Secondary Systems Design Standard

Summary
This standard outlines the performance design parameters for secondary systems constructed to connect to and form part of the TransGrid network. Transgrid publishes this information under clause 5.2A.5 of the National Electricity Rules.

Document Control			
Date of issue	November 2023	**Update**	Removed reference to the Secondary Systems Overview, previously in Section 5.2.

Disclaimer and important notice

This document and the information in it is for general guidance only and may be subsequently updated or amended. This document does not constitute technical or other professional advice, and should not be relied on as a substitute for obtaining detailed technical and professional advice about its subject matter.

To the maximum extent permitted by law, TransGrid and its officers, employees and consultants involved in the preparation of this document:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this document;
- are not liable (whether by reason of negligence or otherwise) for any statements or representations in this document, or any omissions from it, or for any use or reliance on the information in it.

Contents

1. Purpose 4

2. Scope 4

3. Objectives 4

4. Acronyms and Abbreviations 4

5. General 5

5.1. Design parameters 5
5.2. Safety in design 5
5.3. Design documentation 6
5.4. Design standards 6

6. Operational requirements 7

7. Secondary System Redundancy Requirements 7

8. Protection Design Standard 7

8.1. Protection Conceptual Agreement 8
8.2. Feeder protections 8
8.3. Capacitor protections 8
8.4. Busbar protections 9
8.5. Shunt reactor and interzone protections 9
8.6. Transformer protections 9

9. Market Metering 9

9.1. Metering conceptual Agreement 9

10. Integrated Control Specification 9

10.1. Interlocking principals 9
10.2. Interlocking design 9
10.3. Bay control operation 10
10.4. Feeder auto reclose 10
10.5. CB synchronism/ energisation check 10
10.6. Automatic voltage control 10
10.7. Control metering 10
10.8. Alarm and indication systems 11

11. SCADA System.......... 11
11.1. Automation conceptual agreement 11
11.2. Operational technology (OT) and cyber security 11
12. Communications System Design Requirements.......... 11
12.1. Communications conceptual agreement.......... 11

1. Purpose

This design standard for Secondary Systems outlines the minimum protection, electrical, automation, and communication design required for deployment of secondary systems into TransGrid's network.

2. Scope

This standard covers the secondary system schemes, standard design references and design parameters required for TransGrid to safely protect and control high voltage equipment at 500kV and below.

This standard is not intended as a substitute for National Electricity Rules, applicable Australian Standards or other Regulatory Standards, Codes or Acts.

3. Objectives

TransGrid requires secondary systems to be provided in accordance with this standard to ensure

- Safety of TransGrid's assets;
- That relevant Australian legal requirements are met;
- Systems are practical in operation and maintenance;
- Reliability and continuity of power supply from the power transmission network;
- Minimum disruption to the power supply system following a fault;
- That the requirements of the National Electricity Rules are met;
- System stability is maintained;
- Integration with existing systems;
- Alignment with TransGrid's network operational strategies and TransGrid's established maintenance practices; and
- That the exposure of risk to the TransGrid's business is minimised.

4. Acronyms and Abbreviations

The following abbreviations and acronyms may appear in this standard.

Term	Definition
ACA	Automation Conceptual Agreement
AEMO	Australian Energy Market Operator
AVC	Automatic Voltage Control
CB, CT, VT	Circuit Breaker, Current Transformer, Voltage Transformer
CCA	Communications Conceptual Agreement
EDMS	Electronic Document Management System
GWh	Giga Watt Hour
HMI	Human Machine Interface
IED	Intelligent Electronic Device (Relay)

Term	Definition
ITP	Inspection and Test Plan
NER	National Electricity Rules
PCA	Protection Conceptual Agreement
PRIM	Protection Relay Information Management System
RMS	Root mean square
RNF	Relay Notification Form
RTI	Relay Test Instruction
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System
SSZ	Substation Security Zone
VAr	Reactive or apparent power (volt – ampere reactive)
HSM	High Speed Monitors

5. General

5.1. Design parameters

The design scope shall include consideration of the following inputs:

- Operational requirements;
- Planning requirements;
- Redundancy requirements of secondary systems;
- Reliability requirements of all secondary systems;
- Maintainability requirements of all secondary systems;
- Principal preferred documentation format;
- Principal preferred IED hardware;
- Principal preferred computer operating system and software platforms; and
- Relevant design standards.

5.2. Safety in design

Designs shall be in accordance with the Safe Work Australia Safe Design of Structures Code of Practice.

5.3. Design documentation

Where required, design documentation for construction shall include the following:

- Protection Single Line Diagram;
- RNFs - Design documents providing detailed schemes, connection details, relay models and tripping sequence. This document is provided for each bay;
- RTIs - Documents providing IED settings, configurations, rating advice, test injection tables and tripping sequence. This document is provided for each protection;
- Schematic diagrams;
- Layouts and Label Schedules;
- Cabling connection details;
- AC design calculations;
- DC design calculations;
- Cable schedules;
- Control System Overview Diagram;
- Time Synchronisation Diagram;
- AC Single Line Diagram;
- DC Single Line Diagram;
- Building Arrangements;
- Logic/function diagrams; and
- ITPs.

5.4. Design standards

All Secondary Systems shall meet the following standards:

- AS2067 - Substations and high voltage installations exceeding 1 kV a.c.;
- AS2293 - Emergency escape lighting and exit signs;
- AS2676 - Installation and maintenance of batteries in buildings;
- AS3000 - Wiring Rules;
- AS3008 - Selection of cables Cables for alternating voltages up to and including 0.6/1 kV;
- AS3010 - Combustion Engine Generators connected to an electrical installation;
- AS3011 - Electrical installations — Secondary batteries installed in buildings;
- AS3439 - Low-voltage switchgear and control gear assemblies;
- AS3731 - Stationary Batteries - Nickel-Cadmium;
- AS4029 - Stationary batteries — Lead-acid;
- AS4044 - Battery chargers for stationary batteries;
- AS5000.1 - Electric cables - Polymeric insulated For working voltages up to and including 0.6/1 (1.2) kV;
- AS5000.3 - Electric cables - Polymeric insulated Multicore control cables;
- IEEE485 - Recommended Practice For Sizing Lead-Acid Batteries For Stationary Applications;
- IEEE1115 - Recommended Practice For Sizing Nickel-Cadmium Batteries For Stationary Applications
- STANDARD FOR POWER SYSTEM DATA COMMUNICATIONS (AEMO);
- National Electricity Rules Version 106;
- In addition to the mandatory standards, the Connection Asset secondary system designs will be assessed for:
  - Operability
  - Maintainability

- Ease of future augmentation.

6. Operational requirements

The following shall be addressed in the secondary system design to ensure that it meets the operational requirements of the transmission network:

- Network Reliability should be maximised for all Secondary System designs through all aspects of construction, operation and maintenance;
- Any single secondary system equipment failure must not prevent the operation of local manual switching of substation circuit breakers; and
- Measures shall be implemented to prevent the unsafe operation of HV Equipment. Interlocking signals and isolation points must maintain high voltage network security and safety.

7. Secondary System Redundancy Requirements

If the Connection Assets installation utilises any of the following systems, they must be duplicated and be provided with an adequate measure of physical and electrical segregation. Systems are required to avoid common points of failure between duplicated or redundant facilities such as:

- Batteries;
- Battery chargers;
- Auxiliary supplies;
- Protection IEDs;
- CB trip coils; and
- Cables containing No.1 and No.2 protection quantities, including but not limited to:
    - Trip circuits to CBs
    - CT and VT secondaries
    - Communication systems.

No single secondary system device failure shall cause the loss of SCADA for more than one bay. Data communications to the TransGrid Master-station shall be duplicated. SCADA data concentrators and communications to the TransGrid Master station shall be redundant and change-over seamlessly.

8. Protection Design Standard

Protection systems shall be designed to reliably clear the faults to maintain the system stability, prevent consequential asset damage, causing minimum disruption and provide a cost effective solution over the lifecycle of the assets. Protection schemes shall be designed so that all faults are cleared, despite the failure of one protection scheme or failure of an associated circuit breaker. This principle embodies the concept of equipment redundancy, which is essential to provide a reliable, secure and cost-effective level of power system protection.

The following design criteria shall apply to protection and integrated control schemes:

- The protection scheme is designed to cater for the coincidence of one fault and
    - the failure of any one component in the protection schemes designed for purpose of clearing the fault

OR

- the failure of a circuit breaker whose operation is necessary to interrupt the flow of fault current.

- Each of the primary sensing relays in a duplicated protection scheme shall be sourced from a different manufacturer; and
- All protection systems shall comply with the latest Schedule S5.1a.1 tabulated in Chapter 5 of NER for primary and backup fault clearance times.

8.1. Protection Conceptual Agreement

IUSA, DNA and Dedicated Connection Asset protection system interfaces that connect to Transgrid systems shall be defined in the Protection Conceptual Agreement (PCA). The PCA is a negotiated agreement between the Connection Applicant and Transgrid. The PCA is to outline the protection systems required for adjacent Transgrid assets, IUSA, DNA and Dedicated Connection Assets; and to define the interfaces between them. The PCA will also delineate the responsibilities for technical functionality and commissioning.

8.2. Feeder protections

All transmission lines and cables are to be protected by duplicate high-speed distance or duplicated line differential protection.

- The duplicate line differential protection is to be provided subject to agreement with remote end works for the following cases:
  - For feeders with rated voltage of 220 kV and above
  - All feeders where accelerated fault clearances are required to maintain system stability
  - Line differential protections shall match the remote end protections;
- Alternate to line differential protections is distance in a permissive scheme;
- Protection intertrips shall match the remote end intertrips;
- Line differential relays shall have integrated distance protections;
- Typical operating times including output relay times shall be:
  - 20 msec for distance protections
  - 25 msec for Line differential
  - 15 msec for CB Fail reset;
- Protection communication end to end (excluding protection relay processing) times shall be less than 15 msec; and
- Protection communications shall not be switched and shall be route diversified for No. 1 and No. 2 protections.

8.3. Capacitor protections

- All capacitors banks are to be protected by duplicate protection; and
- Typical operating times including output relay times shall be:
  - 20 msec for overcurrent, earth fault, bridge unbalance protections pickup
  - 15 msec for CB Fail reset;

8.4. Busbar protections

- All busbars 66 kV and above are to be protected by duplicate high-impedance or low impedance busbar differential protection; and
- Typical operating times including output relay times shall be;
  - 20 msec for differential protection
  - 15 msec for CB Fail reset.

8.5. Shunt reactor and interzone protections

- All shunt reactors and interzone at 66 kV and above are to be protected by duplicate high-impedance or low impedance differential protection; and
- Typical operating times including output relay times shall be;
  - 20 msec for differential protection
  - 15 msec for CB Fail reset

8.6. Transformer protections

All transformers with a nominal voltage on any winding up to 132 kV or with a rating of 60 MVA and above are to be protected by duplicate transformer differential protection. Transformers at 66 kV, 33 kV and 22 kV level are to be protected by duplicated transformer differential protection unless otherwise specified.

9. Market Metering

9.1. Metering conceptual Agreement

The metering conceptual agreement should be prepared by the metering service provider to outline the concept design of the metering and power system monitoring systems to be installed at the connection point. The agreement shall outline the Meter, Power System Monitor, CT and VT details and any interfaces they have to other secondary systems.

10. Integrated Control Specification

This section provides the schemes for control operation of isolators, earth switches and circuit breaker with interface to SCADA and substation HMI/Data Concentrator.

10.1. Interlocking principals

The Interlocking methodologies shall ensure that all apparatus is safe to operate. Interlocking shall:

- Prevent the switching operation of live equipment on to earth; and
- Prevent operation of isolator and earth switches on load.

10.2. Interlocking design

Interlocks shall be provided using open and close pallet status of CB, isolator, earth switches and voltage/live line detectors.

Interlocking circuits shall be fail safe. i.e. the operation shall be prevented if part of the interlocking circuit is faulty and results in open circuit or loss of auxiliary supply.

To ensure the inadvertent operation of isolators and earth switches from the accidental closing of output contact from IED, the hardwire interlocks are required which are external to the IED.

HMI Red Tag (substation HMI): HMI tag is a software tag applied on substation HMI to specific apparatus intended to make it nonoperational. All control operations other than local operation at bay equipment are blocked by HMI red tag.

10.3. Bay control operation

Bay control shall be implemented in relation to the following different modes:

- SCADA control;
- Substation HMI;
- Push button or HMI on both Protection No.1 and Protection No.2 IEDs; and
- Local operation on bay equipment with safe to operate lamp (hardwired interlocks used for safe to operate circuit).

10.4. Feeder auto reclose

Auto reclose schemes are generally required to be implemented in one device which shall be a combined protection and control IED or external device.

The second protection IED shall provide initiate and inhibit command to Combined P&C IED or external device.

10.5. CB synchronism/ energisation check

CB synchronism/energisation check shall be provided to ensure that CB is not closed out of synchronism and correct operation of the auto-reclose scheme

10.6. Automatic voltage control

Automatic Voltage Control (AVC) provides control of reactive plant CB on discrete settable voltage settings with suitable time delays.

AVC shall have the following features:

- Settable under voltage and overvoltage element with timers to close and open CB;
- Capacitor discharge timers;
- Two voltage source capability; and
- Capable of selecting voltage source from two different sources through remote selection commands from SCADA.

10.7. Control metering

IEDs will use internal metering functions to provide analogue quantities to SCADA, local and substation HMI:

- Voltages and currents;
- Active and reactive power; and
- Frequency.

10.8. Alarm and indication systems

Alarm and indication systems provide information for any fault in primary and secondary system to Network Operations, Asset Monitoring Centre and other users to make appropriate decisions to ensure the network is operated in a secure, reliable and safe manner.

11. SCADA System

SCADA and automation systems shall be designed to accurately and reliably allow the local and remote operation, alarm, indication and condition monitoring of substation assets.

SCADA systems shall be designed to maximise availability, reliability and shall ensure that the failure of a single IED only affects the SCADA for a single bay. This principle embodies the concept of equipment redundancy, which is essential to provide a reliable, secure and cost-effective level of power system availability.

Secondary system and SCADA designs shall comply with the NER.

11.1. Automation conceptual agreement

The Connection Applicant is required to submit an Automation Conceptual Agreement (ACA). The ACA is a negotiated agreement between the Connection Applicant and TransGrid. The intent of the ACA is to define the proposed Connection Asset secondary system physical and virtual interfaces and delineate the responsibilities for functionality and commissioning. The ACA shall be used to define the interface points for the SCADA systems and permit TransGrid to assess the operability and maintainability of the proposed secondary systems.

11.2. Operational technology (OT) and cyber security

The TransGrid secure network shall provide the means for secure data connectivity of local and remote substation IEDs. TransGrid shall define particulars of the OT interfaces within the ACA to ensure cyber security is maintained.

- All protection, control, SCADA, condition monitoring IEDs, fault recorders, disturbance recorders and travelling wave fault locators shall be connected to SSZ network hardware.
- Any TransGrid operational data communications shall require access controls, encryption, key management, password and other physical and virtual network security measures.

12. Communications System Design Requirements

12.1. Communications conceptual agreement

The Connection Applicant is required to submit a Communications Conceptual Agreement (CCA). The CCA is a negotiated agreement between the Connection Applicant and TransGrid. The intent of the document is to define the proposed connection asset communication system physical and virtual interfaces and delineate the responsibilities for functionality and commissioning. The CCA shall be used to define the interface points for the SCADA system and permit the TransGrid to assess the operability and maintainability of the proposed system against the standards and operational intent of the connection asset.

Due to the vendor specific nature of wide area communications systems and the variable connection asset requirements for protection, SCADA and telecommunications signalling infrastructure, the Connection Applicant may be required to install hardware in accordance with remote end TransGrid installations.