ElectraNet

Substation Automation System

Document Number: 1-09-FR-20

VERSON 1.1 May 2024

This functional requirements document is in line with the organisation's 1-09-ACS-03 Substation SCADA and Automation Asset Class Strategy.

Intellectual property rights and disclaimer

This document is published in accordance with the requirements of Chapter 5 of the National Electricity Rules (**NER**). It is a functional requirement document only and is not intended to contain any comprehensive or project specific designs, specifications or other information. Whilst care has been taken to ensure that the contents of this document are accurate, ElectraNet Pty Limited (**ElectraNet**) does not represent or warrant that the information contained in this document is complete, accurate or adequate in any respect. ElectraNet reserves the right to amend this document at any time without notice to any person.

The user must carefully examine and check the information contained in this document and carry out its own independent technical and legal assessment and due diligence to ensure that the information in this document is used appropriately and that in doing so, all requirements (including requirements at law) are satisfied. For the avoidance of any doubt, the publication of this document does not limit or detract from the user's obligations at law, and does not and will not give rise to any claim (including, without limitation, in contract, tort, equity, under statute or otherwise) against ElectraNet or any of its 'Associates' (as that term is defined in *Corporations Act 2001* (Cth)).

Contents

1. Purpose

This document details the common functional requirements for ElectraNet's Substation Automation System (SAS).

2. Scope

This document defines the common functional requirements for the SAS applied to ElectraNet's 330, 275, 132 and 66 kV transmission network assets. The detailed requirements for specific SAS functions are detailed within the documents 1-09-FR-22 and 1-09-FR-23.

3. Terms, acronyms, and initialisms

3.1 Terms

Term	Definition
AC	Alternating Current, is periodic electric current with negligible direct component.
ACR	Automatic Circuit Recloser, ACRs are normally used on overhead electricity distribution networks. An ACR is a circuit breaker with an integrated: ▪ CT ▪ VT ▪ protection relay.
AEMO	Australian Energy Market Operator, manages electricity and gas systems and markets across Australia.
BESS	Battery Energy Storage System, is an energy storage technology that uses batteries to absorb and release energy on demand.
BCU	Bay Control Unit, is a unit used for the control and monitoring switching devices, data logging, capturing meter values, interlocks and logic functions switching sequences and other purposes.
CB	Circuit breaker(s), is a mechanical switching device, capable of making, carrying, and breaking currents under normal circuit conditions and also making, carrying for a specified duration and breaking currents under specified abnormal circuit conditions such as those of short circuit.
CT	Current Transformer(s), is a transformer for use with meters and/or protection devices in which the current in the secondary winding is, within prescribed error limits, proportional to and in phase with the current in the primary winding.
DC	Direct Current, is an electric current that is time-independent.
DNP3	Distributed Network Protocol 3, is a set of communications protocols used between components in process automation systems. DNP3 has been standardised in IEEE Std 1815.
DNSP	Distribution Network Service Provider, is an organisation that engages in the activity of owning, controlling, or operating an electrical distribution system.

Term	Definition
EMS	Energy Management System, is a system of computer-aided tools used by ElectraNet operators to monitor, control, and optimize the performance of the transmission system.
FBD	Function Block Diagram, is a graphical language for logic controller design, that describes the function between input variables and output variables.
FMEA	Failure Modes and Effects Analysis, is a structured approach for identifying possible failures in design, manufacturing or assembly process, product, or services.
FSC	Fixed Series Capacitors, is a series capacitor bank that has a reactance or reactances that are defined by the discrete reactances of the capacitors and are not variable.
GIS	Gas Insulated metal enclosed Substation, is a substation, or part of a substation, which is made up of gas insulated metal enclosed switchgear.
GPS	Global Positioning System, is a U.S.-owned utility that provides users with positioning, navigation, and timing services.
HMI	Human Machine Interface, is an interface between operating staff and the instrumentation and computer systems to the plant.
HV	High-Voltage, is a voltage greater than 1000 V AC or 1500 V DC.
I/O	Input/Output, describes any operation, program, or device that transfers data to or from a computer.
IED	Intelligent Electronic Device, is a microprocessor-based device equipped with software algorithms that provides protection, control, monitoring, or automation functions of power system equipment.
IP	Internet Protocol, is a protocol for connectionless transmission that corresponds approximately to a protocol within the network layer of the OSI reference model.
IRIG-B	Inter-Range Instrumentation Group-B, is a standard format for transferring timing information between power system devices, such as relays and meters.
IT	Information Technology, is the use of computers, software, networks, and other digital technologies to store, retrieve, transmit, and manipulate data.
KCC	Keswick Control Centre, is the SMSC, facility installed in Keswick, South Australia.
LAN	Local Area Network, is a computer network located on a user's premises within a limited geographical area.
LV	Low-Voltage, is a voltage in the range 50 to 1000 V AC or 120 to 1500 V DC
LVAC	Low Voltage Alternate Current, is an alternating current voltage in the range 50 to 1000 V AC.
MMS	Manufacturing Message Specification, is an ISO 9506 standard messaging systems for transferring real time process data and supervisory control information between networked devices or computer applications.
MTBF	Mean Time Between Failure, is the average time between repairable failures of a technology product.
MTTF	Mean operating Time To Failure, expectation of the operating time to failure.

Term	Definition
MTTR	Mean Time to Recovery, is the average time it takes to recover from a product or system failure. This is the total duration of the outage; from the time the system or product fails to the time that it becomes fully operational again.
NER	National Electricity Rules, are rules made under the national electricity law and govern the operation of the national electricity market.
NTP	Network Time Protocol, is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
OLTC	On-Load-Tap-Changer, a device for changing the tapping connections of a winding, suitable for operation while the transformer is energised or on load
PCC	Pirie St Control Centre, is the SMSC, facility installed in Pirie St, South Australia.
PLC	Programmable Logic Controller, is a solid-state control system which has a user programmable memory for storage of instructions to implement specific functions.
PSDCS	Power System Data Communication Standard, is a data communications standard made under clause 4.11.2(c) of the National Electricity Rules.
RTU	Remote Terminal Unit, is an intelligent electronic device that monitors field digital and analogue parameters and transmits data into SCADA.
SAS	Substation Automation System, is a collection of hardware and software components that are used to monitor and control an electrical system, both locally and remotely.
SCADA	Supervisory Control And Data Acquisition, is the monitoring and remote control of equipment from a central location using computer systems.
SIPS	System Integrity Protection Schemes, is a protection system that detects abnormal or predetermined system conditions and takes automatic corrective actions.
SMSC	System Monitoring and Switching Centre, are the facilities used by ElectraNet for managing the South Australian transmission system.
SVC	Static Var Compensator, is a device specifically provided on a network to provide the ability to generate and absorb reactive power and to respond automatically and rapidly to voltage fluctuations or voltage instability arising from a disturbance or disruption on the network.
VT	Voltage Transformer(s), is a common term for capacitor and inductive (including power) voltage transformers. VTs are transformers where the voltage across the secondary terminals is, within prescribed error limits, proportional to and in phase with the voltage across the primary terminals.
WAN	Wide Area Network, is a network that provides communication services to a geographic area larger than a single area.

3.2 Acronyms and initialisms

Acronym or initialism	Definition
Auxiliary transformer	Is a type of transformer used in for auxiliary or secondary purposes rather than the primary power distribution.
Bay	The part of a substation within which the switchgear and control-gear relating to a given circuit is contained.
Bay level	Is the level of the Substation Automation System (SAS) that provides automation functions to individual devices within a bay.
Check meter	Is a meter installed as a source of check metering data for Type 1 and Type 2 metering installations as specified in schedule 7.4 of the National Electricity Rules.
Condition monitoring device	Is a device installed to obtain information about physical state or operational parameters of a piece of equipment.
Data concentrator	Is a device used in SCADA systems to collect, aggregate, and process data from multiple sources distributed across a network.
Disconnector	Is a mechanical switching device which provides, in the open position, an isolating distance in accordance with specified requirements.
Disturbance recorder	Is an instrument in continuous operation, provided with a memory making it possible to record events and transient variables before and during fault conditions
Earthing switch	Is a mechanical switching device for earthing parts of a circuit, capable of withstanding for a specified time currents under abnormal conditions such as those of short circuit, but not required to carry current under normal conditions of the circuit.
Ethernet	Is the LAN technology that specifies the standard technical specifications of hardware for connectivity. The Ethernet standards are governed by the IEEE 802 series and vary with cabling distance and transfer speed.
GPS clock	A microprocessor-based clock that derives it time information from the GPS.
Modbus	Is a data communication protocol based upon a request-response (previously referred to as a master-slave) model. It is used for transmitting information between IEDs that are connected to buses or networks over serial lines, Ethernet or wireless.
Non-revenue meter	Is a meter installed for reasons other than revenue metering or check metering.
Remote engineering access controller	Is a device that provides remote access to IEDs. The controller prevents unauthorised access and allows authorised personnel to configure, monitor, retrieve data, diagnose, and troubleshoot equipment or systems from a remote location.
SCADA gateway	Is a device commonly known as an RTU. The SCADA gateway is an interface between individual devices and the SCADA system.
Revenue meter	Is a meter installed for the measuring and recording of the transfer of energy across points of interconnection for billing or for other purposes.
Station level	Is the level of the Substation Automation System (SAS) that consolidates automation functions from the bay levels to provide automation functions to the entire substation.
Third-party	A person or organisation that that does not have a direct relationship ElectraNet.

4. Substation automation system requirements

The SAS refers to an integrated system of IEDs in a substation providing remote monitoring, supervisory control, automatic control, and remote engineering access of the substation assets necessary for the management of the electricity transmission network.

This document describes the functional requirements of the SAS but does not include the specific protection requirements. Protection related components described in the document 1-09-FR-01, described in 1-10-ADM-20.

4.1 Safety and environmental requirements

SAS are classified, by ElectraNet, as safety critical systems. They must be designed such that the failure of a single system component does not result in the loss of remote monitoring, control, and management of the complete or multiple parts of a substation.

4.2 Planning and design requirements

4.2.1 General requirement

4.2.1.1 SAS philosophy

1. The SAS design must meet the necessary operational, maintenance, asset management and regulatory requirements for the remote monitoring, control, and access of the substation's assets in accordance with ElectraNet's obligations as transmission network service provider. these are described in the NER and 1-09-FR-22.
2. The SAS must carry out the acquisition of all the necessary indications, alarms, controls, and measurements associated with the various assets in the substation and remote systems using variety of industry standard physical interfaces and communication protocols.
3. The SAS design must comply with the performance requirements of ElectraNet's Asset management system described in this document and that of NER in accordance with PSDCS.
4. The SAS design must be equipped with the state-of-the-art processing and communication technologies as well as legacy systems support to acquire, exchange, and integrate the data associated with the various primary and secondary assets of the substation, in its ultimate layout. It must achieve it without any deterioration of the required performance levels over its projected useful life.
5. The SAS design must be efficient and scalable to allow the expansion of the system over its projected useful life with minimal impact on the in-service system components.
6. The SAS architecture design must be segregated into the Station Level and Bay Level to maintain the life cycle of the Station and Bay level components independent of each other across the life of the substation. It must be achieved using open standard communication protocols in the devices at each level.
7. The SAS devices described in this document, other than those described in 1-09-FR-01, must be physically segregated from the later to provide complete integrity of the protection systems.
8. One SAS must manage all the various voltage levels within a substation at any site except for site-specific requirement by ElectraNet.

4.2.1.2 Equipment technology

ElectraNet's SAS must be established utilising microprocessor-based equipment that can provide integrated functionality, a high degree of self-supervision, event recording and information exchange via communication channels. The requirements for equipment hardware platforms are specified within 1-09-FR-28.

4.2.2 Supervisory control points

1. The supervisory control of the primary plant to isolate or energise a piece of substation equipment or circuit must be performed only via remote control facilities in the substation control room HMI (computer based or mimic control panels) or SCADA system at KCC or PCC.
2. The provision of supervisory controls must not be implemented in the proximity of the primary plant unless plant risk assessment to do so with appropriate operating procedure is approved by ElectraNet.
3. Any control provisions in the vicinity of the primary plant must be for use during maintenance while the plant is isolated.
4. The design must allow for the concurrent availability of supervisory controls from remote SCADA at KCC or PCC and substation-local HMI at any given of time.
5. The SAS must allow the monitoring and control of the complete substation from any control building within the substation if there is more than one control building in a substation.

4.2.3 SAS elements

The SAS design must be segregated into the following two levels:

1. station level
2. bay level.

4.2.3.1 Station level

The station level SAS devices must collect substation indications, status, measurements, and controls from bay level devices to provide remote control, monitoring and engineering access of substation assets via the substation control room, SMSC, corporate IT network and third-party facilities (where applicable). The main devices at Station level must include:

1. substation SCADA gateway
2. data concentrator
3. HMI
4. remote engineering access controller.

4.2.3.1.1 Substation SCADA gateway

1. The substation SCADA gateway, sometimes referred to as Substation RTU, exchanges data and controls with the Bay/Process level devices. It then processes and exchanges it with Substation local HMI, SCADA/EMS system at KCC and PCC and third parties' SCADA systems (where applicable).
2. It must use a variety of industry-standard communication interfaces and protocols to exchange data and control with the afore-mentioned systems. These are described in 1-09-FR-22.
3. Two SCADA gateways must be provided in the substation to provide higher availability required for operational purposes and meet statutory obligations under the NER.

4. The Substation SCADA gateway must also perform station wide plant interlocking for the motorised/solenoid type switchgear and other primary equipment in the substation to provide safe control from remote and the plant local control panel.
5. ElectraNet's SCADA/EMS system at KCC or PCC must act as an intervening facility under PSDCS to exchange the data of ElectraNet's or third-party transmission network user facilities with AEMO.
6. The SCADA Gateways in ElectraNet's substation must not be used to exchange DNSPs' or third-party transmission network users' facility data with AEMO.

4.2.3.1.2 Data concentrator

1. Data concentrators must exchange data and controls from substation IEDs, other SCADA masters in the substation and/or third-party facilities. It must process the acquired afore-mentioned day and exchange it with the substation SCADA gateway.
2. Data concentrators must be required in exceptional cases where there is a limited capability of the substation SCADA gateway to communicate with the legacy or proprietary system devices.
3. The BCU may perform Data concentrator function for any new bay level devices with legacy/proprietary interface where they are not able to communicate directly with the SCADA gateway(s).

4.2.3.1.3 Human machine interface

It must perform the following:

1. Provide local monitoring and control of the complete substation from the substation control room.
2. Consist of computer-based system on control desk with keyboard, mouse, two display monitors and a printer, referred to as local HMI.
3. The HMI system must allow the Operators to independently monitor and control the substation from any control building while sharing the same alarm management, sequence of events and archiving system.
4. Use off-the-shelf software providing the substation status, alarms, and control provisions via graphics on an intuitive and user-friendly video display. The software must be maintainable over the projected useful life of the HMI system.
5. Provide an alarm management system to acknowledge and clear any substation alarms and provides a log of all the substation events including operator actions from the HMI.
6. Provide archiving of the Sequence of Events and System events and measurements for subsequent retrieval for post fault analysis.
7. Provide a read only access from corporate IT network to assist in fault investigations and corrective maintenance. Running remote access HMI application must be seamless to the HMI Operator in the substation control room.
8. A dedicated supervisory control must be provided for each CB in the control room independent of any of SAS devices.

4.2.3.1.4 Remote engineering access controller

Remote engineering access Controller must enable remote access to the substation IEDs for remote configuration, access, and data retrieval. The Controller must access the relays via the substation IP based LAN in accordance with the operational technology systems, described in 1-10-ADM-20.

4.2.3.2 Bay level

The bay/process level devices must collect associated inputs and controls of the various substation assets via hardwired interface. They then process and exchange those inputs and controls with the substation SCADA gateway for the purpose of remote monitoring and control of the substation.

The main devices at bay/process level must include:

1. BCU
2. protection and special control IEDs
3. condition monitors and miscellaneous devices.

4.2.3.2.1 BCU

It must:

1. Collect the hardwired I/O signals from the primary and secondary system assets of the associated bay and exchange them with the Substation SCADA gateway using industry standard communication interfaces and protocols.
2. Calculate the station metering measurements using CT and VT inputs with the required accuracy and communicate them to the SCADA gateway.
3. Be provided on per substation bay basis to achieve the desired system availability described in 4.1 Safety and environmental requirements. The design must assess it in the case of partially-populated substation bays where substation is not built to its ultimate layout.
4. Collect the non-bay specific miscellaneous I/Os. A miscellaneous BCU(s) must be provided in each control building.

4.2.3.2.2 Protection and special control IEDs

These IEDs are dedicated for automatic power system related functions such as protection, automatic reclosing, synch check, system synchronising, automatic voltage regulation, automatic switching of reactive plant, point on wave, wide area control, synchro phasors etc.

They make part of the SAS but are described separately in 1-09-FR-01. These devices exchange data and control either with the SCADA gateways or data concentrators via a communication protocol or hardwired interface to the peripheral I/O Units.

4.2.3.2.3 Condition monitors and miscellaneous devices

These IEDs are dedicated for condition monitoring or other miscellaneous applications in the substation and will be subjected to site specific requirements.

4.2.3.3 Communication systems

1. The SAS devices must communicate with each other within the substation and remote system via the substation IP based LAN and WAN infrastructure in accordance with the with the operational technology system systems, described in 1-10-ADM-20.
2. The SAS must make use of the state-of-the-art communication technologies and protocols while replacing or augmenting any new assets in the substation.
3. The SAS devices must exchange data and controls with each other via DNP3 protocol.
4. The devices must exchange data and control with each other via IEC 61850 MMS or Modbus communication protocols for site-specific requirements as exception.
5. Use of legacy and customised technology and communication protocols must be considered as exception only where their technical and economic feasibility clearly outweigh the costs and risks associated with the current standards option. The legacy systems may include serial

communications, outdated communication protocols and hardwired I/O interfaces to exchange signals via the Bay level devices via, protection IEDs, control IEDs, and condition monitors etc.

6. The SAS must be able to communicate with the remote SCADA systems at KCC or PCC, other substations, and third-party facilities over private or public telecommunication network while maintaining the reliability and security of the data.

4.2.4 SAS key functions

The SAS must perform the following key functions for the remote control and monitoring of the substation:

4.2.4.1 Measurements

The SAS must provide the following measurements:

1. Energy flows such as active power, reactive power, apparent power through the line exits, transformers, capacitor, reactors, SVCs etc. Auxiliary LVAC systems energy flows must be provided only if they are significant enough to adversely affect the required performance of power system network applications in SCADA/EMS system.
2. HV, frequency and power factor
3. Transformer tap positions
4. Set points for automatic switching schemes
5. Condition monitoring of auxiliary systems such as:
    a. transformer oil and winding temperature
    b. transformer dissolved gas levels
    c. substation control room(s) temperature
    d. standby generator fuel level.

The desired performance criteria for latency, dead bands, accuracy, availability, and engineering units of various types of measurements are described in 1-09-FR-22.

4.2.4.2 Status monitoring

The SAS must provide the status of the following:

1. Open and close status of CBs, ACRs, disconnectors, earthing switches using the plant auxiliary contacts. LV systems and auxiliary transformers related switchgear status must only be provided if specified explicitly in the project contract specifications.
2. Setting groups of the protection relays described in 1-09-FR-01.
3. Armed and disarmed status of automatic control schemes.
4. Health of the SAS devices and communication equipment.

4.2.4.3 Control

1. Selecting, opening, and closing of CBs, motorised disconnectors, and earthing switches.
2. Safe operation of the CBs, motorised disconnectors, and earthing switches via station wide interlocking.
3. Tap change control for OLTCs.
4. Arming/disarming of automatic control schemes.
5. Switching protection relays setting group.

6. Dispatching set points for automatic control schemes.
7. Dispatching set points for generators (where applicable).

4.2.4.4 Alarming

1. The SAS must provide the alarm for all the adverse conditions associated with primary and secondary substation assets which may represent a risk to substation integrity and system security.
2. It must include the abnormal or faulty conditions of the primary plant, infrastructure, auxiliary and secondary systems:
    a. CBs, CTs, VTs
    b. power transformers
    c. capacitor banks
    d. reactors
    e. SVCs
    f. cables
    g. GIS
    h. protection operation
    i. SAS devices and communications
    j. auxiliary AC and DC distribution
    k. auxiliary AC and DC supply systems
    l. fire and security system
    m. condition monitors devices
    n. disturbance recorders
    o. non-revenue meters
    p. revenue and check meters
    q. site-specific systems.
3. The status, alarms, measurements, and controls associated with a non-standard or uncommon applications such as:
    a. BESS
    b. SVCs
    c. FSCs
    d. synchronous condensers
    e. SIPS

    must be provided according to the equipment vendor and site-specific operational requirements.
4. The detailed physical interface and functional/performance requirements of measurements, status monitoring, controls and alarms are described in the document 1-09-FR-22 and 1-09-FR-28.

4.2.4.5 Time synchronisation

1. The SAS must provide a GPS based clock system in each control building to synchronise all the IEDs in the substation to South Australian local time.
2. The time synchronisation system must enable all the IEDs to store and report the status, alarms, events, and disturbance records in the IEDs, SCADA/EMS and HMI system in the local time with resolution and accuracy of 1ms.
3. The GPS clock must have multiple channels to provide modulated and unmodulated IRIG-B time signals as well NTP over Ethernet.
4. The time synchronisation system must make use of repeaters within the Control building should the aggregated impedance of all the IEDs deteriorates the performance of the time synchronisation system.
5. The detailed requirements of time synchronisation are described in the document 1-09-FR-21.

4.2.4.6 Programmed logic functions

The SAS must perform the following calculations for the safe operation and improved alarm performance:

1. station wide plant Interlocking
2. grouping/calculation of alarms and indications.

4.2.4.6.1 Station wide plant Interlocking

1. The SAS must provide the station wide plant interlocking to ensure safe switching operations to be carried out in the aspect of personnel safety and system security.
2. The interlocking schemes must be implemented to ensure that all switchgears are operated only in the intended sequence.
3. It must be implemented in the SCADA gateways(s) where the status, indications and alarms will be available to use in the interlocking. It must be achieved by means of PLC application in the SCADA gateways using IEC 61131-1 programming language preferably using FBD.
4. All the remote supervisory controls from the substation HMI and SCADA/EMS System at KCC or PCC, must be processed within the SCADA gateway for interlocking purposes the SCADA gateway issues the control command to the plant via bay level devices.
5. SCADA gateway must enable control on per plant basis, in the respective BCUs, for use in the plant control circuit to enable safe supervisory control of from the plant's local control panel, where such control is made available.
6. The design must ensure a failsafe degradation of the interlocking functions should one or more inputs become faulty or unavailable.
7. The detailed Interlocking requirements are described in the document 1-09-FR-14.

4.2.4.6.2 Grouping/calculation of alarms and indications

The SAS must perform the calculations to create grouped or derived alarms for reporting to the local HMI, SCADA/EMS or third-party SCADA systems. It must comprise of:

1. Grouping multiple signals such that any one of them will raise the grouped indication/alarm.
2. Derive alarms where the alarms require some masking under certain conditions or status of the substation primary or secondary assets.
3. The design must ensure a failsafe degradation of the derived/group alarms should one or more individual alarms/indications become faulty or unavailable.

SAS station level and bay level devices, other than those specified in 1-09-FR-01, must not perform any automatic control scheme or function, unless ElectraNet has a site-specific requirement.

4.2.4.7 Ancillary services

1. The SAS must include provisions for the configuration, file transfer, log and data capture, and diagnostic observation of the SAS devices from the engineering workstation for substation local or remote engineering access via ElectraNet's corporate IT network.
2. Although these services would often involve movement of large blocks of data as well as interaction with SAS devices, they must not adversely affect the required performance and security of critical real time operational services on SAS devices (including protection devices).

4.2.5 Security requirements

The SAS must ensure the following:

1. Access control: controlled access to selected devices, information, or both to protect against unauthorised interrogation of the device or information.
2. Use control: control use of selected devices, information or both to protect against unauthorised operation of the device or use of information.
3. Data integrity: integrity of data on selected communication channels to protect against unauthorised changes.
4. Data confidentiality: confidentiality of data on selected communication channels to protect against eavesdropping.
5. Restrict data flow: restrict the flow of data on communication channels to protect against the publication of information to unauthorised sources.
6. Timely response to event: responds to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.
7. Network resource availability: Ensure the availability of all network resources to protect against denial-of-service attacks.

These requirements must be implemented in conjunction with the requirements of operational technology systems, described in 1-10-ADM-20.

It must include the physical security including physical access to the automation system network and equipment, but also includes securing network equipment and cables. Electronic security may include items such as encryption, network intrusion detection, and authentication, firewalls, and IED access detection to establish an electronic perimeter of the system.

4.2.6 Characteristics

4.2.6.1 Availability

Station level: higher availability must be considered in the station level design by providing adequate redundancy in the system components used for interlocking and data exchange with the bay level devices and network control centres.

Bay level: the failure of a system component at this level should not render the remote monitoring and control of overall substation unavailable via the other healthy system components. To cater for the failure of BCU, a supervisory hardwired trip and close control with back indications must be provided for each breaker on the associated protection panel independent of the protection and other SAS devices.

4.2.6.2 Expandability

1. The SAS design must be easily expandable to add new points and/or functions, or both while connecting new SAS devices for new applications or substation augmentation during its projected life in the ultimate layout of the substation.
2. The SAS design must allow seamless expansion or with a minimal downtime, preferably in the order of 5-10 minutes.
3. The SAS design expandability must not result in the degradation of the required performance of any SAS element or function at any given time.
4. The expandability of the SAS must be applicable to the following elements:
    a. physical space
    b. power supply capacity
    c. processor throughput and number of processors
    d. memory capacity of all types
    e. point limits of hardware, software, or protocol
    f. communication bus length, loading, and traffic
    g. program routines, addresses, labels
    h. communications buffers and scan times.

4.2.7 Security of operation

1. The SAS design must be able to recognize an inappropriate or undesirable operation or condition in such a fashion that causes an appropriate alarm, a non-operation, or both.
2. The SAS devices must use both a select-before-execute user interface sequence and a checkback-before-operate communication sequence for control operations.

4.2.8 Diagnostics

The repair times following hardware or software failures can be minimized if the system provides good diagnostic tools. The diagnostic tools must be designed with the following functionality:

1. Defining failure inside or outside the system.
2. Localizing failure inside the system and to a particular device.
3. Remote operation.
4. Highly effective in minimising the repair/downtime times of hardware and software failures.

4.3 Constructability requirements

The SAS must be designed with the following functionality:

1. Each bay level device must be designed such that its I/O capability is expandable. The preferred method of expansion is through the addition of modular I/O boards.
2. The SAS design must allow the space for ultimate capacity of the expansion of the system in adjacent panels for BCUs and in the control building.
3. Hardware and software requirements as defined within 1-09-FR-28.
4. Build requirements as defined within 1-09-FR-26.

5. Circuitry and connections requirements as defined within 1-09-FR-27.
6. Mimic panel or soft push buttons on the front facia of the BCU must not be provided or used to execute controls to the switchgear or other assets.
7. All testing connection points, and isolation facilities must be provided at the front of protection and control panels with clear labels.

4.4 Maintainability requirements

SASs must be designed with the following maintenance facilities:

1. Each device must be equipped with self-monitoring and diagnostic capabilities to minimise hidden failures.
2. The BCUs should be of the modular design which allows the replacement of the defective module only.
3. Where equipment incorporates firmware, a unique number, traceable to the release of the firmware and the version of the system to which it pertains, must be clearly marked on the component, or be available from the informative interface, as well as being documented in the instruction manual.
4. Maintenance aids such as printed wiring extension boards, jumper leads, and other special tools must be provided.
5. Full facilities and range of adjustment must be provided to allow the calibration of the equipment to be maintained over its design life, whilst installed on site.
6. Each device, which is in service, must be capable of being safely isolated from the rest of secondary system without the need for primary system outages, specialist tools and knowledge.
7. If the device, which is to be isolated, is connected to other device(s) to form a protection or control scheme (e.g. feeder protection), the isolation must be conditioned with the isolation status of the remotely connected device(s).
8. Each device must be capable of being tested by analogue and digital injections from external test set after being isolated from the rest of secondary system. This requirement is also extended to the ability of capturing communication messages to the SAS.
9. If a device becomes defective, the failed equipment must be capable of being removed and replaced without primary system outages.

4.5 Operability requirements

The SAS must be designed with the following functionality:

1. It must provide alarms, indications and measurements to the operators and maintenance personnel in an unambiguous fashion to perform the required operational and maintenance activities. It should allow the controls to be securely executed in a two-step process avoiding inadvertent execution by a mouse click touching without pushing or leaning.
2. The design must be ergonomic as far as practically possible without any adverse impact on their physical health and safety of the personnel using the system.
3. The system must degrade in fail-safe manner in case of defect in any of the system component and must provide sufficient unambiguous information to the remote and local personnel related to the unavailability and defect.
4. The SAS devices must not mal-operate during primary equipment energisation or de-energisation.

4.6 Availability requirements

The SAS design must comply with the availability requirements listed in 1-09-ACS-03. The SAS supplier must clearly state the MTBF and MTTR for SAS devices and system.

4.7 Reliability requirements

1. The SAS design must comply with the availability requirements listed in 1-09-ACS-03.
2. The SAS supplier must clearly state the MTTF for the devices and system. The failure modes of equipment and the effects of these failures must be formally analysed by the supplier. The results of these FMEA must be made available for review upon request.
3. Failure distribution vs. time data for equipment while in the possession of the supplier, and for those field units for which data are available from the users, must be made available upon request.
4. Manufactured and/or supplier-procured parts and components that can cause a critical or major system failure are subject to these requirements described above. When these values are not within acceptable limits, redundant systems and/or components must be utilised.

4.8 Testing and validation requirements

Each secondary system device must comply with the requirement listed in 1-09-FR-28.

City West Substation

Appendices

ElectraNet

References

Legislation

Legislation	Abbreviation	Description
Electricity Act 1996	SAEA	South Australian Government Legislation
National Electricity Rules	NER	AEMC rules pursuant to National Electricity Law, contained in a schedule to the National Electricity (South Australia) Act 1996.
Electricity Transmission Code	ETC	Essential Services Commission of South Australia code pursuant to Part 4 of the Essential Services Commission Act

Standards

Name	Title
IEC 61131-1	
IEC 61850 (series)	Communication networks and systems for power utility automation
PSDCS	Power System Data Communication Standard *Informative: This is a standard published by AEMO.*

ElectraNet documents

Name	Title
1-09-ACS-01	Secondary Systems - Protection Asset Class Strategy
1-09-FR-09	Protection Signalling and Intertripping
1-09-FR-14	Switchgear Interlocking
1-09-FR-21	Time Synchronisation
1-09-FR-22	Substation SCADA
1-09-FR-23	Operator Control Interface
1-09-FR-26	Cubicle and Panel
1-09-FR-27	Circuitry
1-09-FR-28	Equipment Hardware and Software
1-10-ADM-20	Internet Protocol Network Equipment

ElectraNet