Secondary Systems Design – Standard

Table of Contents

1. Introduction

1.1 Purpose

Powerlink secondary systems provide the functions of real time monitoring, control and protection for the Queensland high voltage electricity transmission network.

The requirements of the secondary systems are set out under the relevant sections of:

- The regulatory framework established by the Australian Electricity Regulator (AER);
- Specific requirements under the National Electricity Rules (NER) made by Australian Energy Market Commission (AEMC);
- Specific requirements of the Australian Energy Market Operator (AEMO).

Secondary system functions are to be designed to achieve the reliability, availability and security that meets the requirements of the AEMC and AEMO policies and standards, including the National Electricity Rules.

The purpose of this document is to describe the requirements for design and decision making processes for secondary systems to achieve these measures.

There will be instances in some new and existing secondary system designs where designers will not be able to meet all of the specified requirements, and will recommend suitable non-standard solutions based on the specific site constraints and/or customer requirements. These non-standard solutions shall still comply with the relevant standards, codes, regulations and guidelines and will be subjected to the rigorous Safety in Design Process to ensure effective constructability and maintainability in the future. Such non-standard design solutions will be reviewed and agreed upon by Secondary System & Telecommunications Strategies Team or assigned delegates.

1.2 Scope

This document describes the overarching design policy for secondary systems including:-

- Plant and system protection;
- Plant control;
- Plant monitoring;
- Local and remote monitoring and control;
- Wide Area Monitoring, Protection and Control schemes;
- Metering;
- Power system monitoring;
- Secondary system interface with customers;
- Secondary system cyber security;
- Substation infrastructure including air-conditioner control and monitoring, and AC & DC supply control and monitoring;
- Secondary system panel construction;
- Secondary system marshalling kiosks and termination racks;
- Secondary system data management.

Control centre systems such as EMS are not included in this document.

1.3 References

Document code	Document title
AEMO Power System Data Communication Standard	AEMO Power System Data Communications Standard
AESCSF	Australian Energy Sector Cyber Security Framework
IS18:2018 (QGCIO)	QLD Government Information Security Policy
National Electricity Rules	National Electricity Rules

1.4 Defined Terms

Terms	Definition
AC	Alternate Current
AEMC	Australian Energy Market commission
AEMO	Australian Electricity Market Operator
AER	Australian Electricity Regulator
AVR	Automatic Voltage Regulator
CB	Circuit Breaker
COMTRADE	Common format for Transient Data Exchange
DC	Direct Current
DDR	Digital Disturbance Recording
EMS	Energy Management System
FCAS	Frequency Control Ancillary Services
HMI	Human Machine Interface
ICCP	Inter-Control Centre Communications
IED	Intelligent Electronic Device
ITC	Interface Termination Cubicle
NER	National Electricity Rules
NPS	Negative Phase Sequence
OSD	Operations and Service Delivery
PMU	Phasor Measurement Unit
SCADA	Supervisory Control and Data Acquisition
SPAR	Single Pole Auto Reclose
STATCOM	Static Synchronous Compensator
SVC	Static VAR Compensator
TPAR	Three Poles Auto Reclose
WAMPAC	Wide Area Monitoring, Protection and Control
BESS	Battery Energy Storage System

2. Secondary System Design Overview

2.1 Secondary System Functions

The secondary system will be designed to provide the following functionalities:-

- Plant protection and system protection;
- Automatic plant control;
- Manual plant control facilities;
- Plant monitoring;
- Local and remote monitoring and control;
- Remote interrogation for the provision of event data/COMTRADE files for automatic or manual collection;
- Wide-area monitoring, protection and control;
- Power system monitoring;
- DC supplies;
- Interface with customer secondary systems;
- Infrastructure to support secondary system operations;
- Cyber security monitoring and access control facilities.

2.2 Secondary System Reliability and Availability

Secondary systems are comprised of various components that have differing reliability and availability requirements. Protection systems have the highest reliability requirements resulting in duplicated protection schemes as defined in National Electricity Rules Chapter 5 and Protection Design Policy.

Real time monitoring and control has the next highest requirement for reliability and availability as defined in the AEMO Power System Data Communications Standard. A redundant data communication system is required between each substation and Powerlink Control Centre. High availability equipment is essential within the substation to provide the automation function. The system shall be designed so that the impact of failure of one system is limited to one bay.

The third group of equipment is used for condition monitoring and event analysis. This group of equipment does not require duplication or redundancy, however, system architecture and designs shall utilise synergies and opportunities for increasing availability where prudent.

The control system must be designed to the extent that a single failure will not affect more than one CB or control link.

The secondary system shall be designed to facilitate simple fault diagnosis and implemented such that it is easy to maintain and repair. This will result in reduced maintenance and repair times. The automation and monitoring equipment shall also facilitate self-monitoring so that equipment malfunction can be quickly detected and repaired.

Mal-operation of the secondary systems can adversely affect the primary system and consequently affect network performance. To achieve reliable and secure operation, secondary systems shall be designed using good electricity supply industry practice. Design practices shall minimise design errors. Secondary system ergonomics shall be designed to minimise human error incidents.

Secondary systems shall be designed to allow remote diagnosis of an event and facilitate rapid restoration of the primary system. This will aid in the achievement of secondary system reliability targets.

2.3 Whole Life Cycle of Secondary Systems

The initial capital costs for secondary systems assets are a significant portion of the whole life cycle cost. Selection of equipment and designs that are efficient to implement are important in minimising the life cycle asset cost.

Reliability of the secondary systems affects the maintenance costs, and hence the life cycle cost of secondary systems assets. Selection of equipment and designs that are reliable, durable, and easy to install, commission, maintain and repair will be required to optimise the secondary system whole life cycle asset cost.

Customer connections including renewable connections within existing substations should not impact future regulated secondary system replacement considering the establishment of Site Infrastructure Panels and Network Panel within the existing substation control building/telecommunication building.

Obsolete equipment should not be considered in the design phase unless it has been approved by Secondary Systems Strategies Team with proper control measures in place and where newer variants of equipment exist that provide the same functionality these should be considered as the preference.

2.4 Legislation and Compliance Requirements

Secondary systems must comply with appropriate Queensland Acts and Regulations, the National Electricity Rules, the subordinate AEMO Power System Data Communications Standard and relevant Australian Standards.

Compliance with various safety related requirements such as Safety in Design is a high priority.

3. Standard

3.1 Secondary System Design Basic Philosophy

The secondary systems shall be designed in accordance with the following design philosophies:-

- Powerlink Secondary System Design Manual (SSDM) shall be developed to provide detailed design for Secondary System Automation Systems (SAS) based on this standard; Secondary system templates are developed based on SSDM.
- The secondary system shall be modular and arranged in logical, functional circuitry modules such that it allows operation, maintenance and isolation of each module without affecting other modules;
- Powerlink design templates shall be used for all Greenfield and Brownfield projects irrespective of whether the design portion is carried out in-house or outsourced;
- The secondary system functions shall be integrated to minimise the numbers of IEDs and networking devices used in the system. The number of models of IED shall be minimised to reduce training cost and spare part inventories;
- Period contract arrangements with the equipment suppliers shall be organised to minimise the whole of life cycle cost of the equipment. This has flow on benefits for the Change Management, training for the new equipment, and proficiency of the existing equipment;
- Powerlink Standard alarm lists must be used while designing alarm functions, grouping alarms or deriving alarm summaries;
- Remote interrogation on secondary systems equipment shall be provided;
- Wide Area Monitoring, Protection and Control (WAMPAC) schemes shall be implemented via diverse means (including EMS, local control of substations, distributed control and customer schemes) to ensure their reliability and security;
- The secondary systems shall be compliant with International Standards and Australian Standards.

3.2 Plant and System Protection

3.2.1 Plant Protection

The secondary system shall provide infrastructure for protection systems required by, Protection Design Standard.

3.2.2 System Protection

To ensure system reliability as required under NER chapter 5, the secondary system shall be capable of providing, when requested, emergency voltage control schemes and under frequency load shedding schemes.

When requested, an under-voltage load shed system shall be provided at a substation to monitor and detect an under-voltage condition and automatically disconnect load to prevent voltage collapse. The under-voltage control system shall be able to be remotely enabled or disabled via the SCADA system.

When requested, an emergency voltage control scheme shall be provided at a substation to monitor and detect a low voltage event, and then close associated capacitors and trip associated reactors. Similarly, the emergency voltage control scheme shall monitor and detect a high voltage event, close associated reactors, and trip associated capacitors. The emergency voltage control system shall be able to be remotely enabled or disabled via the SCADA system. Individual reactive devices shall be able to be remotely selected or deselected via the SCADA system.

When requested, an under-frequency load shedding scheme shall be provided to monitor and detect an under-frequency condition and automatically trip selected circuit breakers.

When requested, an overload scheme shall be provided at a substation to monitor and detect an overload condition and automatically disconnect load to prevent plant damages. The overload scheme shall be able to be remotely enabled or disabled via the SCADA system.

Alarms and indications for the actions associated with these system protection schemes shall be designed in accordance with Powerlink SCADA Requirements for Operational Purposes Standard.

3.3 Plant Control

3.3.1 Auto-reclose

The auto-reclose function shall be designed in accordance with Auto-reclose Scheme Standard. The design shall provide enable/disable control and indications to the SCADA system as well as alarm activation at the HMI when TPAR or SPAR operation has occurred.

3.3.2 Transformer Control and Monitoring

Transformers are provided with on-load tap changing equipment, suitable for regulating the voltage of three phases simultaneously by changing tap positions while the transformer is fully or partly loaded.

The secondary system must be designed such that the on-load tap changing equipment can be controlled to operate the transformer tap changer in any of the following modes:-

- automatically by Powerlink's Automatic Voltage Regulator (AVR);
- manually by remote operation via SCADA;
- manually by operation from substation HMI;
- manually by operation at the transformer.

The voltage control algorithm for the AVR shall be provided to control all transformers within the transformer bank. The algorithm shall be simple and have adjustable setpoints with a settable deadband. The setpoints shall be adjustable via HMI or SCADA. Transformers can be removed from bank control and manually controlled individually.

When the controlled voltage is outside settable limits, automatic tap changing shall be inhibited. When the transformer load is above the tap changer rating, tap changing shall be inhibited.

The requirements for transformer tap changer alarms and indications will be in accordance with SCADA Requirements for Operational Purposes standard. Where alarms and indications are provided to customers they will be sent via ICCP link between the respective control centres.

3.3.3 Circuit Breaker Control and Monitoring

The secondary system design shall provide CB trip and close control signals and CB double pole status signals and alarms appropriate to the type of circuit breaker. These controls, status signals and alarms are to be available locally on the HMI and remotely via the SCADA links.

Appropriate synchronising facilities will be provided to perform a synchronism check before closing the CB.

CB SF6 Gas Density is to be monitored. Circuit Breakers shall be equipped with two-stage gas density detection – alarm and lockout. The first stage alerts the Network Incident Management Team to the fact that gas density is becoming critical and the secondary stage triggers a trip and/or lockout of the circuit breaker and raises a lockout alarm. The automatic decision of whether a CB trips or locks closed is implemented by an internal circuit breaker setting.

All gas circuit breakers shall be set to trip and then lockout upon reaching the secondary stage low gas level.

In addition to the two stage monitoring system, circuit breakers shall be provided with a gas density analogue transducer to permit remote monitoring of the SF6 gas pressure.

Circuit Breakers associated with transformers, capacitor banks and reactors shall have Point On Wave (POW) functionality as specified in AM Substation Design Principles Specification.

The circuit breaker automation shall operate in one of the following modes namely, Normal Mode, Sync Close Mode, Maintenance Mode or Emergency Mode. If there is no synchronising function present, Sync Close Mode and Emergency Mode are not required. Close inhibit is a function that is independent of the circuit breaker close modes.

- **Close Inhibit**

Close inhibit is a local substation function that prevents any remote closure of the circuit breaker, regardless of circuit breaker control mode. The control of this is only available via the local substation HMI. Current status of the close inhibit state is provided to the Energy Management System (EMS).

- **Normal Mode**

In the normal mode, the circuit breaker close operation can be initiated by local manual operation, remote operation, autoreclose initiation or emergency close control. The automation system will detect the required mode and perform the following:

  - Parallel Close Synch Check: This is used where the two sides of the CB are already operating in synchronism with one another. The circuit breaker closes when all synchronising conditions such as voltage, frequency and phase angle conditions are met at the instant the “CB Close” signal is executed.
  - Synch check functionality must be provided for:-
    - ✓ All CBs that may be used to connect two buses including all CBs in a breaker-and-a half arrangement, and bus coupler CBs;
    - ✓ All feeder CBs including generator feeder CBs and radial feeder CBs (as embedded generator may exist or be developed);
    - ✓ All transformer CBs except CBs that are equipped with POW function.
    - ✓ Bypass all synchronising checks if any Circuit Breaker isolators are open.

- **Sync Close Mode**

This is used where the two sides of the CB are not in synchronism with one another. The circuit breaker closes if all synchronising conditions are met within 60 seconds after the “CB Close” signal is executed or if one or both sides of the circuit breaker are de-energised.

- **Maintenance Mode**

The circuit breaker may only be operated when the associated isolators are open.

- **Emergency Close Mode**

The circuit breaker will close irrespective of the state of the sync status, providing “Close Inhibit” is off.

In any mode and at any time the circuit breaker can be opened manually through the automation system unless disabled at the circuit breaker.

3.3.4 Disconnector Control and Monitoring

The secondary system design shall provide reliable and secure disconnector open and close control signals and double pole status signals. These controls and status signals are to be available locally on the HMI and remotely via the SCADA links.

Appropriate interlocking logic must be provided to prevent;

- operation of a motorised disconnector under load
- operation of a motorised disconnector when the associated CB is closed;
- operation of a motorised line disconnector when the CB is closed in a breaker-and-a-half scenario;
- operation of a motorised disconnector if the associated earth switch/s are closed.

3.4 Plant Monitoring

Remote monitoring and control facilities shall be designed in accordance with section 4.11 of NER, Power System Security Support.

3.4.1 VT Monitoring

The secondary system shall be designed to provide monitoring and event recording of VT abnormal condition for 3 phase and single phase VTs (including Capacitive Voltage Transformer (CVT) and ElectroMagnetic Voltage Transformer (EMVT)). The VT abnormal condition shall set an urgent alarm at both HMI and SCADA systems.

3.4.2 CT SF6 Gas Density Monitoring

The secondary system shall be designed to provide the facility for Gas Density monitoring on SF6 CTs and provide a non-urgent alarm to SCADA if low gas density is detected.

3.5 SVC/STATCOM Control System

The SVC/STATCOM will include thyristor, IGBT, IGCT, valves, DC capacitor and cooling pumps/fans components. The control system for this equipment will be supplied by the manufacturers. The control system must ensure:-

- High availability;
- High reliability;
- Minimised life cycle cost of the control system asset.

The supplier will provide detailed reports to demonstrate compliance and adherence to these requirements.

3.6 Local and Remote Monitoring and Control

3.6.1 Alarm Policy

The secondary system shall provide alarm facilities, monitor automation equipment status where necessary, and measure and record appropriate electrical quantities of the high voltage system as stated in policy SCADA Requirements for Operational Purposes standard.

The individual alarms sourced directly from the plant and IEDs shall be displayed locally on the HMI and sent to the control centre via SCADA gateway. Detailed alarms with millisecond timing accuracy shall be provided on the HMI and SCADA. The secondary system shall be designed so that all secondary system IEDs are connected to an accurate time synchronisation system. Time critical signals within the system shall be time stamped with a resolution and accuracy of 1 millisecond with respect to Eastern Standard Time for event collection at HMI and SCADA system.

The secondary system protection equipment shall provide and communicate comprehensive self-diagnostic functions. Communication of the self-diagnosis shall be through monitored serial or Ethernet links. Where serial or Ethernet links are not employed, devices will provide a contact to annunciate device failure. Where 4-20 mA loops are provided, loop failure shall be annunciated.

An audible hooter alarm shall be provided to alert staff working in a substation to a safety or plant issue in protection and control buildings. The audible alarm shall be enabled or disabled at the discretion of field staff. Facilities shall be available to enable or disable the audible alarm either locally or remotely.

3.6.2 SCADA Requirements

Secondary system monitoring equipment and facilities shall be designed so that secondary system data such as plant status, control commands, indications and alarms are up to date and in a consistent format.

SCADA protocol used in secondary system shall be the recognised international standard.

The data format must be in accordance with the AEMO standard, specified in AEMO Standard for Power System Data Communications: Section 2.2- Representation of Information.

The monitoring system shall be designed to ensure secondary systems data updating, as specified in AEMO Standard for Power System Data Communications: Section 2.3- Age of Information and Table 1- Time Intervals.

The monitoring system shall be designed to meet AEMO reliability requirement as specified in Section 3- Reliability Requirements of AEMO Standard for Power System Data Communications. The system must be designed and maintained so that the total critical outage periods for remote monitoring and control equipment within a year period does not exceed the total critical outage periods specified in AEMO Standard For Power System Data Communications Section 3, Table 2- Critical Outages of Remote Monitoring Equipment or Remote Control Equipment.

SCADA performance testing facilities shall be provided within the secondary system to allow timing tests to show conformance with AEMO Standard for Power System Data Communications Section 2.3- Age of Information and Table 1- Time Intervals.

3.6.3 Substation HMI

The secondary monitoring system shall be designed to provide a HMI in each substation building, including SVC and STATCOM buildings, for local control and monitoring of the substation. The HMI will provide event collection with millisecond resolution accuracy and allow remote access to the HMI system.

Alarming shall be consistent with Section 3.5.1 Alarm Policy. Alarms shall be acknowledged and deleted from the HMI. Thin client architecture shall be used for HMI devices where possible.

During project works, the HMI must be updated to show the correct operational state of the substation at all times.

3.6.4 Integrated Operational Network & Service

The Integrated Operational Network & Service (IONS), formerly the Operational Systems Wide Area Network (OpsWAN) shall be designed to facilitate data communications from Powerlink substation and communications sites to the Powerlink Virginia Datacentre and Business Continuity Site. The network is a partial mesh design with multiple ‘hub’ sites that interconnect a group of WAN circuits together. As far as possible this network shall follow the underlying telecommunications network.

The network shall be designed to provide secure and reliable data transfer over Powerlink’s telecommunications infrastructure. Dual communication circuits shall be designed to each site, preferably over diverse paths where adequate digital communication facilities are available. Logical circuits shall be designed to make efficient and effective use of Powerlink’s telecommunications infrastructure.

When Powerlink digital communications facilities are not available, third party communications infrastructure may be utilised. Use of these telecommunications links shall follow Powerlink’s IT security policies, especially in terms of data encryption over non-Powerlink owned assets.

3.6.5 Substation Visual Monitoring

Visual Monitoring (i.e., OpsWAN camera) of the substation is required to be provided to proactively monitoring substation high volage plants.

3.7 Network Design

The high level design for the station bus is detailed in the relevant version of the Substation Design Manual.

The overall technical requirements are outlined in the Station Bus Network Requirements Specification.

3.8 Application Testing

Application testing is undertaken to prove that the secondary systems equipment and standard configurations perform as intended.

Application testing is required for any of the following conditions:-

- Using new hardware or equipment;
- Using new firmware;
- Using a new function within a protection and control device;
- Deviation from the standard template design.

3.9 Wide-Area Monitoring, Protection and Control Schemes

Wide-Area Monitoring, Protection and Control schemes including the system integrated protection scheme, anti-islanding and run-back schemes are expected to improve the reliability and security of the power system network. They involve the use of system-wide information and communication of selected local sites to remote locations to minimize power supply disruptions and ensure the security of the network according to the National Electricity Rules.

WAMPAC schemes shall be designed to:

- Meet the site specific requirements and functionalities ;
- Be reliable to meet additional site specific requirements;
- Be secure to avoid any potential mal-operations;
- Have adequate remote control and configuration and be visible via drawings, local HMI and EMS;
- Comply with Powerlink's policy of configuration management of monitoring, protection and control equipment;
- Designed according to associated Australian and international standards;
- Utilise open protocols;
- Be manageable and be maintained according to Powerlink's maintenance standard.

3.10 Metering

Metering design shall comply with Metering – National Electricity Market Standard. The metering installation shall be located at the associated connection point (which is not necessarily the asset boundary location). Metering shall be IP based metering.

3.11 Power System Monitoring

3.11.1 Power Quality Monitoring

To achieve the level of power quality required under NER chapter 5, secondary system design will provide the following facilities:

- Power frequency voltage measurement and recording
- Harmonic measurement and recording
- Voltage unbalance measurement and recording

The measurements and recordings shall conform to IEC 61000-4-30 Testing and measurement techniques - Power quality measurement methods.

Power quality and power system performance monitoring devices shall be connected to the multiservice bus. Remote interrogation of the equipment and event file transfer to the central server shall be done via Operational Digital Networks. The system shall automatically generate and transfer event recordings. The system shall provide automated reports to users. Event alerts and equipment alarms shall be provided to the HMI and SCADA system in accordance with the SCADA Requirements for Operational Purposes standard.

Negative Phase Sequence (NPS) values shall be provided for one bus of each voltage. The NPS values are to be calculated in conformance with AS1359. Monitoring and indication of NPS to the HMI and SCADA system will be provided in accordance with Powerlink's SCADA Requirements for Operational Purposes standard.

3.11.2 Power System Performance Monitoring

The secondary system will be designed to provide the following facilities for power system performance monitoring:

- Station level DDR (Digital Disturbance Recording) functionality;
- Phasor monitoring system;
- FCAS recorder.

Station Level DDR (currently called High speed monitoring system) shall be capable of sampling power system quantities such as power, voltage, frequency, current, and phase angle of the system at a high speed. Time tagged high speed data shall be made available for remote extraction via Operational Digital Networks immediately after any power disturbance to assist fault diagnostics.

Where applicable, the secondary system shall be designed to provide FCAS (Frequency Control Ancillary Services) data recording facilities to Generators when requested by the Generator. FCAS data recorders at substations will be streamed to the associated power station via proper communication interface.

The secondary system shall be designed to facilitate installation of phasor measurement units on nominated feeders at nominated substations for the on-line monitoring of power system dynamic characteristics when requested by Planning. Synchronised Phasor Measurement Unit (PMU) functionality shall be implemented according to associated international standard such as IEC/IEEE 60255-118-1 Synchrophasor for Power Systems - Measurements.

3.12 Secondary System Interface with Customers

3.12.1 Segregation of ownership of secondary system facilities at joint owned sites

One or more Interface Termination Cubicle (ITC) shall be installed between Powerlink secondary system and the customer's secondary system. ITCs serve as interface points between two parties and also act as boundary points for installation and testing of the secondary system.

All information necessary for local protection and control purposes such as CTs, VTs, transformer tap changer control and circuit breaker trips will be sent between Powerlink and the customer through the ITC.

Other information required from the customer's equipment will comply with Powerlink's SCADA Requirements for Customer Connections policy. That information shall be transferred between the customer's control centre and the Powerlink control centre. If that is not possible the next preferred option is through an equipment

SCADA link from the customer's equipment to the Powerlink control centre. The least preferred option is for the customer to feed the information into Powerlink's substation automation system so it can be passed to the Powerlink control centre.

Powerlink shall not house/install or provide customer access to Powerlink's equipment other than via signals provided through ITC.

3.12.2 Customer Control

Powerlink will be solely responsible for the control of Powerlink owned transformer tap changers including renewable connections and BESS (Battery Energy Storage System). Provision shall be made for the customer to trip Powerlink's circuit breakers as necessary to protect the customer's primary plant.

A minimal approach to providing control is preferred so that maximum reliability of the interface is maintained. This interface can be either serial or parallel within the constraints of the required performance.

3.12.3 Customer Data Requirements

Customer monitoring of data will be as per the "over the fence" view. This means the amount of data provided to the customer will be whatever is minimally necessary to successfully and safely operate the system (for both parties).

It must also be noted that any data provided to an external Customer is subject to commercial arrangements with regards to the amount of data to be supplied (i.e. point count), reliability, speed and cost.

Monitoring of data supplied from customers will be as per the "over the fence" view. This means the amount of data provided by the customer will be whatever is minimally necessary to successfully and safely operate the system (for both parties).

3.12.4 Interface to Power Stations and Renewable Connections

Power stations including synchronous generators need some degree of visibility of primary plant status belonging to Powerlink. A high speed line end open status is to be provided from Powerlink's secondary system to these power stations. For other renewable connections including solar farm, wind farm, BESS (Battery Energy Storage System) and synchronous condenser, the requirement of line end open status from Powerlink secondary systems needs to be consulted with associated customers.

The power station including renewable generations is required to provide SCADA alarms, indications and measurements to AEMO as specified by AEMO. It is required to provide SCADA alarms, indications and measurements in accordance with Powerlink policy SCADA Requirements for Generator Connections. This is provided via a SCADA link directly between the power station and Powerlink's EMS.

3.13 Secondary System Cyber Security

Secondary system design shall meet the requirements of the QLD Government Information Security Policy IS18:2018, and the Australian Energy Cyber Security Framework (AESCSF) and/or its successors.

All technology systems and components used to support the secondary system shall:-

- Provide a Defence in Depth approach to security in order to protect secondary systems from unauthorised access;
- Provide intrusion detection and logging to detect anomalous digital network traffic and provide forensic information;
- Permit the use of network SPAN (Switch Port Analyser) monitoring ports for troubleshooting and Cyber Security monitoring;
- Capture a system baseline using the SPAN monitoring port to record normal network activity when in normal operations (at least an hour);
- Ensure that the availability of systems is maintained, while also protecting the integrity and confidentiality of systems and information through segmentation of networks and systems;

- Reduce the risk of cyber-attacks against secondary systems by hardening and performing regular vulnerability assessments;
- Allow only authenticated access (via a central directory where possible);
- Permit the use of 2FA (Two-Factor Authentication) or MFA (Multi-Factor Authentication) for remote access;
- Firmware patches for known cyber threats on new secondary systems equipment shall be installed before commissioning where possible. For equipment that is in service, firmware patching shall be performed if the risk is unacceptable. Firmware patching requires Application Testing to ensure that the new firmware patch does not adversely affect/alter the performance and function of the product or its design.

3.14 Secondary System Panel Construction

Consideration must be given to ergonomic and safety in design requirements, in addition to minimising the whole life cycle cost of secondary system assets when designing a secondary systems panel.

AS/NZS 3000 shall be followed wherever is reasonably practicable in accordance with AS/NZS 3000 Wiring Rules – Specification for the panel design. Adequate internal lighting, working space and a sufficient numbers of power outlets shall be provided within the protection and control building in accordance with the Standard.

The panels shall be labelled with operational names such as feeder and circuit breaker numbers on the panel-front.

Trip isolation links, CT and VT links must be provided in the secondary system panel in compliance with electrical safety and WH&S regulations.

Control wiring from motorised isolators and CBs must be linked, protected and labelled.

The CT test links shall be clearly labelled and well organised so that the test technicians can easily identify the test links and measure the correct part of the circuit.

Revenue and metering panel CT and VT links shall be standardized with other panel links, and the links shall have provision to be sealable for revenue metering panels.

MCBs must be capable of being locked open to ensure safety of staff working on a circuit.

Substation panel doors and swing frame latches shall be designed and installed so that they do not hinder access or egress while working within or on the panel. Swing doors must be fitted with arrangement to hold them open while they are being accessed.

All components installed in the substation panel shall be in compliance with electrical safety and WH&S regulations to ensure a safe working environment.

The appropriate design practice and method must be utilised (e.g. providing barriers and complying with “hot to top” convention) in panel design to prevent inadvertent trips.

3.15 Secondary System Marshalling Kiosks and Termination Racks

Design of secondary system marshalling kiosks shall consider:-

- Minimising the total life cycle cost of the asset, including maintenance cost and outage requirements;
- Future secondary systems replacement to minimise rework on control cables and associated marshalling kiosks in a yard.

3.16 Substation Infrastructure Control and Monitoring

3.16.1 Air Conditioning

The secondary system shall be designed to provide remote and local monitoring and alarm facilities for air conditioning system conditions and room air temperature.

3.16.2 AC and DC Power Supplies

The AC and DC supplies in a substation shall comply with AM Substation Design Principles Specification and DC Supplies Specification. The secondary system for AC and DC supply control and monitoring shall be designed such that:

- Local and remote monitoring, indications and alarms for AC supplies and generator conditions are provided;
- Battery banks shall be of valve regulated cell type. Where battery banks are installed in substation buildings they shall be installed in an air-conditioned environment and to the requirements of AS 3011.2. A dedicated battery room or cabinet is not required if the room housing the batteries is only accessible to authorised personnel;
- The secondary system for DC supply control and monitoring shall be designed to provide remote and local monitoring as well as indication and alarm facilities for the condition and function of the battery charger, battery bank unit and individual battery cells. The monitoring unit shall be able to retain its memory in the event of power supply failure.

3.17 Secondary System Software

All software and firmware associated with secondary system devices should be tested and approved in alignment with current practices and be of a stable version of release. Where possible a software and firmware version across same devices should be kept to a minimum.

3.18 Secondary System Data Management

Data used and created for secondary systems is to conform to the common format and be recorded in Powerlink's prescribed systems and in alignment with the relevant data governance standards and policies.

The centralisation of data sources is to be pursued to remove duplications and easy to maintain.