsolicited reporting from other Remote Stations.
The collision avoidance should function with a Master Station which is configured for continuous transmission and should inhibit Remote Stations from transmitting to the Master Station once the Master Station has commenced receiving data from another Remote Station.
The collision avoidance should feature a random delay re-transmission mechanism which avoids multiple Remote Stations from attempting to transmit simultaneously once another Remote Station ceases to transmit data to the Master Station.

12.1.6 Operating Mode

The system should provide wireless serial data communications between the SCADA Master / Control Application and the RTU equipment at the remote locations. For the PTMP mode, the

equipment should include a collision avoidance capability as described above to permit the system to be configured for simultaneous operation in the following modes :

- Polling from the Master only (no spontaneous reporting from RTU)
- Spontaneous reporting from the slave RTU equipment (no polling from the Master)
- Combined polling from the Master and spontaneous reporting from the RTU equipment

12.2 Radio Equipment Specifications

12.2.1 Remote Station Equipment Specifications

12.2.1.1 General

- Operating Mode: Half duplex or optional full duplex (with external duplexer) Configuration: Fully configurable via Windows based software
- Firmware: Field upgradeable flash based Memory
- Enclosure / Housing: metal die cast
- Dimensions: 170 mm x 150 mm x 42 mm
- Weight: <= 1.3 kg

12.2.1.2 Transmitter

- Frequency Range: 330-520 MHz (in various frequency sub-bands)
- Tx/Rx Frequency Splits: Fully software configurable for Tx/Rx frequency splits within frequency sub-band without the need for re-tuning
- Channel Selection: Dual synthesizer, 6.25 kHz channel step
- Channel Spacing: 12.5 or 25 kHz
- Frequency Stability: <1ppm - 30 to 60 ºC ambient (standard) Frequency Aging: <= 1ppm/annum
- Tx Power: Half Duplex Mode = 5W (+37 dBm) 1 dB software adjustable with over-temperature protection
- Full Duplex Mode = 1W (+37 dBm) 1 dB software adjustable with over-temperature protection
- Modulation: Narrow band digital filtered binary GMSK Occupied Bandwidth: Complies to FCC, ETSI, ACA requirements Tx Key up Time: < 2 mSecond
- Timeout Timer: Programmable 0-255 seconds
- Tx Spurious: <= -37 dBm
- PTT Control: Auto (Data ports) / RTS line override on all ports

- NOTE: Data ports should operate using 3 wires–Tx, Rx, Gnd.

12.2.1.3 Receiver

- Frequency Range: 330-520 MHz (in various frequency sub-bands)
- Tx/Rx Frequency Splits: Fully software configurable for Tx/Rx frequency splits within frequency sub-band
- Channel Selection: Fully synthesized, 6.25 kHz channel step
- Channel Spacing: 12.5 / 25 kHz - fully software configurable Frequency Stability: <1ppm - 30 to 60 ºC ambient (standard) Frequency Aging: <= 1ppm/annum
- Sensitivity: -118 dBm for 12 dB SINAD Selectivity: Better than 60 dB Intermodulation: Better than 70 dB
- Spurious Response: Better than 70 dB
- AFC Tracking: Digital receiver frequency tracking
- Mute: Fully software configurable digital mute

Modem

- Data Ports: Two user data ports independently configurable
- Shall operate using 3 wires – Tx, Rx and Gnd.
- Data Serial Port #1: RS232, DCE, 600-76,800 bps asynchronous (38,400 bps max. when both ports enabled)
- Data Serial Port #2: RS232, DCE, 300-38,400 bps asynchronous
- System Port: RS232, 19,200 bps asynchronous
- Flow Control: Selectable hardware/software/3 wire interface RF Channel Data Rate: 4800/9600/19,200 bps Half and Full duplex Data Buffer: 16 kbyte of on-board RAM
- Bit Error Rate: < 1x10 -6 -113 dBm (4800 bps)
- < 1x10 -6 -106 dBm (9600 bps) Data Turnaround Time: <10 mS
- Collision Avoidance: Carrier and data sensing multiple access based collision avoidance system
- Multiple Data Streams: Able to support simultaneous delivery of up to 255 multiple data streams and data protocols
- Each data port should be able to be configured to selectively route and repeat individual and grouped data streams through the modem and the user data ports
- Power Supply
- Power Supply: 13.8 Vdc nominal (10-16 Vdc) Transmit Current: 750 mA max. 1 W

- 1600 mA max. 5 W Receive Current: <125 mA
- Sleep Mode external control, < 1 mA

12.2.1.4 Connections

- User Data Ports: 2 x DB9 female ports wired as DCE (modem)
- System Port: RJ45 for Network Management, Diagnostic and Configuration
- Antenna: N female (additional SMA connector for full duplex option) Power: 2 pin locking, mating connector supplied

12.2.1.5 Diagnostics and Network management

- Standard LED Display: Indicators for Pwr, Tx, Rx, Sync, TxD and RxD (for both data ports)
- Network Management: Optional transparent, non-intrusive (simultaneous with user data) Network Management and Remote Diagnostics incl. :
    - Reporting of the following main parameters (in the indicated units)
- Transmit Power (dBm)
- Received Signal Strength (dBm)
- Internal Temperature (degrees Celsius)
- External DC Power Supply (Volts)
- Received Frequency Error (Hertz)
    - Optional 'over-the-air' remote modification of all radio and modem configuration parameters
    - local storage of data error and channel occupancy statistics
    - In-built Error Rate testing capabilities

12.2.2 Hot Standby Master Station Equipment Specifications

12.2.2.1 General

- Operating Mode: Full duplex with optional internal or external duplexer or Half Duplex
- Configuration: Fully configurable via Windows based software Firmware: Field upgradeable flash based Memory Enclosure / Housing: Metal 19" rack mount
- Dimensions: 2 x Standard Master Station - 2 RU (485 x 90 x 390 mm)
- 1 x Control Panel – 1RU (485 x 45 x 390 mm)
- Weight: Standard Master Station <= 13 kg (excluding optional internal duplexer)

12.2.2.2 Transmitter

- Frequency Range: 330-520 MHz (in various frequency sub-bands)
- Tx/Rx Frequency Splits: Fully software configurable for Tx/Rx frequency splits within frequency sub-band without the need for re-tuning of radio (note - internal and external duplexers have varying splits and require retuning)
- Channel Selection: Dual synthesizer, 6.25 kHz channel step
- Channel Spacing: 12.5 or 25 kHz
- Frequency Stability: <1ppm - 30 to 60ºC ambient (standard) Higher stability GPS referenced option
- Frequency Aging: <= 1ppm/annum
- Tx Power: 5W (+37 dBm) 1 dB software adjustable with over- temperature protection
- Modulation: Narrow band digital filtered binary GMSK Occupied Bandwidth: Complies to FCC, ETSI, ACA requirements Tx Keyup Time: < 1 mSecond
- Timeout Timer: Programmable 0-255 seconds
- Tx Spurious: <= -37 dBm
- PTT Control: Auto (Data ports) / RTS line override on all ports
- NOTE: Data ports should operate using 3 wires–Tx, Rx, Gnd.

12.2.2.3 Receiver

- Frequency Range: 330-520 MHz (in various frequency sub-bands)
- Tx/Rx Frequency Splits: Fully software configurable for Tx/Rx frequency splits within frequency sub-band
- Channel Selection: Fully synthesized, 6.25 kHz channel step Channel Spacing: 12.5 / 25 kHz - fully software configurable Frequency Stability: <1ppm - 30 to 60ºC ambient (standard) Frequency Aging: <= 1ppm/annum
- Sensitivity: -118 dBm for 12 dB SINAD Selectivity: Better than 60 dB Intermodulation: Better than 70 dB
- Spurious Response: Better than 70 dB
- AFC Tracking: Digital receiver frequency tracking
- Mute: Fully software configurable digital mute

12.2.2.4 Modem

- Data Ports: Two user data ports independently configurable
- Shall operate using 3 wires – Tx, Rx and Gnd.

- Data Serial Port #1: RS232, DCE, 600-76,800 bps asynchronous (38,400 bps max. when both ports enabled)
- Data Serial Port #2: RS232, DCE, 300-38,400 bps asynchronous
- System Port: RS232, 19,200 bps asynchronous
- Flow Control: Selectable hardware/software/3 wire interface RF Channel Data Rate: 4800/9600/19,200 bps Half and Full duplex Data Buffer: 16 kbyte of on-board RAM
- Bit Error Rate: < 1x10 -6 -113 dBm (4800 bps)
- < 1x10 -6 -106 dBm (9600 bps) Data Turnaround Time: <10 mS
- Collision Avoidance: Carrier and data sensing multiple access based collision avoidance system
- Multiple Data Streams: Able to support simultaneous delivery of up to 255 multiple data streams and data protocols
- Each data port should be able to be configured to selectively route and repeat individual and grouped data streams through the modem and the user data ports
-

12.2.2.5 Power Supply

- Power Supply: 13.8 Vdc nominal (11-16 Vdc) Transmit Current: 2000 mA max. 1 W
- 3200 mA max. 5 W Receive Current: <1000 mA

12.2.2.6 Connections

- Note: various duplicated configurations are possible
- User Data Ports: 2 x DB9 female ports wired as DCE (modem)
- System Port: RJ45 for Network Management, Diagnostic and Configuration
- Antenna: dual N female (single N female with optional internal duplexer)
- Power: dual redundant 2 pin locking, mating connector supplied
- Alarm Outputs: Common single alarm fault indicator output

12.2.2.7 Diagnostics and Network management

- Standard LED Display:
    - Indicators for Pwr, Tx, Rx, Sync, TxD and RxD (for both data ports)
    - Analogue Bar Graph display of TxPwr, RSSI, DCVolts and
    - Freq. Error values
    - Note – the above indicators are available for both parts of the redundant station together with A/B fault indicators

- Network Management: Optional transparent, non-intrusive (simultaneous with user data) Network Management and Remote Diagnostics incl. :
    - reporting of the following main parameters (in the indicated units)
- Transmit Power (dBm)
- Received Signal Strength (dBm)
- Internal Temperature (degrees Celsius)
- External DC Power Supply (Volts)
- Received Frequency Error (Hertz)
    - optional 'over-the-air' remote modification of all radio and modem configuration parameters
- Standard LED Display:
    - Status Indicators for Pwr, Tx, Rx, Sync for both parts of the redundant Station plus A/B failure indicators
    - Analogue Bar Graph display of TxPwr, RSSI, DCVolts and
    - Freq. Error values
- The repeaters will be hot stand-by or single depending on the number of remotes station to be covered from the repeater. The tenderer should clearly specify the type and number of repeater used.

12.3 Wireless RF/ Sigfox / LoRa Transceivers

- Device should able to transmit up to +15 dBm to +22 dBm with highly efficient integrated power amplifiers.
- Devices should support LoRa modulation for LPWAN use cases and FSK modulation for legacy use cases as per application requirement.
- The devices Shall be designed to comply with the physical layer requirements of the LoRaWAN specification released by the LoRa Alliance
- The radio should be suitable for systems targeting compliance with radio regulations including but not limited to ETSI EN 300 220, FCC CFR 47 Part 15, China regulatory requirements and the Japanese ARIB T-108. Continuous frequency coverage from 150 MHz to 960 MHz allows the support of all major sub-GHz ISM bands around the world.
- Supplier should Provide the technical certificate meeting the criteria for Bandwidth range,Datarate for transmission, Coverage, Power consumption, Battery Life etc.

CHAPTER-13

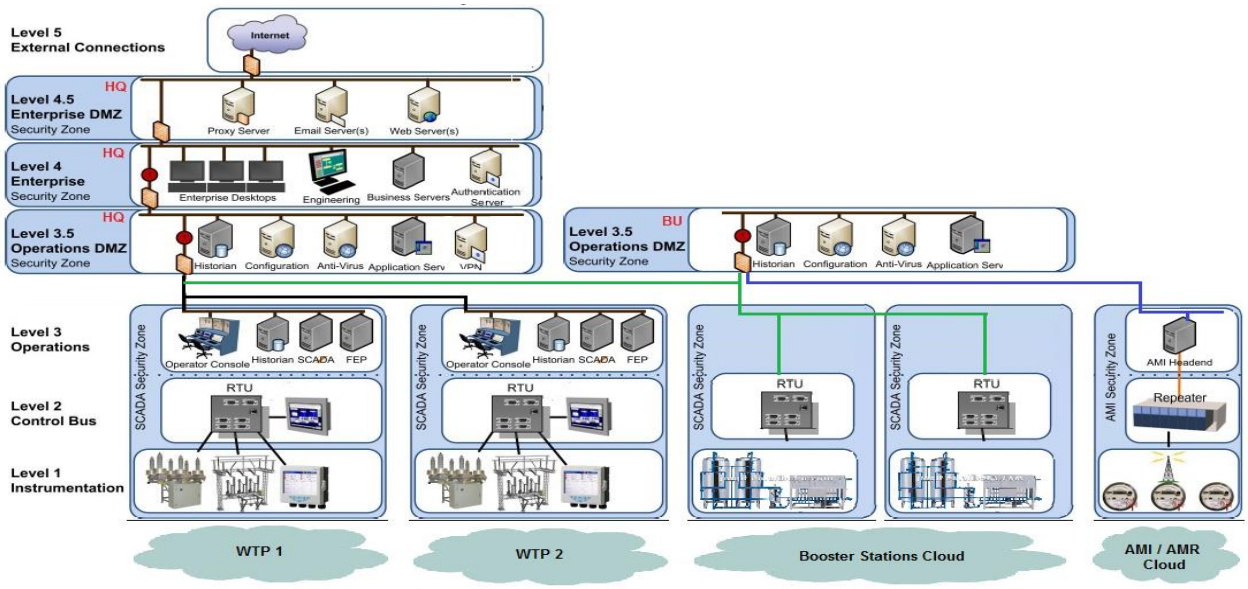
SCADA/ICS Security Architecture

13. SCADA/ICS Security Architecture

13.1 Security Architecture Overview:

The architecture shown in the below (Figure 1) presents the necessary arrangement involving and including:

- Security for the corporate/enterprise network connection to the Internet;
- Security zone architecture intended to isolate critical networks;
- Multiple screened subnets/Demilitarized Zones (DMZ) with no transit traffic.
- It is important that:
- The implementation of the architecture should allow no connections between security zones that are not firewall protected;
- An inventory of all remote access paths that enter the Generic architecture be completed to ensure there are no connections that bypass the firewall infrastructure;
- Remote access be through a VPN connection with strong access controls (i.e., at least 2 factor authentication).



13.2 SECURITY ZONES

A security zone should have a well-specified boundary, and communication between zones should be filtered in accordance with policy. Services, protocols, and applications that are not essential within a zone should be disabled within the zone. Any boundary-crossing traffic carrying those services, protocols, or applications should be blocked at the boundary. For example, ICS/SCADA protocols such as Modbus TCP are required components for controlling

process devices. Whenever possible, these protocols should be disallowed outside the Operations security zone. If that is not possible, then compensating measures need to be taken to protect them from attack and/or misuse from sources outside the process control network.

A zone-based architecture should be implemented to strengthen the capability to perform secure data transfers across the generic SCADA architecture.
Segment the architecture into 5 security zone levels:

- External Connections
- Enterprise DMZ
- Enterprise
- Operations DMZ (HQ Operations DMZ and BU Operations DMZ)
- Operations

The adopted model loosely follows the zone model described in the Purdue Reference Model (PRM) for Computer Integrated Manufacturing of IEC Standard 62254-1 and reference model IEC Standard 622443-1 that suggests a model with 6 zones.

- Zone 1: Automation: Process (equipment under control), Safety & protection, Basic control/Local control),
- Zone 2: Operation Control: Supervisory control,
- Zone 3: Operation support: Operation management,
- Zone 4: Business support: Business planning and logistics,
- Zone 5: Corporate IT: Enterprise IT & common services, and
- Zone 6: External Integration: Connections and information transfer to third parties.

13.3 SCREENED SUBNET (DEMILITARIZED ZONE (DMZ))

A screened subnet (or DMZ) is a perimeter network segment that is logically between two networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted, sources with restricted access to information that needs to be released outside the protected network while shielding the internal network from outside attack.

- An internal DMZ between the enterprise network and the operations network(s) should be added. An Internal DMZ provides enterprise access to operations information, typically the Historian that holds data from the ICS/SCADA network and remote stations.
- No transit traffic is allowed across servers located in the internal DMZ. As a corollary, the historian should not be located on the enterprise network but should reside in the DMZ of HQ and/or the Business Unit, though some secure implementations utilize mirrored historians in the operational network and in the internal DMZ.
- Similar to the above, any server that is jointly accessed from the enterprise network and the ICS/SCADA network should be located in the DMZ and transit traffic blocked.
- Special attention should be paid to locking down DMZ servers (e.g., removing all unnecessary services, whitelisting IP/MAC addresses to limit access to only those workstations approved by policy)
- Traffic should be subjected to port filtering disallowing unnecessary services between security zones. The only devices that should exist in the DMZ are devices that store data that needs to be shared between networks (e.g., Historian).
- Multiple segregated DMZs for Operations Zone Level 3.5 are necessary; one for the HQ and one for every Business Unit.

13.4 FIREWALLS

- UTM to be installed at each security zones.
- Ensure a firewall exists between the enterprise network and the SCADA network.
- Do not allow direct communication between the enterprise network and the ICS/SCADA network. This limitation can be implemented by the use of a Demilitarized Zone (DMZ) as described earlier in this document. If direct traffic between the enterprise zone and operations zone (e.g., engineering access) is required, provide strong authentication and encryption using VPN or SSL/VPN connection.

13.5 Main Security Architecture Requirements

- **Security Architecture main objectives are to:**
    - Restrict logical access to the SCADA/ICS network.
    - Protect individual ICS components from exploitation.
    - Maintaining functionality during adverse conditions.

These objectives are met by implementing the following:

- Segregate the “SCADA/ICS Network” from the "Enterprise Network" and *prevent any communication between them*.
- Move the Common Services to a firewall DMZ where it can be accessed securely.
- Protect the ICS components by adopting Industrial-oriented security controls, as opposed to IT-oriented security controls.
- Eliminate "Single Point of Failure" by implementing redundancy on all critical components.
- To account for security concerns and satisfy the above security objectives can be achieved by the following:

I.	Shifting the location of the planned Firewall deployment from the WAN link Perimeter to the ICS network perimeter. In other words, the firewall should be Positioned between the ""Enterprise Network"" and the "SCADA/ICS Network".
II.	Placing the “Common Services” (Historian, Domain Controller, etc …) on the DMZ arm of the firewall. Common Services are the services which are accessed by both networks; the ""Enterprise Network"" and the ICS Network (see figure 2).
III.	A Windows Domain Controller should be placed on the DMZ arm of the firewall. This Domain Controller should give DNS services and Active Directory services for the SCADA/ICS VLAN. In this scenario, the firewall should be configured to allow access from the SCADA/ICS VLAN to the Domain Controller on the DMZ through The appropriate ports (DNS port and Active Directory ports). In addition, the firewall should allow replication between the Domain Controller on the DMZ and the Domain Controller on the “Enterprise Network” through the Appropriate ports as well. Note that by doing this, the need for any communication between the SCADA/ICS Network and the Enterprise Network is Omitted.
IV.	Deploying Industrial Micro-firewalls to protect the ICS components. Industrial firewalls have the capability to understand and deep-inspect industrial protocols

	Such as Modbus and OPC. They can also block writing to certain Memory Addresses in the PLC to protect it from having its firmware overwritten (see Figure 2).
V.	Firewall configuration should abide by the security rule of thumb of "giving the least privilege"
VI.	A rule of "No Inter-VLAN Communication" should be established and never violated.
VII	For communications between the SCADA/ICS Networks in the different plants and the SCADA control rooms in the Head Office and Exit 10, a Firewall-to-Firewall VPN should be configured. This will ensure the Integrity and Confidentiality of the data sent from the local SCADA (in different plants) to the Central SCADA control rooms.

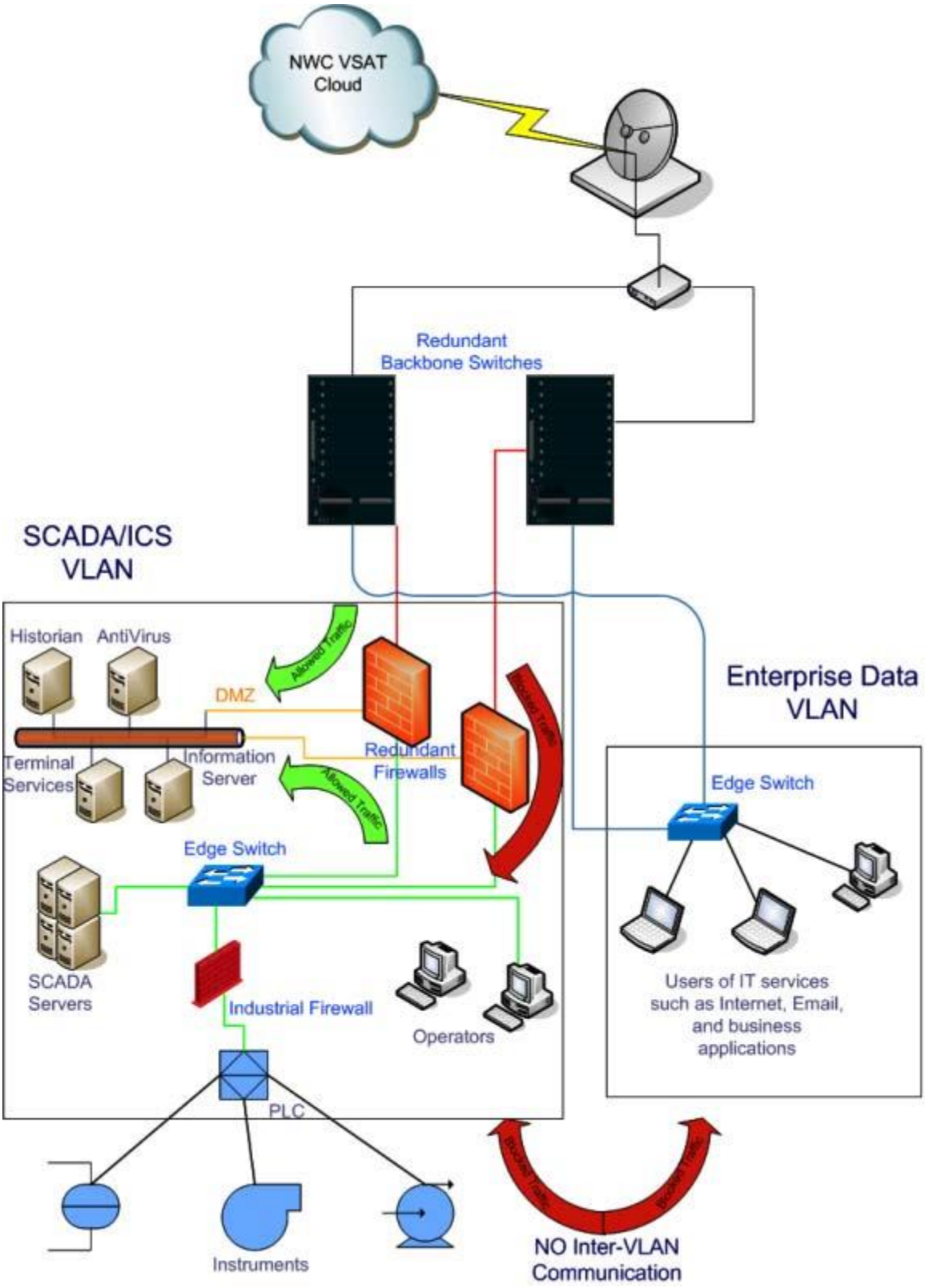

NWC VSAT Cloud
Redundant Backbone Switches
SCADA/ICS VLAN
Historian
AntiVirus
DMZ
Allowed Traffic
Terminal Services
Information Server
Allowed Traffic
Redundant Firewalls
Edge Switch
SCADA Servers
Industrial Firewall
Operators
PLC
Instruments
Enterprise Data VLAN
Edge Switch
Users of IT services such as Internet, Email, and business applications
NO Inter-VLAN Communication

Figure 2

- **SCADA/ICS Components Architecture and Data Flow Analysis:** all SCADA/ICS communication is confined within the SCADA/ICS VLAN with two exceptions. These two exceptions are the Historian server and the Information server. Both servers need to be accessed by users on the "SCADA/ICS Network" and users on the "Enterprise Network". To satisfy this requirement without violating the rule of "NO Inter-VLAN Communication"**,** both servers should be located on the DMZ arm of the firewall as shown in figure 2 above.

13.6 Technical Security Controls:

The objective of this type of controls is to electronically Protect & Detect using Defense-in-Depth strategy/approach. Defense-in-Depth is multiple layers of defense distributed, in series, throughout the network to avoid single points of failure. These layers include:

- Next Generation Firewalls UTM with "Intrusion Detection" capabilities: these firewalls have an advantage over traditional IT firewalls as they are capable of Deep Packet Inspection of key SCADA and ICS protocols such as Modbus and OPC classic. They can also provide fine grained controls of allowed commands issued to PLCs (controlling units).
- Restricted Remote Access: any access to be done remotely should be done through one single entry point. This entry point should have the appropriate security features such as authentication, authorization, auditing, and encryption enabled. All other entry points, such as modems and others, should be removed.
- Implement Device and Application Control: on all SCADA servers and workstations. This feature will disable removable media interfaces (CD-ROM, USB flash drives, and USB storage devices) and prohibit illegitimate applications from running or being installed. SCADA Admins should uninstall any applications that are not relevant or related to SCADA system.
- Anti-virus solution: A unified enterprise antivirus solution should be installed on the DMZ perimeter network along with UTM firewall to server the ICS network.
- System Hardening:
    - Remove or disable unused services in the operating systems and applications to prevent unauthorized use.
    - Ensure all inbuilt system security features are enabled.

- Ensure all SCADA-related servers and Controllers have the latest patches/fixes installed.

- Host-based Intrusion Detection System (HIDS): should be installed on all critical SCADA servers to detect and block any intrusion attempts.
- Internet Browsers and corporate applications including E-mail: should be uninstalled and their usage prohibited on all SCADA servers and workstations.
- Port Security, also called MAC address locking, is one method to secure the physical connection at the end of each port on a network switch.
- SCADA security features, which come as part of the SCADA software solution, should be implemented and fully utilized. In other words, only necessary access rights should be given to engineers and operators depending on their roles and responsibilities.

13.7 Procedural Security Controls:

- Personnel security: Ensure all staff with operational or administration access to process control systems are appropriately screened.
- Physical Access Control and Environmental Protection: Restrict physical access to Control Rooms by implementing a solution that requires a badge and a PIN number. Address environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection)
- Operational maintenance: logging files should be periodically checked and the reviewer should sign off that the action was performed.
- Change Control/Management: a Change Management process should be in place to control any changes related to SCADA components.
- Incident response: Establish processes and procedures to monitor, assess, and initiate responses to security alerts and incidents.
- "Vulnerability Check" and "Penetration Test": should be run periodically to discover any newly introduced security breaches/flaws.
- Awareness and training: ensure that all personnel have the appropriate knowledge and skills required to fulfill their role without compromising security.

13.8 Managerial Security Controls:

- Strategy and planning; should be aligned with business strategy and objectives.

- Establish ongoing governance and risk management process: recommended to adopt the risk management methodology being used at the corporate level.
- Establish reporting and communication channels: that support SCADA security governance activities
- Establish and maintain SCADA security policies; these policies should be updated, documented, and communicated to the users.
- Ensure the development of procedures and guidelines that support information security policies.
- Manage third party risk; ensure that all security risks from vendors, support organizations and other third parties are managed.
- Engage projects; ensure that all projects and initiatives that may impact the process control systems are identified early in their life cycle and include appropriate security measures in their design and specification.

13.9 SCADA application System Security

All security settings to the system will be defined and configured within the Wonderware Application Server. It will
Control the access and control of various components of the runtime environment.

13.10 Credentials Validation

When a user logs on for the first time, security credentials are checked and verified at the GR level. After the login is validated, a cache is created on the local machine form which the login was initiated. Later logins via the same credential will no longer need to be validated on the GR level. Each user then has specific permissions to interact with the system (operator, administrator, etc.) on any node.

13.11 Security Matrix

The Runtime security provided by Application Server is not only restricted to control access to user Interfaces; it also controls access to attributes/tags and the data they represent.

The security schema is a three-level configuration model to create and maintain the following:

- Users associated with specific roles
- User roles associated with specific system administration, configuration and run-time
- (Operational) permissions, which map to security groups
- Security groups associated with specific running components in the system

The following security matrix illustrates how this security will be applied. It defines a cascading model of users associated with specific roles that are associated with specific security groups containing specific components.

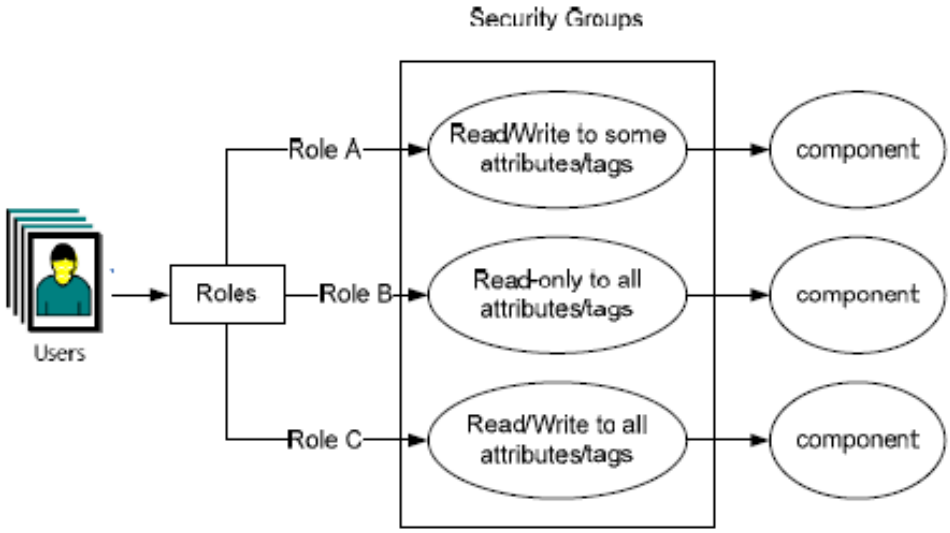


Illustration of Security Matrix

13.11.1 Security Groups

These security groups will group different components of the system that have similar permissions together. They are then mapped to roles. Permissions determine what kind of access users have for each attribute/tag of the components. There are two basic operational permissions:

- Acknowledge alarms
- Change the value of attributes

Following NWC SCADA System Architecture, the attributes/tags should be classified as follows:

- Plant (Local Operation) attributes/tags group (group for each plant) that can be accessed by local users and central SCADA following their Roles.
- Network Elements attributes/tags group that can only access by central SCADA users and following their Roles.

13.11.2 Roles

The roles will reflect the general and operational permissions for group of users on the used SCADA system. There should be four roles:

- Administrator: Users having this role should have – HQ Administrator:
    - General permissions related to application configuration and administration tasks
    - Operational permissions related to the security settings
    - Develop new components and Modify existing properties
    - Deployment of developed screens into production
    - All other possible permissions listed below
- Configuration: Users having this role should have – Central SCADA Administrator:
    - Permission to configure the attribute's value.
    - Discrete Device input.
    - Permission to add new screen, components - replicated, etc…
    - Operational permissions to tune attributes/tags in the run-time environment. Examples
- of tuning are attributes that adjust alarm set points
- Exploitation: Users having this role should have:
    - The ability to run commands and change analog values

- Access to diagnostic display, communication diagnostics, and system alarms in runtime
- Operational permissions to do certain normal tasks like changing set point, output and control mode for a PID object, or commanding a Discrete Device.
- Manually acknowledge an alarm in the run-time environment.

- Visualization only: Users having this role should have:
  - Only visualization and monitor the plant and navigate through it.

13.11.3 Users

Users represent personals that interact with the system and have certain roles as described in section above. Automatic logout on max time elapsed or inactivity on the keyboard and mouse should be available for the users have high access level – to be agreed with Business, complete logout or reduction access rights to the minimum level (visualization only).

CHAPTER-14

14. Deviation from Standards

Deviations from the requirements of this STANDARDS document are not permitted without a written waiver formally authorized by the Document Owner.

15. Risk Recovery Plan Implementation

Create and implement a recovery plan for either a complete or partial failure occurrence of all levels of SCADA system, including recommendations, disaster sources identifications, programs backups and data restoration. In addition, all documentations (SAT, FAT, Control philosophy, O&M …), licenses and as built drawings should be delivered to NWC.

Contractor should Fulfill the recovery plan as per approved Client criteria if Complete or partial damages to the system

- Contractor should provide the complete recovery methods & Procedure which enables to reproduce the System back to work Normal. Time period has to be subjected to approval of the owner requirements.
- Contractor should have to Provide/ Reproduce the complete system including the following
    a) Supply and installation of damaged parts
    b) Complete Laying and Termination of system as per previously approved IO List.
    c) Programming for the required controller parts.
    d) Testing & Commissioning of the required system
    e) Integration of required system to the central Control system
    f) Updated Backup for the Database with renewal of connection.
- Contractor should have to Provide/ Reproduce the complete documentation including the following
    a) As Built Drawings
    b) Complete Updated IO List
    c) Updated Program Backup for the controller system which should be recover with the last updated version of software
    d) Updated Application Backup for the SCADA System.
    e) Updated Backup for the Database

16. Consultation and Execution

- Diagnose a specific problem and analysis the need to choice and design specific solutions suitable for the current situation with the implementation of this standard, then delivered it to the consultant for review, edit and approve.
- Depending on the specs in this document should approve the martial
- Contractor should submit the proper planned schedule for the execution of work and subjected to prior approval. it should include the following required data specifically
    a) All activities for the Project, Specifically confirms the Duration of each activities.
    b) Important Milestone covering the project during the project duration.
    c) Work Breakdown Structure for the complete Project.
    d) Complete organizational chart and the Resource usage for each WBS
    e) Progress update at each milestones or as required as per condition.

17. Suggestions for improvement

Employee contribution to the effectiveness of the way NWC conducts its business is welcomed. Any employee of NWC may suggest changes / revisions to this document by completing a Request for Improvement form.

18. Reference

Ref.Document No.	Title
1	OIML R49-2/ Water meters intended for the metering of cold potable water and hot water/
2	Sea Water Desalination Code- ECRA 2011
3	ISO 4064-1:2014 & ISO 4064-5:2014 / Water meters for cold potable water and hot water / Metrological, Technical & Installation requirements.
4	IEC 61010-1/ Safety requirements for electrical equipment for measurement, control, and laboratory use

5	OSP fiber optics civil works guide, The Fiber Optic Association, Inc.
6	technical Standards for Outside Plant (OSP) Installations

Appendix A

1. Cooling towers

Online measurements	1	Temperature
	2	Flow meter / global
	3	vibration / motor
Online Quality Analysers	1	pH
	2	Chlorine
	3	Conductivity
	4	Turbidity

Control loop	1	Fan	A	Auto fan speed / w outlet temperature
	2	Inlet valve	A	As per a set point
			B	Fully open / close

Trends	1	Temp in / out		
	2	Global flow in / out		

Protection System	1	Fan motor vibration	A	vibration limits

Alarming	1	fan motor vibration	A	User defined
	2	outlet temp	A	User defined
	3	inlet flow	A	User defined

Reports	1	online measurements	A	temp in / out
			B	global flow , accumulative global flow in / out
	2	fan	A	Running hrs

2. Softeners

Online measurements	1	Individual Flow meter
	2	Flow meter / global

	3	Dislodging Flow meter / global
	4	distribution chamber level meter

Control loop	1	Mixer	A	As per a set point
	2	Sludge valve	A	As per a set point
			B	Open , Close / w inlet flow

Trends	1	Inlet / outlet global flow
	2	softener individual inlet flow
	3	sludge global flow
	4	distribution chamber level

Protection System	1	distribution chamber level	A	maximum level

Alarming	1	distribution chamber level	A	maximum level
	2	Mixer	A	off

Reports	1	Inlet / outlet flow	A	global flow , accumulative global flow
	2	softener individual inlet flow	B	flow , accumulative global flow in / out
	3	sludge global flow	A	global flow , accumulative global flow

3. Sand Filters

Online Measurements & Analysers.	1	pH meter
	2	Turbidity meter , inlet global
	3	Turbidity meter , outlet each filter
	4	Backwash feed tank level
	5	backwash waste tank level
	6	sand filter water level , each part / each filter
	7	Sand filters Feed chamber level

Control loop	1	Feed pH	A	auto / w acid system
	2	Backwash feed tank level	A	as per level set point
	3	backwash waste tank level	A	as per level set point
	4	Outlet valve , each filter	A	as per filter water level set point

Trends	1	Feed pH
	2	Feed turbidity
	3	Outlet turbidity , each filter

	4	Backwash feed tank level
	5	backwash waste tank level

Protection System	1	Sand filters Feed chamber over flow	A	by level , opening outlet valve for filters
	2	backwash waste tank over flow	A	by level , stopping backwash pump
	3	filter over flow	A	by level , opening filter outlet valve

Alarming	1	pH value low and high	A	low 6.5 , high 7.5
	2	Outlet turbidity , each filter	A	maximum 1.0
	3	sand filters feed chamber level	A	maximum level
	4	backwash waste tank level	A	maximum level
	5	filter water level	A	maximum level

Reports	1	feed pH	A	pH in
	2	feed turbidity	A	global in
	3	Outlet turbidity , each filter	A	outlet each filter

4. Reverse Osmosis

Online analysers.	1	Feed Temperature
	2	Feed pH
	3	Feed ORP
	4	Feed SDI
	5	Feed Pressure
	6	Feed tank level
	7	Feed TDS
	8	Feed IRON
	9	Feed Flow
	10	stage product TDS / each stage
	11	stage product pressure / each stage
	12	stage product flow meter each stage
	13	stage Reject TDS / each stage
	14	stage Reject pressure each
	15	stage Reject flow meter / each stage
	16	stage DP / each stage

	17	block global Product flow / each block
	18	micro filter DP , global
	19	H.P.P temp / each
	20	H.P.P vibration / each

Control loop	1	Feed pH	A	set point / w acid system & no. of lines
	2	Reject pH	A	set point / w acid system & no. of lines
	3	Feed ORP	A	set point / w SBS system & no. of lines
	4	Feed Pressure	A	set point / w regulating valve
	5	Anti scalant Pump speed	A	set point / w anti system & no. of lines

Trends	1	Feed Temperature
	2	Feed pH
	3	Reject pH
	4	Feed ORP
	5	Feed SDI
	6	Feed Pressure
	7	Feed tank level
	8	Feed TDS
	9	Feed IRON
	10	Feed Flow
	11	normalized flow / each stage
	12	normalized flow / each block
	13	normalized product tds / each stage
	14	normalized reject tds / each stage
	15	normalized DP / each stage

Protection System	1	feed pH , low or high	A	pH value measurement , stop RO plant
	2	feed TDS high ,	A	TDS value , stop RO plant
	3	feed Iron , High	A	Iron value measurement , stop RO plant
	4	Feed Pressure , low or high	A	Pressure Value measurement , stop RO plant
	5	Feed Temperature , High	A	Temp. Value measurement , stop RO plant
	6	Feed ORP , low Or high	A	ORP Value measurement , stop RO plant

Alarming	1	Feed Temperature	A	MAX= 40
	2	Feed pH	A	low = 6 , max 6.5
	3	Feed ORP	A	low = 0.0 max = 325 mV
	4	Feed SDI	A	max =3.0
	5	Feed Pressure	A	as per the design
	6	Feed tank level	A	Minimum to run the LPP. Plant design
	7	Feed TDS	A	as per the design and membrane projection (2500 ppm)
	8	Feed IRON	A	max= 0.05 ppm
	9	Feed Flow	A	if less than the design (product + Reject)
	10	normalized flow / each stage	A	if 10% less than a set point
	11	normalized flow / each block	A	if 10% less than a set point
	12	normalized product tds / each stage	A	if 15% more than a set point
	13	normalized reject tds / each stage	A	if 15% more than a set point
	14	normalized DP / each stage	A	if 15% more than a set point
	15	micro filter DP	A	DP max= 1.0

Reports	1	Feed Temperature	A	global
	2	Feed pH	A	global
	3	Feed ORP	A	global
	4	Feed SDI	A	global
	5	Feed Pressure	A	global
	6	Feed tank level	A	global
	7	Feed TDS	A	global
	8	Feed IRON	A	global
	9	Feed Flow	A	global
	10	normalized flow / each stage	A	individual
	11	normalized flow / each block	A	individual
	12	normalized product tds / each stage	A	individual
	13	normalized reject tds / each stage	A	individual
	14	normalized DP / each stage	A	individual
	15	running Hrs for HPP	A	each HPP

Appendix B

Instrument List for Waste water Treatment Plant as per different applications

Analytical Measurement

1.1 Total Chlorine Residual
1.2 Dissolved Oxygen Meters
1.3 pH
1.4 Suspended Solids

Flow Measurement, Closed Conduit Liquid Flow

2.1 Magnetic Flow Meters
2.2 Sonic Flow Meters
2.3 Turbine Flow Meters
2.4 Venturi Tubes and Flow Tubes

Flow Measurement, Closed Conduit Gas Flow

3.1 Orifice Plate
3.2 Venturi Tubes and Flow Tubes
3.3 Averaging Pitot Tubes
3.4 Turbine Flow Meters

Flow Measurement, Open Channel
4.1 Kennison Nozzle
4.2 Palmer-Bowlus Flume
4.3 Parshould Flume
4.4 Weir

Level Measurement
5.1 Bubbler Level Measurement
5.2 Capacitance Probe
5.3 Float Level Instruments
5.4 Sonic and Ultrasonic Level Sensors

Pressure Measurement

6:1 Pressure Cells
6.2 Differential Pressure

Performance Testing
7.1 Flow