Network Standard

NETWORK		
	Document No	: NW000-S0149
	Amendment No	: 0
	Approved By	: Head of AEP & S
	Approval Date	: 18/07/2019

NW000-S0149 **NS273 SECONDARY SYSTEMS CONFIGURATION MANAGEMENT**

ISSUE

For issue to all Ausgrid and Accredited Service Providers' staff involved with the development of secondary systems equipment configuration documentation and files, and is for reference by field, technical and engineering staff.

Ausgrid maintains a copy of this and other Network Standards together with updates and amendments on www.ausgrid.com.au.

Where this standard is issued as a controlled document replacing an earlier edition, remove and destroy the superseded document.

DISCLAIMER

As Ausgrid's standards are subject to ongoing review, the information contained in this document may be amended by Ausgrid at any time. It is possible that conflict may exist between standard documents. In this event, the most recent standard shall prevail.

This document has been developed using information available from field and other sources and is suitable for most situations encountered in Ausgrid. Particular conditions, projects or localities may require special or different practices. It is the responsibility of the local manager, supervisor, assured quality contractor and the individuals involved to make sure that a safe system of work is employed and that statutory requirements are met.

Ausgrid disclaims any and all liability to any person or persons for any procedure, process or any other thing done or not done, as a result of this Standard.

All design work, and the associated supply of materials and equipment, must be undertaken in accordance with and consideration of relevant legislative and regulatory requirements, latest revision of Ausgrid's Network Standards and specifications and Australian Standards. Designs submitted shall be declared as fit for purpose. Where the designer wishes to include a variation to a network standard or an alternative material or equipment to that currently approved the designer must obtain authorisation from the Network Standard owner before incorporating a variation to a Network Standard in a design.

External designers including those authorised as Accredited Service Providers will seek approval through the approved process as outlined in NS181 Approval of Materials and Equipment and Network Standard Variations. Seeking approval will ensure Network Standards are appropriately updated and that a consistent interpretation of the legislative framework is employed.

Notes: 1. Compliance with this Network Standard does not automatically satisfy the requirements of a Designer Safety Report. The designer must comply with the provisions of the Workplace Health and Safety Regulation 2017 (NSW - Part 6.2 Duties of designer of structure and person who commissions construction work) which requires the designer to provide a written safety report to the person who commissioned the design. This report must be provided to Ausgrid in all instances, including where the design was commissioned by or on behalf of a person who proposes to connect premises to Ausgrid's network, and will form part of the Designer Safety Report which must also be presented to Ausgrid. Further information is provided in Network Standard (NS) 212 Integrated Support Requirements for Ausgrid Network Assets.

2. Where the procedural requirements of this document conflict with contestable project procedures, the contestable project procedures shall take precedent for the whole project or part thereof which is classified as contestable. Any external contact with Ausgrid for contestable works projects is to be made via the Ausgrid officer responsible for facilitating the contestable project. The Contestable Ausgrid officer will liaise with Ausgrid internal departments and specialists as necessary to fulfil the requirements of this standard. All other technical aspects of this document which are not procedural in nature shall apply to contestable works projects.

INTERPRETATION

In the event that any user of this Standard considers that any of its provisions is uncertain, ambiguous or otherwise in need of interpretation, the user should request Ausgrid to clarify the provision. Ausgrid's interpretation shall then apply as though it was included in the Standard, and is final and binding. No correspondence will be entered into with any person disputing the meaning of the provision published in the Standard or the accuracy of Ausgrid's interpretation.

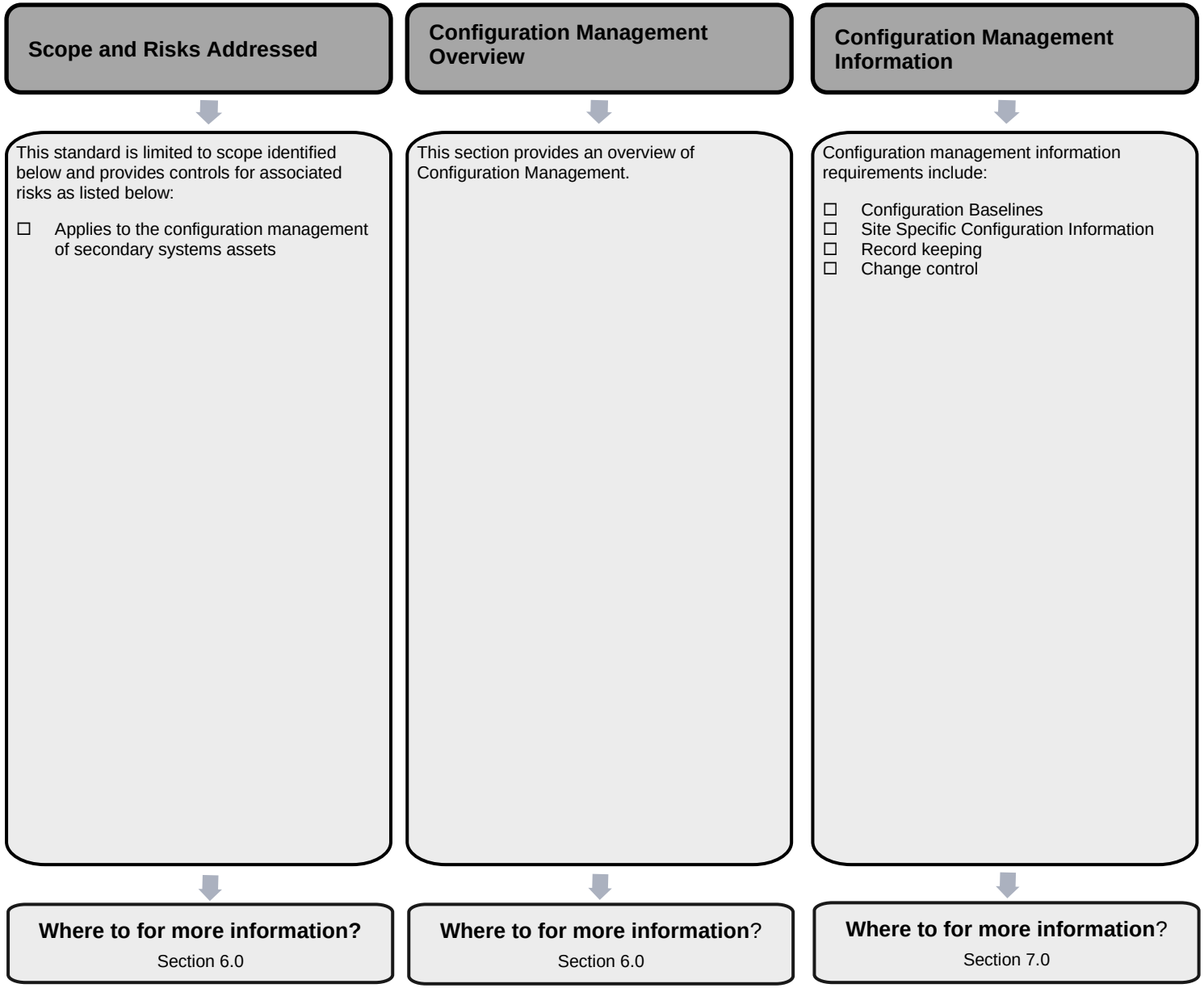
KEYPOINTS

This standard has a summary of content labelled "KEYPOINTS FOR THIS STANDARD". The inclusion or omission of items in this summary does not signify any specific importance or criticality to the items described. It is meant to simply provide the reader with a quick assessment of some of the major issues addressed by the standard. To fully appreciate the content and the requirements of the standard it must be read in its entirety.

AMENDMENTS TO THIS STANDARD

Where there are changes to this standard from the previously approved version, any previous shading is removed and the newly affected paragraphs are shaded with a grey background. Where the document changes exceed 25% of the document content, any grey background in the document is to be removed and the following words should be shown below the title block on the right hand side of the page in bold and italic, for example, Supersedes – document details (for example, "Supersedes Document Type (Category) Document No. Amendment No.").

KEY POINTS OF THIS STANDARD



Network Standard
NS273
Secondary Systems Configuration Management

Contents

1.0 PURPOSE

The purpose of this standard is to describe the requirements for secondary systems configuration management.

2.0 SCOPE

This standard pertains to the configuration management for secondary systems assets installed on the Ausgrid network in line with:

- ISO 10007:2017 – Quality Management – Guidelines for Configuration Management; and,
- ISO 9001:2016 – Quality Management Systems – Requirements.

3.0 AUTHORITIES AND RESPONSIBILITIES

For this network standard the authorities and responsibilities of Ausgrid employees and managers in relation to content, management and document control of this network standard can be obtained from the Company Procedure (Network) – Production / Review of Engineering Technical Documents within BMS. The responsibilities of persons for the design or construction work detailed in this network standard are identified throughout this standard in the context of the requirements to which they apply.

4.0 RELATED DOCUMENTS

4.1 General

All work covered in this document shall conform to all relevant Legislation, Standards, Codes of Practice and Network Standards. Current Network Standards are available on Ausgrid's Internet site at www.ausgrid.com.au.

4.2 Ausgrid documents

- Company Form (Governance) - Network Technical Document Endorsement and Approval
- Company Procedure (Governance) - Network Technical Document Endorsement and Approval
- Company Procedure (Network) – Network Standards Compliance
- Company Procedure (Network) - Production / Review of Engineering Technical Documents within BMS
- Customer Installation Safety Plan
- Electrical Safety Rules
- Electricity Network Safety Management System Manual
- NS178 Secondary System Requirements for Major Substations
- NS181 Approval of Materials and Equipment and Network Standard Variations
- NS212 Integrated Support Requirements for Ausgrid Network Assets

4.3 Other standards and documents

- ENA Doc 001-2008 National Electricity Network Safety Code
- ISO 10007:2017 – Quality Management – Guidelines for Configuration Management
- ISO 9001:2016 – Quality Management Systems - Requirements

4.4 Acts and regulations

- Electricity Supply (General) Regulation 2014 (NSW)
- Electricity Supply (Safety and Network Management) Regulation 2014
- Work Health and Safety Act 2011 and Regulation 2017

5.0 DEFINITIONS

Accredited Service Provider (ASP)	An individual or entity accredited by the NSW Department of Planning and Environment, Energy, Water and Portfolio Strategy Division, in accordance with the Electricity Supply (Safety and Network Management) Regulation 2014 (NSW).
Business Management System (BMS)	An Ausgrid internal integrated policy and procedure framework that contains the approved version of documents.
CAD	Computer Aided Design
Configuration	Interrelated functional and physical characteristics of a product or service that defines an end user function.
Document control	Ausgrid employees who work with printed copies of document must check the BMS regularly to monitor version control. Documents are considered "UNCONTROLLED IF PRINTED", as indicated in the footer.
DARTS	Digital & Analogue Relay Tracking System.
HPRM	Hewlett-Packard Records Manager - Ausgrid's corporate record management system.
IED	Intelligent Electronic Device - digital relays, using a microprocessor to perform several protective, control and automation functions
Network Standard	A document, including Network Planning Standards, that describes the Company's minimum requirements for planning, design, construction, maintenance, technical specification, environmental, property and metering activities on the distribution and transmission network. These documents are stored in the Network Category of the BMS repository.
PAC	Protection, Automation & Control
Review date	The review date displayed in the header of the document is the future date for review of a document. The default period is three years from the date of approval however a review may be mandated at any time where a need is identified. Potential needs for a review include changes in legislation, organisational changes, restructures, occurrence of an incident or changes in technology or work practice and/or identification of efficiency improvements.
RTI	Relay Test Instruction –detailed document that lists the devices installed on the panel, instrument transformer details, the functional behaviour of the panel, test injection values for protective functions and the list of attached setting files.
Vault	Ausgrid's Drawing Management System

6.0 CONFIGURATION MANAGEMENT

Configuration management is an activity that applies technical and administrative direction over the life cycle of a product, its configuration identification and status, and related product and configuration information.

A good configuration management program ensures that:-

1. Designs are traceable to requirements,

2. Change is controlled and documented,
3. Interfaces are defined and understood; and,
4. There is consistency between the product and its supporting documentation.

Further, configuration management provides documentation that describes:-

1. What is supposed to be produced,
2. What is being produced,
3. What has been produced; and,
4. What modifications have been made to what was produced.

7.0 CONFIGURATION INFORMATION

Configuration information comprises both design and operational information and includes Configuration Baselines and site specific IED configurations.

7.1 Configuration Baselines

A Configuration Baseline consists of the approved configuration information that represents the definition of the secondary systems asset.

Configuration Baseline information should be established for all IEDs and must include the following:-

1. Approved hardware, firmware and software,
2. List of approved relay functions and elements,
3. Standard Template Schematics, and;
4. IED Base Configurations.

Configuration Baseline information must be documented in the appropriate IED Application Guide.

7.1.1 Hardware, Firmware and Software

Secondary systems equipment installed on Ausgrid's network must utilise approved hardware only. Further, all related firmware and software must be adequately evaluated and approved for use prior to release on the network.

Firmware and software versions must be controlled and only altered in conjunction with an appropriate evaluation on a new version.

Approved hardware, firmware and software for IEDs must be listed in the applicable IED Application Guide.

7.1.2 IED Functions and Elements

Only approved IED functions and elements can be utilised for use on Ausgrid's network and these must be adequately evaluated prior to approval for use.

Approved IED functions and elements must be listed in the applicable IED Application Guide.

7.1.3 Standard Template Schematics

Standard Template Schematics provide IED input/output requirements and configurations for standard PAC schemes used by Ausgrid.

These schematics may refer to specific IED models and can form part of the Configuration Baseline for more than one IED. They should be produced in CAD format with a unique drawing number and detailed in a relevant Network Standard, e.g. NS178.

7.1.4 IED Base Configurations

IED Base Configurations are required to ensure standardisation of setting configurations for different applications and to minimise IED lifecycle costs.

The suite of Base Configurations for each IED should cover each standard application for that IED. Further, there must only be one Base Configuration for each application (not including revisions).

All Base Configurations must have an "Intended Application" description included in the relevant IED Application Guide.

IED Base Configurations must be adequately tested prior to release on the system to ensure configuration errors are minimised.

IED Base Configurations should be produced in IED specific formats (i.e. produced using IED software), be listed in the appropriate IED Application Guide and stored in an approved corporate quality system.

7.2 Site Specific IED Configuration Information

7.2.1 Site Specific Design Schematics

Site specific design schematics are diagrams which show the electrical interconnections and functions of PAC circuits and schemes. Schematics facilitate the tracing of PAC circuits and the associated functions without regard to actual physical size, shape and location of the IEDs and other devices, i.e. links, terminals, labels, etc.

Site specific designs may be unique to a particular site or be a standard design with an associated drawing(s).

Site specific design schematics shall be created for all PAC schemes in zone and sub-transmission substations. Distribution sites shall be based on a standard design and have appropriate records to describe the site specific configuration e.g. IED Base Configurations utilised, number of LV distributors and CT ratios.

7.2.2 RTIs

In distribution (including field protection devices such as reclosers), zone and sub-transmission substations an appropriate RTI must be created for each protection and control panel (including SCADA panels) and as a minimum they must include the following information:-

- The devices installed on the panel, including full order codes and firmware versions,
- The transformation ratio required for instrument transformers,
- A detailed list of relevant device setting parameters (e.g. pickups, time settings, reach points, etc), alarms and labels that are relevant to the operation and testing of the IEDs (this may be in the format of static screen shots for SCADA systems),
- Information relevant to the testing of the relay, e.g. secondary test injection values for protective functions which are more complex than a single quantity threshold such as transformer differential, distance, etc,
- Information relevant to the functional behaviour of the panel which cannot be derived from the associated Site Specific Design Schematics,
- A reference to the associated protection setting calculation file(s); and,
- A list of attached setting files which must be loaded into the devices and reference to the associated IED Base Configurations on which the configurations are based upon.

7.2.3 Site Specific Setting Files

Site specific IED setting files must be based on the most recent IED Base Configuration that is applicable to the intended application to ensure configuration consistency and traceability. Where an adequate IED Base Configuration does not exist a new one should be created for the application.

Minor changes from the IED Base Configuration are acceptable and they must be justified and documented in an appropriate quality document, e.g. RTI or calculation file. Minor changes include:-

- Site specific relay details, i.e. substation name, panel name, etc,
- Alteration of relay element settings, e.g. pickup, time setting, etc,
- Enabling or disabling an approved IED element contained in the IED Base Configuration, e.g. Hi-Set DMT, etc,
- Enabling or disabling IED inputs and outputs; and,
- Minor logic changes (e.g. logic modified to support intertrip to embedded generator at remote end). In these instances a note must be included on the RTI to describe the change and the intention of the functionality that has been changed/added.

If a site-specific setting file is based on an IED Base Configuration that has a different intended application the site-specific intended application must be described in a note on the RTI.

Where significant changes are required from the IED Base Configuration consideration should be given to creating a new IED Base Configuration. Significant changes include:-

- Changes to relay logic that alter the functionality of the device,
- Addition of new relay elements not approved for the existing IED Base Configurations; and,
- Addition of IED inputs and outputs that affect the functionality of the device.

Site specific IED setting files should be produced in the approved formats which are listed in the IED Application Guide. Site specific IED setting files for Protection and SCADA applications should be stored against the appropriate IED device in the corporate quality system.

7.3 Documented Information

Configuration information must be relevant and traceable and must utilise standard naming and numbering conventions (including revision status) to ensure proper control.

To ensure the integrity of configuration information and to provide a basis for the control of change all configuration information must be listed in an approved IED Application Guide and stored in a corporate quality record system, e.g. DARTS, HPRM, SAP, Vault etc.

7.3.1 IED Application Guides

IED Application Guides detail how IEDs are used and configured within the Ausgrid network. This includes references to the standard designs, where the IED has been used, Configuration Baselines, IED Base Configurations and detailed setting descriptions.

IED Application Guides are to be stored in HPRM.

7.4 Change Control

After the initial release of configuration information all changes must be controlled to ensure integrity and traceability.

The process for controlling changes must be documented. The process should include requirements for revision numbering, descriptions of changes and their justification.

Changes must be managed though an approved corporate quality system, e.g. DARTS, HPRM, SAP etc.

8.0 RECORDKEEPING

The table below identifies the types of records relating to the process, their storage location and retention period.

Table 1 Recordkeeping

Type of Record	Storage Location	Retention Period*
Approved copy of the network standard	BMS Network sub process Standard – Company	Unlimited
Draft Copies of the network standard during amendment/creation	HPRM Work Folder for Network Standards (HPRM ref. 2014/21250/250)	Unlimited
Working documents (emails, memos, impact assessment reports, etc.)	HPRM Work Folder for Network Standards (HPRM ref. 2014/21250/250)	Unlimited

* The following retention periods are subject to change eg if the records are required for legal matters or legislative changes. Before disposal, retention periods should be checked and authorised by the Records Manager.

9.0 DOCUMENT CONTROL

Content Coordinator : Manager - Secondary Systems

Distribution Coordinator : Senior Engineer – Guidelines, Polices and Standards

Annexure A – Sample Compliance Checklist

Network Standard Checklist Form

NS273 Secondary Systems Configuration Management

Project Identification:	
Prepared by: <Name & Position Title>	Date:

This checklist is for internal Ausgrid use only and does not apply to ASPs or contractors who have specific compliance requirements in relation to Contestable project works. The checklist is unique for each network standard and is available within BALIN and the BMS as a separate form that can be amended as required, completed and saved in HPRM with the other project documentation.

This section is used to identify compliance checks that when applied to the work associated with this Network Standard will satisfy an audit process to establish that the requirements of the standard have been followed. It is expected that applicable items would normally be checked as Comply (Yes) as non-compliance is generally not tolerated.

Where non-compliance is the result of specific site conditions or design decisions this needs to be identified in the notes section of the form for each non-compliance and approval sought from an appropriately authorised Ausgrid manager responsible for design approval.

Should additional information be available to document non-compliance decisions, these can be attached to the checklist form. The checklist and any attached explanatory notes should be saved in the project document repository.

Item	Description	Refer clause	Completed/ Actioned
	Scope		
	This standard specifies Ausgrid's requirements for the configuration management of secondary systems assets		
	Configuration Baselines		
1	Approved hardware, firmware & software recorded in IED Application Guide	7.1.1	Yes/No/NA
2	Approved IED functions / elements recorded in IED Application Guide	7.1.2	Yes/No/NA
3	Standard Template Schematic(s) produced in CAD format with a unique drawing number or contained in a relevant Network Standard	7.1.3	Yes/No/NA
4	IED Base Configuration(s) produced for each unique application	7.1.4	Yes/No/NA
5	IED Base Configuration(s) assigned an appropriate name & revision numbering & listed in the IED Application Guide		
6	IED Application Guide stored in corporate record management system	7.3.1	Yes/No/NA
	Site Specific Configurations		
7	Site Specific Design Schematics produced	7.2.1	Yes/No/NA

8	RTIs reference appropriate IED Base Configuration(s) & Site Specific Setting Files	7.2.2	Yes/No/NA
9	Site Specific Setting Files produced in accordance with requirements	7.2.3	Yes/No/NA
10	Site Specific Setting Files stored against the appropriate IED device in the corporate quality system	7.2.3	Yes/No/NA

Notes: ……

……

……

……

……