snowy hydro Limited renewable energy	
Snowy Technical Standards	
SHL-ELE-156 (G)	***Annexure G - Control Systems General Low Voltage Electrical Requirements***
Subject Matter Expert *Kapila Nanayakkara* *Principal Electrical Engineer*	Version Date: 1 January 2017 Revision: *Original*

This annexure forms part of the General Low Voltage Electrical Requirements Standard (SHL-ELE-156).

1. Scope

This Annexure sets out the requirements for Control Systems.

Control Systems must be designed and constructed conforming to the General Electrical Requirements and this Annexure.

1.1. Applicable Standards

The design, manufacture and testing of equipment and components detailed in this annexure must comply with the requirements of all relevant Australian Standards or in the absence of appropriate Australian Standards, with relevant IEC, ISO or International Standard, together with the requirements of competent authorities having jurisdiction over all or part of the manufacture, installation or operation of the equipment, except where modified by this specification.

All works must comply with the requirements of the most recent releases of the regulations and standards noted in Snowy Standard SHL-ELE-156. In the event of a conflict between different Codes, Standards or Regulations, the highest requirement must apply.

2. Safety Requirements

Control Systems must be designed, manufactured and tested with the safety requirements detailed in the General Electrical Requirements (SHL-ELE-156).

3. Technical Requirements

3.1. Design

3.1.1. System Integrity

The design of the control system must consider the following key requirements:

- No single fault will cause the complete failure of the control system.
- No single failure of any system equipment or power source will interrupt or disrupt any system function.
- No communication links failure will render forced outage of the whole plant.
- For redundancy provisions of equipment, no single fault within the control system can cause the failure of the duty equipment and at the same time cause the standby plant to be unavailable.
- No failure within the system or wiring will impose an earth path for any power source.
- Alarms and trips will remain active in manual and automatic modes.

The control system must incorporate comprehensive self-checking facilities and adequate test facilities so that,

internal faults can be detected within the control system and provide alarms prior to any resulting disturbance to the process. All alarms must be displayed at the local HMI and at the remote control centre.

3.1.2. System failure modes

The control system must be designed to react in a predictable manner to certain system failures. Examples of system failures and the corresponding control system reaction are outlined below:

- Logic processing failure (as detected by system diagnostics) - the controller will transfer to its backup. If the backup does not exist, or is unavailable, the controller outputs will be set to a known state and enable any manual shutdown facilities to provide orderly shutdown of equipment. Generally outputs will de-energise on the failure of the controllers
- Controller or IO power supply failure - the controller will transfer to its backup. If the backup does not exist, or is unavailable, the controller outputs will de-energise.
- Controlled device power supply failure (i.e. motor supply failure) – the controller will command any backup equipment to start without waiting for any process deterioration. The failed device will either be commanded to restart upon power resumption or remain in a shutdown state should a backup device be operating.
- Communications failure to a controlled device (i.e. motor) – should the controlled device be critical to prevent any process deterioration, a communications failure will cause the controlled device to operate.

Note any such system failure modes and the resulting reaction must not affect the plant protection system and will ensure a high level of plant reliability.

3.1.3. Plant process safety

Where required, either due to legislative requirements or as a means of managing plant process risk, a process protection system must be completely segregated from the control system.

3.1.4. Field device design

Each field device must be wired to a dedicated input or output on the control system.

Field devices, which, for reasons of safety must be wired in series and connected directly into a motor, stop circuit (e.g. safety rope switches), must have an electrically separate contact wired to the control system to provide status and alarm indication.

3.1.5. Application and Programming Software

The application programs must be developed using efficient, logical and proven sub routines and be clearly and extensively documented (i.e. tag descriptions and logic comments) to allow easy understanding and fault finding. The use of standard library functions or standard logic sequences is preferred.

Sequence logic must have the following features

- The correct position of all plant devices must be checked and verified rather than inferred before a sequence can be executed by the operator or the sequential control system. The desired condition versus the actual condition of all monitored devices must be checked continuously.
- The failure of any equipment or the loss of power supply to that equipment must be supervised to raise an alarm. It is important that, on power supply or equipment failure, the equipment is designed to fail to a reliable state and so avoid disturbance to the operation of any other equipment
- All sequences must flow smoothly with a minimum of delay and abnormal conditions must be quickly detected and responded to. A sequence must be terminated if it cannot proceed because of control or

safety interlocks and an automatic stop must be initiated. Indication and test facilities must be provided to allow the rapid location and repair of faults

3.1.6. Diagnostics design

The control system must be programmed and/or constructed to enable simple unambiguous trouble-shooting and fault finding.

The operator must be able to access, via the local HMI, the status of all plant devices at any time.

3.1.7. Interface design

The control system must have the ability to transfer and receive data and commands from other controllers, IEDs and remote control centres.

The interface must be designed to robust, with the appropriate error checking on all signals. Watchdog timers must be implemented to detect communication failures and raise an appropriate alarm. Where commands are transmitted to a controller, an appropriate feedback or acknowledgement signal must be transmitted to the device issuing the commands.

3.1.8. Human machine interface (HMI)

The local HMI must provide comprehensive control and monitoring for all related plant with capability to operate down to individual drives and valves in the field.

The HMI control faceplates must provide a control release (action and execute) interlocked with all non-modulating control, to prevent accidental HMI control changes without reducing the operator's ability to make immediate control changes when necessary

3.1.9. Display Functions

The following display functions are required as a minimum:

Table G2.2 Standards

Display	**Functionality**
Alarm displays	Refer to alarm management section for various display types
Mimic diagram	A symbolic, schematic representation of the plant or process. All plant must be represented on these displays.
Real time trend	A continuous line representation of the current value or binary status of a point against time (X/T). All analogue inputs (discrete or serial) must be assigned to predefined trend groups which can only be modified in the engineering environment.
Historical trend	A continuous line representation of the value or binary status of a point that includes data which has been retrieved from historical storage. Historical trending must be integrated into the real time trend display functionality. From the latter display, by defining time periods of data which has been historised , historical trending is realised.
Operator definable trend	A real time trend that is configurable by the operator. At least ten operator definable trend groups must also be provided.

Faceplate display	Pop up control windows for each indicator, drive, sequencer, controller, setpoint, bias, drive, duty standby, and selector. Control actions initiated by the operator must be immediate. The feedback must be arranged to eliminate overshooting the target when adjusting set points and positioning actuators. It must be possible to select “maintenance mode” for each drive from its respective faceplate.
Faceplate detail	The status and variable conditions of signals related to the associated faceplate.
Sequence step	Dynamic graphic display of sequences, action steps and transition criteria able to be traced to the process condition.
Sequence guide	Dynamic graphic display of sequence guidance information as follows ● What sequence step action is being carried out by the sequence ● Every sequence that is active at any time ● Timeout on a sequence step action. The Operator can then go to the sequence display to determine the hold-up condition. ● Prompt operator control actions (where no automation is provided) as part of a sequence ● This may include the plant startup and plant shutdown sequences
Plant co-ordination displays	Selection and indication for plant modes of operation (i.e. generator, synchronous condenser, overload). The display is also to include automatic generation control functions, and plant capability limit functions, plant load and load rate.
Process Displays	Operational information, such as start up and on line operation, rather than physical plant layout.
Standby Plant	Standby availability of redundant motor drives and standby plant sequences consolidated in one display across multiple plant areas.
Controller logic dynamic display	From the controller window display and the detail display the operator must be able select a controller logic graphic dynamic display indicating all status which impacts on the operation (e.g. start/open permissives, protection commands, auto commands, drive status, limit switch antivalence, over torque, status discrepancy, runtime exceeded, position, etc.). It also includes the regulating control logic associated with the P&ID controllers, and other analogue functions.
First Up Protection Trip Displays	Displays for each major motor drive and plant protection trip system (e.g. turbine, generator, dual fired boiler, solar thermal steam generator) which show a list of trip cause flags for each trip system, to quickly ascertain the “first up” cause of trip.
Large Screen Displays	A collection of salient / key plant status and process data that provide an effective overview of total plant operational status primarily for use on a large screen display.
System Status	To monitor and verify the condition and operation of all parts of the control system. All system monitoring information must be shown on the system graphical displays with a top down hierarchy such that the location of failed modules (cards) can be identified with a room, cubicle, and rack and slot number.

Each HMI display must have continuously updating date and time.

The displays must be organised into a hierarchy, with plant overview displays at the top of the hierarchy then the plant area level, the plant group level, and the individual equipment level must provide increasing detail.

The displays must use a SHL approved colour palette and the colour palette must be applied consistently across all displays. A minimalistic approach to the graphics must be undertaken, with unnecessary details avoided to maximise operator understanding and situational awareness.

All displays must include active links to display other associated displays.

3.1.10. Historical data storage

A historical data storage system must provide an historical record of all value and status changes.

Analogue (including calculations), alarm state and binary state changes (including SOE's) must be recorded in the historical data storage. The current value, the time and date stamp, and point quality must be stored when the alarm and binary points change state and when analogue values change by more than the exception band. Analogue points must also be stored on the basis of time expired since the last stored value. Exception band settings must be set appropriately to ensure adequate resolution of the signal, with the particular process speed taken into account in the selection of the exception band.

The historical data storage must provide the capacity to store on hard disk, the previous 5 years of continuous (worst case) data collections for ready retrieval. The transfer of data from on line to archival storage must be automatic when the archival medium is available. Notification to the operator must be provided when the archival media requires changing. Retrieval of historical data must be by historical displays, trends, reports, and electronic export in Microsoft Office compatible format.

3.1.11. Alarm management

The configuration of the alarm system must be undertaken in accordance with SHL's alarm standard. Process alarm levels must be approved by the relevant asset owner.

Alarm disable facility (maintenance facility)

Password protected functionality must be provided for the operator to disable an alarm condition. Such a requirement is usually associated with toggling alarms caused by malfunctioning field devices, which prevent the effective use of the alarm screen display. An "alarm disabled" display must be provided, which must list alarms which have been disabled. The operator must be able to reset the disable condition from the alarm disable display using the password.

Maintenance switch

The HMI must be provided with a 'maintenance switch' functionality to allow for the suppression of alarms to the remote control centre. Critical alarms, such as fire alarms, must still be transmitted to the remote control centre regardless of the state of the 'maintenance switch'.

Alarms must still be annunciated on the local HMI regardless of the state of the 'maintenance switch'.

Note that an operational unit must be prevented from operating in Automatic Generation Control mode or from being remotely started when the 'maintenance switch' is enabled. This does not prevent an operational unit

from being controlled locally.

First up system

A “First Up” alarm system must be provided to quickly identify the initial cause of trips.

First Up alarms must be captured such that the initial cause of a major plant equipment (e.g. bearing temperature high, oil pressure low) trip is clearly identified to the operator on the HMI alarm display and first up display. The logic must function on the basis that once the initial cause of the trip is captured, subsequent trip causes (and associated alarms) that are activated as a result of the trip must be blocked.

The processing cycle time for first-up alarm logic must be configured to allow discrimination of the first and subsequent alarms.

System monitoring

All control system hardware and software must provide comprehensive on-line diagnostics and fault monitoring which must be alarmed to the local HMI and remote control centre.

System alarms must have their own alarm priority class, but must have the same functionality as process alarms.

System monitoring must include Processors, Communications, I/O cards, Power supplies, Circuit Breakers and Cubicle temperature (for cubicles containing active components).

Where redundant equipment is provided, each item must be monitored and alarmed, and the status (e.g. failed, ready, slave, master) must be provided to the operator.

Continuous diagnostics must be provided for all communication paths.

Alarm display

A local alarm display must be provided to display current alarms and past alarms sorted by priority, plant area and time/date.

Alarms must be displayed using a single alarm page with each alarm message on a single line. Additional alarms must be available by paging the display.

The alarm message must provide at least the following information and the location of each field in the message must be configurable.

Table Error! No text of specified style in document..3 Alarm fields

Field	Description
Priority	A unique and consistent coding and colour scheme must be provided to identify each alarm priority.
Time	The time field must indicate the time of day at which the point is first detected to be in alarm. It must show hours, minutes, seconds, milli seconds in 24 hr format, with a resolution of at least one millisecond.
Tag no.	The tag number of alarm or associated device must be provided.
Description	The full description of the alarm must be provided.

Process Value	The dynamically updating value of an analogue value in alarm must be provided.
Plant	The plant area must be provided.
Alarm State	The actual analogue alarm limit value (e.g. >330'C) and the binary alarm state (HI) must be provided. If the actual analogue alarm limit value is a calculated value the analogue alarm limit value must dynamically update.

The first alarm line must be displayed at the top of the screen and subsequent alarms must be displayed below the previous alarm. The alarm screen must not scroll without operator acknowledgement.

Where possible, each alarm displayed must be provided with an active link to display an associated process display and alarm response display.

Alarm annunciation

Detection of an alarm must trigger audible annunciation using a speaker. A silence function must be provided to silence the audible annunciation.

Visual annunciation must consist of displaying the individual alarm in the alarm display with a flashing indicator to identify the unacknowledged state of the alarm.

An acknowledge function must be provided to acknowledge recognition of all currently displayed alarm states.

A clear function must be provided to remove all acknowledged returned to normal alarms on the alarm page.

Alarm response display system

Where possible an alarm response display system, activated by selecting an alarm on the alarm display, must be provided as a diagnostic guide to determine the cause of the plant or equipment abnormality initiating an alarm.

Alarm responses must be assigned to individual alarms, or to multiple alarms.

The alarm response system must also provide the functionality to search for the alarm response of any point, not just alarm on the alarm display.

3.1.12. Time synchronisation

Each value/status/event/alarm/SOE must include time of day stamping to 1mS resolution to ensure correct time discrimination of events.

A GPS clock must maintain the local master time reference. The loss and restoration of the time signal must be alarmed. The GPS clock must provide synchronisation to within 10 ms of actual time.

The GPS time synchronisation must be communicated to all embedded PLCs, Protection relays, Intelligent Electronic Devices (IED), SOE's and other devices as appropriate to enable accurate time stamping at the signal source.

3.1.13. Sequence of Events (SoE)

The purpose of an SOE system is to ensure an accurate chronological order of events is recorded to

significantly aid the diagnosis and understanding of events that occur during contingencies. SOE signals typically relate to plant protection initiations and the resulting major plant component status changes.

High speed digital input scanning modules must be provided with an accuracy of time tagging of better than 10 ms of system time. Certain signals and signals sourced from other intelligent devices (e.g. generator protection relay) must be time tagged at the source and be classified as SOE points.

This functionality may be provided by suitably selected electronic protection relays.

3.1.14. Security and protection

The design of the control system and industrial communications networks must consider the requirements of IEC 62443-2 and IEC 62443-3.

Network architecture

To provide isolation from external influences equipment must be grouped together on a common network and protected from other networks. For Internet Protocol (IP) connections a security perimeter must be established around the network by use of a firewall.

The network must be configured in a logical and consistent manner and must ensure security from unauthorised use, modification and configuration changes.

The network must connect to the Snowy Hydro's Business LAN. Where a connection is required outside the network, measures must be taken to ensure the security of the network is not compromised.

The design of the network must include a defence in depth strategy such that multiple layers of security are implemented. The security design must encompass hardware configuration, software configuration, hardware and software security policies, operation and maintenance policies and procedures (including incident response) and end-user policies and procedures.

Hardware security

Disk drives (hard disk drives, CD/DVD drives, USB drives etc.) must have restricted access. Equipment with disk drives and network equipment must be locked in cubicles with a transparent front door, accessible only by the system administrator.

Security against malicious or inadvertent introduction of external data must be provided.

Firewall

A firewall must be provided and configured to control connections between devices inside and outside the firewall. Firewall rules must be implemented to allow or restrict traffic to specific devices and applications.

The firewall must provide a Demilitarised Zone (DMZ) between the Snowy Hydro's business network and the control systems network.

Software security

Virus/spyware protection software must be provided for the operating systems.

The protection software must be configured and up to date with the latest updates.

Procedures and policies for updating the protection software must be included in Network Administration

Documentation and must be software-automated as much as possible. The procedures and policies for updating the protection software must mitigate the risk of security and reliability threats during and after update.

User authentication

Users must login by username and password or by other secure access devices.

Unique security must be provided for each HMI, user and plant area.

The three access modes must be available; Monitor (view only), Control (Operator), Engineering (Administration/configuration/maintenance).

Separate user names and passwords must be provided for each type of user.

- engineering/Technician (Full access rights)
- operator (Limited access rights)
- view Only (View only access rights).

3.2. Relay systems

Control systems which use electromechanical relays must utilise conventional heavy duty control devices.

3.3. Solid-state systems

All solid state equipment must be built up from proven modules and components.

Control systems of the solid-state type must consist of withdrawable plug in modules mounted on standard width racks. Modules performing identical functions must be interchangeable.

3.4. Control electronics

3.4.1. General

All electronic components must be of standard manufacture and of the best industrial quality. The type, rating and precision of the individual electronic components must be such as to ensure accurate and reliable operations. Components must not operate at more than two thirds of their stated rating.

The control system must be provided with hardware diagnostic facilities. Location of the hardware faults, trips and overloads must be shown on status lamps or other indicators for each type of fault monitored. Also the system must have on-line self-checking routines; all malfunctions are to be indicated at the operator interface.

Failure of any diagnostic check which affects the integrity of the system must result in the automatic change over to stand by equipment where provided. This must include back-up controllers, power supplies and data communication equipment as appropriate.

The continuous diagnostic routines must be able to identify faults down to the card level. Hardware associated with each I/O point must be checked and any fault detected must be reported at the local HMI and at the remote control centre. Any failure of diagnostic check routines must also be reported at the local HMI and at the remote control centre.

The control system must be composed of standard products (hardware, systems software and firmware, etc). All hardware, system software and system firmware supplied for a control system must have been field proven, be

expandable and based on ‘Open’ architecture and must comply with all relevant standards and regulations.

The controller must provide all the control and supervisory functions and separate equipment must be provided for electrical protection, AVR and synchronising. Turbine governor functions must be separate from the PLC.

All electronics and interconnections must be immune or suitably screened to prevent electrostatic and electromagnetic interference caused by power cable surges, radio transmission or other sources encountered in industrial plant.

Equipment must be arranged to have all components easily accessible without it being necessary to dismantle or to remove other components in order to remove a faulty component.

All fixed and moving contacts carrying electronic signals such as switches, non-hermetically sealed relays, plugs and sockets, printed circuit contacts and edge connectors must be gold flashed to minimum thickness of 1 micrometer at the rating surface.

Electronic equipment must where possible be in sealed cabinets.

3.4.2. Power supplies

All power transformers must comply with AS 60076. All power supplies with DC output must comply with AS 61204.1. All bulk DC power supplied must be backed by another to provide 100% redundancy. The redundant power supply must be connected in tandem such that a failure of one power supply must result in the other power supply assuming full load. All power supply failures must be reported at the HMI. Each power supply must be rated 150% of full load and have its own fusing, regulation failure alarm and status indications.

The power supply units must be adequately cooled. If fan cooling is used then fan life must be at least 10 years.

Power supply units must provide galvanic isolation between input and output

Line conditioning equipment must be provided with the power supply, if noise and/or spikes could affect the equipment supplied.

The AC and/or DC power supplies to cubicles must have circuit breakers mounted within the cubicle for total cubicle isolation. The supply must be clearly labelled as to the equipment which it isolates.

Power supplies within the cubicle must be so designed to prevent inadvertent contact with live metal by personnel, and must be physically separated from all other terminals.

Fault and status circuits and indicators must be continuously supplied.

Separate DC power supplies should be provided for I/O modules and control instrument equipment.

3.4.3. Signal types

General

IO Module must meet the following requirements:

- Withstand a common mode voltage of 265 V AC and 375 V DC and must have 1000V galvanic isolation.
- Have power supply fuses and blown fuse indication. With this and other input conditions displayed on LEDs on the front of the module.
- Be connected to terminals in a separate termination cubicle. The terminals may be in the bottom of the associated cubicle, where less than 100 I/O points are terminated in a room.

- Inputs must be configured with adjustable sensor checking which must be applied such that invalid sensor values are not presented to an operator, however bad quality must be notified.
- The printed circuit cards must be assembled in frames, which when mounted in racks or cubicles must give full clear front and rear access to the cards and their connectors. Where it is necessary to mount equipment at the rear of card frames, the mounting must be arranged on hinges to facilitate access to the card frames and wiring.
- Card frames must be equipped with locking devices to prevent the unplugging of boards due to vibration or accidental disturbances.
- Withdrawable cards, modules and cable plugs must be keyed, coded or otherwise marked to ensure there is no possibility of replacement in the wrong position.
- If test points are required for calibration of the card's functions, then such test points must be available on the front edge of the card.
- Any adjustable devices required for card calibration must be accessible without removing the card from the card frame.
- All cards, modules, cable plugs and card frames must be fitted with an approved interlocking system to prevent damage from replacement in the wrong position. All card frames and cards must have a unique labelling or coding system to identify cards with slots.
- Output circuits must be protected internally against damage due to short or open-circuits in the output wiring, and voltage spikes due to inductive loads.
- All static sensitive cards must have a warning label to this effect.
- Plugs and sockets where used must conform to DIN 41612 and cards must be equipped with an effective locking device. Reliance on the friction of the contact pins is not acceptable.
- All cards must be either removable or replaceable with power applied without damage. To this end, connectors must include extended pins for the common (ground) line and others as necessary.

Analogue Inputs

The analogue input cards and modules must be capable of receiving 4 - 20 mA DC signals. An appropriate +24V dc voltage, current limited source for powering associated two-wire transmitters must be provided either from the analogue input circuitry or from a separate IO power supply.

Analog Inputs must have a normal mode rejection of > 50 dB at 48-52 Hz, and a common mode rejection of > 100 dB at 48-52 Hz with 1 Kohm unbalance.

Analogue I/O must provide a ± 5% over-range capability without loss of accuracy. Signals outside this range must be configured as invalid (bad quality).

Analogue Outputs

Isolated analogue outputs of 4 - 20 mA DC must be provided for the field devices. The controller output directions must be configurable, i.e. direct or reverse acting. The outputs must be short circuit protected.

Thermocouple and RTD

The system must be capable of accepting all standard thermocouples and RTDs. This can be via integral input cards or via signal converters. Where signal converters are utilised, it is preferred that the signal converter communications to the controller be via an appropriate industrial communications protocol to reduce ADC-DAC-ADC conversion errors.

Thermocouple cold junction compensation and open circuit detection must be provided.

Millivolt Inputs

The system must be capable of accepting low level millivolt signals from other devices. This can be via integral input cards or via signal converters. Where signal converters are utilised, it is preferred that the signal converter communications to the controller be via an appropriate industrial communications protocol to reduce ADC-DAC-ADC conversion errors.

Pulse Count Inputs

The system must accept pulse signals from external devices, the total accumulated pulses being available to the control database as a process variable. Pulse count inputs must be 24 V dc internally powered.

Digital Inputs

The system must accept digital (on/off) inputs for process alarm conditions or status. Digital inputs must be 24 V DC and may be internally or externally powered. All inputs must be optically isolated with the change of status reported at the work station and available to logic application programs.

Digital Outputs

Digital outputs must be 24 V DC unless otherwise specified. All outputs must be capable of being:

- momentary pulsed “on”
- off command latched on until an “off” feedback signal is received
- pulsed “on” for a predetermined variable time period.

It must be possible to set the outputs to a predetermined state “on” or “off” on power up or power down. Digital outputs must have short-circuit protection.

3.4.4. Installation

The control system must installed in control cubicles. The control cubicles must be in accordance with Annexure C – Electrical cubicles and Junction Boxes.

Earthing of the control system must be in accordance with Annexure K – Low Voltage Earthing.

3.5. SCADA

SHL utilises a SCADA system to provide remote monitoring and control of sites as well as data collection into a PI Processbook system.

3.6. Engineering access

Engineering access must be provided to allow for the maintenance of the system. This will either take the form of a dedicated workstation or a secure link from the SHL business LAN into the control system LAN.