Asset Management Plan

SCADA and Automation - Transmission

Record Number: R628073

Version Number: 5

Date: October 2022

Authorisations

Action	Name and title	Date
Prepared by		29/09/2022
Reviewed by		05/10/2022
Authorised by		12/10/2022
Review cycle	30 months	

Responsibilities

This document is the responsibility of the Asset Strategy and Performance Team, Tasmanian Networks Pty Ltd, ABN 24 167 357 299 (hereafter referred to as "TasNetworks").

The approval of this document is the responsibility of the General Manager, Strategic Asset Management.

Please contact the Substation Strategy Team Leader with any queries or suggestions.

- Implementation All TasNetworks staff and contractors.
- Compliance All group managers.

© Tasmanian Networks Pty Ltd 2014

Disclaimer

UNCONTROLLED WHEN PRINTED

This document has been prepared and made available solely for information purposes. While care was taken in the preparation of the information in this document, and it is provided in good faith, TasNetworks make no representation or warranty (express or implied) as to the accuracy, reliability, or completeness of the information contained in this document, or its suitability for any intended purpose.

TasNetworks (which for the purposes of this disclaimer, includes all their related bodies corporate, officers, employees, contractors, agents and consultants, and those of their bodies corporate) shall have no liability for any loss or damage (including without limitation, liability to any person by reason of negligence or negligent misstatement) for any statements, opinions, information or matter (expressed or implied) arising out of, contained in, or derived from, or for any omissions from, the information in this document, except to the extent that liability under any applicable statute cannot be excluded.

In all cases, anyone proposing to rely on or use the information in this document should independently verify and check the accuracy, completeness, reliability and suitability of that information and the reports and other information relied on by TasNetworks in preparing this document, and should obtain independent and specific advice from appropriate experts or other sources.

Reference Documents

R954721 – TasNetworks Strategic Asset Management Plan

R40766 – TasNetworks Asset Management Policy

R909655 – TasNetworks Risk Management Framework

Record of revisions

Section number	Details
	New format

Table of contents

1 Purpose

The purpose of this document is to describe for Transmission Supervisor Control and Data Acquisition (**SCADA**) and automation equipment and related assets:

- TasNetworks' approach to asset management, as reflected through its legislative and regulatory obligations and strategic plans;
- the key projects and programs underpinning its activities; and
- forecasts for capital (**Capex**) and operational (**Opex**) investment, including the basis upon which these forecasts are derived.

2 Scope

This document covers the SCADA and automation systems and associated strategic devices installed within TasNetworks' Transmission substations. It does not cover the primary assets protected or the protection assets, however, it will cover the linkages to the protection assets where appropriate.

This Asset Management Plan does not cover the telecommunications equipment used to transmit the data from the substations to the network control centres or the equipment within the network control centres.

3 Management strategy and objectives

This asset management plan has been developed to align with both TasNetworks' Asset Management Policy, Strategic Asset Management Plan and Strategic Objectives. This management plan describes the asset management strategies and programs undertaken to manage the SCADA and automation equipment.

The asset management objectives are to:

- manage and meet the strategic goals, measures and initiatives outlined in the TasNetworks Business Plan;
- comply with relevant legislation, licences, codes of practice, and industry standards; and
- continually adapt, benchmark, improve asset management strategies and practices, and apply contemporary asset management techniques, consistent with industry best practices.

4 Description of the asset portfolio

TasNetworks owns and operates 110 kV and 220 kV transmission network and associated substation assets and is required to meet Australian Energy Regulator (**AER**) National Electricity Rules (**NER**) and Australian Energy Market Operator (**AEMO**) standards, specifically for SCADA and automation systems, which includes:

- AEMO data and communications standard;
- AEMO power system security guidelines (Chapters 13, 14 and 16);
- NER sections 4.11.1 Remote control and monitoring devices;
- NER sections 4.11.2 Operational control and indication communication facilities; and
- NER rule clause 4 .11.1(d) provision of remote monitoring equipment.

SCADA and automation systems provide real-time data to monitor the primary equipment within a station and allow a centralised view of the operation and health of the entire transmission

network. SCADA and automation systems provide remote control, keeping personnel out of the substations for safer operation of the primary equipment.

Automation systems are also used for automatic operational sequences to rapidly maintain a secure operating state of power supply following system contingency events. With transmission system faults reported to a centralised area in real-time, allowing easier and more accurate fault analysis ensures faster transmission system restoration.

Modern protection equipment provides more information than previous generation equipment, relying extensively on the SCADA and automation system to transport the information to a centralised area for processing. The reliability of the SCADA and automation systems are more critical now, as TasNetworks does not routinely test modern protection relays/schemes and totally relies on these communications to ensure the protection systems are healthy.

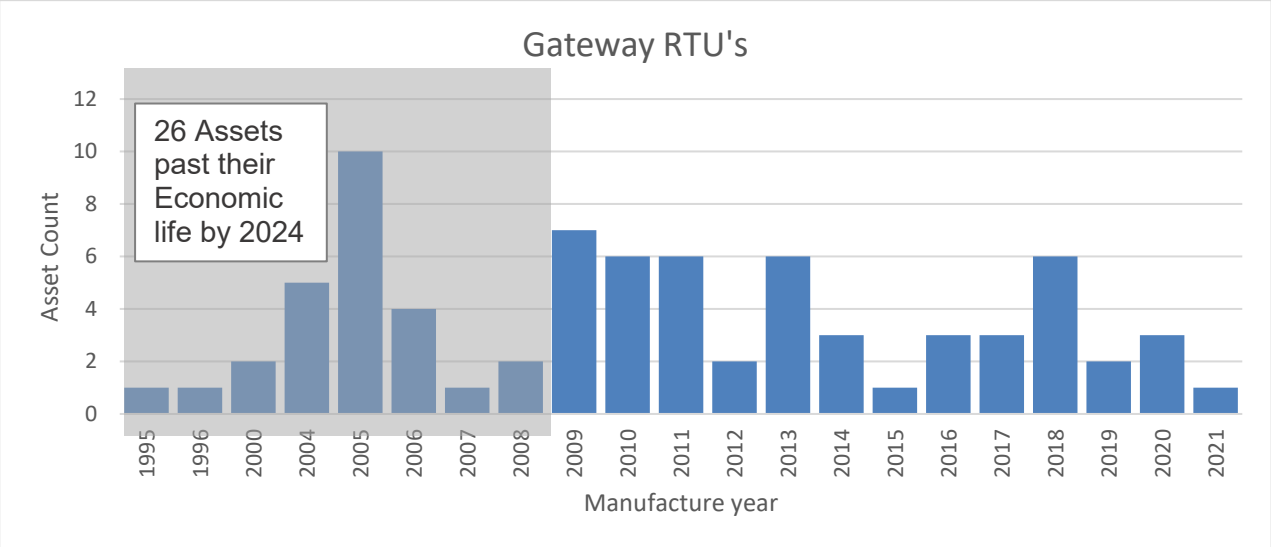
The SCADA and automation systems also provide a number of other critical functions required to operate the transmission network, such as remote access of protection relays, Remote Terminal Units (**RTUs**) and Ethernet switches, online condition monitoring of expensive primary assets, event extraction from system disturbances, and power quality records.

The drivers behind these programs are various and relate to:

- age;
- condition;
- in-service failure;
- cyber security enhancements;
- replacement based on obsolescence/diminished product support;
- spares management and maintainability;
- network performance improvement; and
- TasNetworks' strategic objectives such as, intelligent asset management and better customer services.

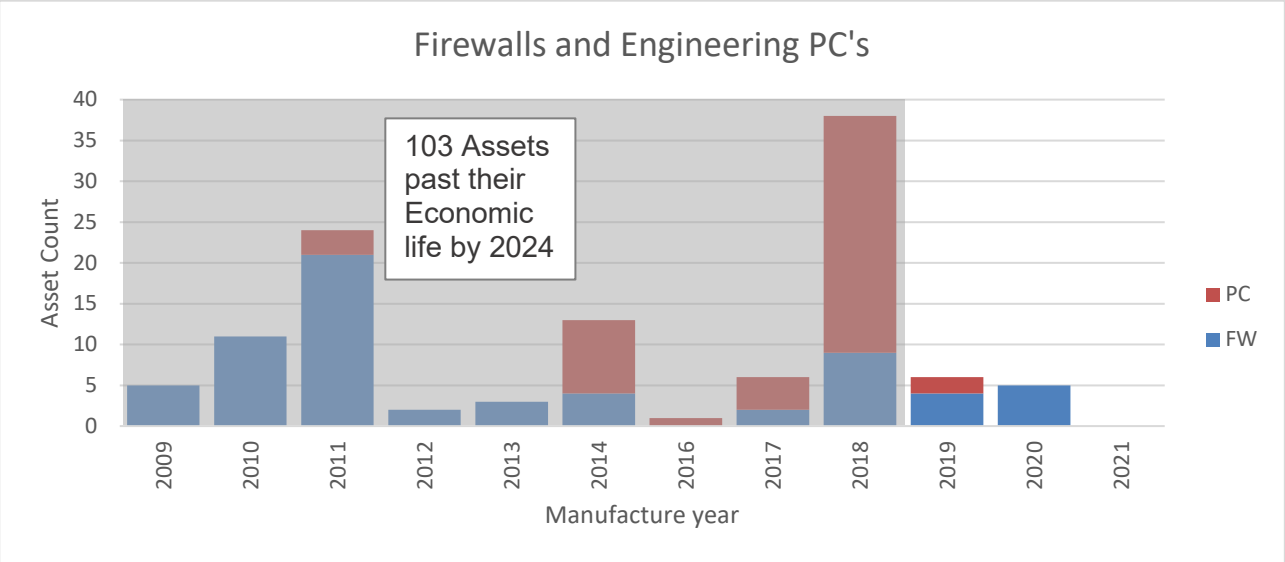
The economic lives of TasNetworks' assets are sourced from the TasNetworks Regulated Asset Base. In the case of SCADA network control and protection systems, this equates to 15 years.

The Gateway RTUs use Ethernet and serial interfaces for networking (i.e. data gathering and data control) with intelligent devices within the substation such as protection relays, automatic voltage regulators and power quality meters, etc. The Gateway RTU is the boundary between the substation intelligent equipment and the Network Operations Control System (**NOCS**).



Data coming to the substation is considered as untrusted data, as per TasNetworks' cyber standards. Therefore, a firewall (**FW**) is installed on each path into the substation to protect the data coming into the substation SCADA and automation networks.

An Engineering Personal Computer (**PC**) is a standard industrial PC with a standard operating platform (i.e. Windows 2010). When these PCs are also used by operational personnel to monitor and control the substation locally they are also referred to as the human machine interface (**HMI**).



Note: The firewalls and engineering pc's have an economic life of 5 years.

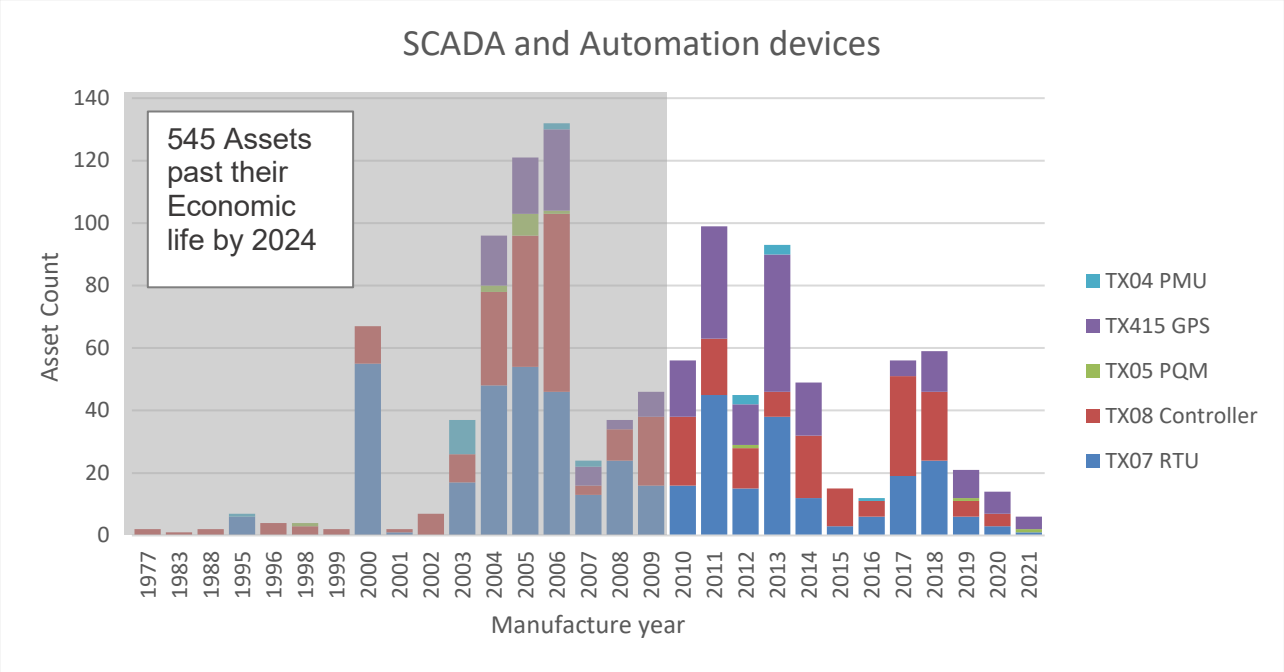
Power quality meters (**PQM**) provide digital fault recording, system disturbance monitoring and continuous fault recording.

The Phasor Measurement Unit (**PMU**) provides Synchro-phasor measurements used for state estimating tools and network-wide disturbance studies.

Data communications devices are the hardware used to transmit data or receive data, between intelligent electronic devices, which make up the majority of SCADA and automation components.

Controllers can either be a bay controller for a specific bay control and/or an automatic voltage regulator on a transformer to provide voltage control. Some of the control functions are contained within a bay level RTU (excludes Gateway RTUs).

Global Positioning System (**GPS**) are used to for time synchronisation at each substation for devices to provide correct protection operations and accurate sequence of events.



5 Associated risk

5.1 Risk Management Framework

TasNetworks has developed a Risk Management Framework for the purposes of assessing and managing its business risks, and for ensuring a consistent and structured approach for the management of risk is applied.

An assessment of the risks associated with the SCADA and automation devices have been undertaken in accordance with the Risk Management Framework.

The quantification of risk is supported by the Health Based Risk Management (**HBRM**) framework. This approach allows the risks of individual assets to be quantified against the defined assessment.

Due to the level of risk identified in some of the assessment criteria, a requirement to actively manage these risks has been identified.

5.2 Performance data

TasNetworks monitors equipment performance by recording a defect notification against the equipment record in the SAP Enterprise Asset Management system. These records can be categorised by recording the symptom of the defect such as non-operation or incorrect operation, the cause, such as hardware failure, incorrect settings, or manufacturing deficiency, the source of finding the defect, such as during routine maintenance, corrective maintenance, or equipment commissioning. These attributes allow reporting and Key Performance Indicators (**KPI**) for the consequences and causes of device asset failure, and the effectiveness of our maintenance strategies.

TasNetworks' asset strategy engineers are currently working with field services technicians to improve the quality of the defect data, as it often requires interpretation and more detailed investigation to ascertain the causes and consequences of device failures. The end goal is to provide "dashboard" reporting for fast assessment by all stakeholders involved in the management and maintenance of the distribution protection assets. Since SAP has been,

implemented, the current reporting, as shown in the table below, shows these failures have remained steady.

Year	18/19	19/20	20/21	21/22
Devices failures	56	62	50	55

Note: these device failures don't include device power cycles, software upgrades, power system requirement changes etc.

Current assessment from the asset data shows if no planned replacements are completed in the R24 revenue period the failure rates will increase. TasNetworks is trying to maintain or lower these failure rates and reduce the cyber security risks while maintaining customer satisfaction.

SCADA system compliance of rules and regulations includes:

- Gateway RTU's are required to meet the AEMO data and communications standards which specifies 99.9543 per cent availability for SCADA and Automation systems, which equates to a four hour outage per annum per site.
- TasNetworks has a number of direct connections to major industrial customers through Extra High Voltage (**EHV**) and High Voltage (**HV**) substations. The individual connection agreements describe the level of service and performance obligations required from the associated connection assets. Failure to meet these agreements will have a financial impact and reputational effects on TasNetworks.

5.2.1 Gateway RTUs

A failed gateway RTU will lead to network operations having no visibility of parts of the network, requiring AEMO to apply constrains to the network (due to no power flow information or remote control should action be required) which will affect customers and lose data for power system analysis. An increase in failed gateway RTUs leads to an increase in costs, environmental and safety risk from operators having to drive to site and man the substation 24/7 to provide network operations until the asset is repaired or replaced. Any substation operations required when the RTU is failed will increase the risk of injury by placing operators in close proximity to EHV equipment, which may cause a safety issue if there is a failure of the primary equipment.

AEMO can potentially fine TasNetworks or restrict its operating license should TasNetworks continually fail to meet the AEMO data and communications standard, that calls for 99.9543 per cent availability for SCADA and automation systems, which allows for a four hour outage per annum.

Another consequence associated with gateway RTUs arises when dedicated spares have fully depleted and manufacturer support has ceased, which also increases cyber security risks as vulnerabilities are identified. Rectifying a failed gateway RTU without dedicated spares requires re-configuration and modifications to the design, re-wiring of the SCADA panel, and re-commissioning of the SCADA system. If this work is performed under emergency conditions, the risk of introducing errors in the installation increase. Additionally, these re-design tasks may require a higher level of engineering skills that may not be available in the short timeframe. The consequence of this rushed and potentially inaccurate installation may lead to poor performance of the new SCADA equipment that impacts the network performance and service to customers. Additionally, when higher skilled resources are required at short timeframes, higher costs are incurred.

Having old or obsolete secondary equipment increases TasNetworks' cyber security risks that could result in operational impacts to TasNetworks including, but not limited to, data breach and loss of control.

5.2.2 Substation firewalls and engineering PCs

Over time, having equipment with unsupported operating software i.e. having out of date operating systems on firewalls and engineering PCs will increase TasNetworks' cyber vulnerabilities and doesn't align with internal cyber standards, North American Electric Reliability Corporation Critical Infrastructure Protection (**NERC CIP**), Australian Cyber Security Centre Essential Eight (**ACSC E8**) and doesn't follow good industry practice. A software vulnerability is a security weakness found in a software program or operating system. Hackers can take advantage of the weakness by writing code to target the vulnerability. Malicious software in these devices has the potential to affect power system security, non-conformity with AER compliance obligations and AEMO operating standards, increasing customer outage times and significate cost to TasNetworks operational costs and a ransom cost to remove the malware.

Engineering PCs will only be used remotely for uploading fault records, viewing the status of protection relays and the SCADA network, extracting protection setting information, performing a software reset of applicable devices, and will not be used for firmware updates and/or settings changes without specific approval.

5.2.3 SCADA and automation equipment

SCADA and automation equipment are electronic devices that will eventually fail in-service at an undefined time. This equipment is used by TasNetworks to meet NER rule compliance and not meeting this has a potential financial cost to TasNetworks and possibility of power system constraints, which can affect customers.

The equipment is rotable, such that when a failure occurs, a direct replacement spare is used to restore the SCADA and automation services, the failed equipment is sent back to the manufacturer for repair and then returned to the spares store to support the rest of the in-service equipment of that model. The SCADA and automation equipment is constantly monitored by the NOCS and will alarm when failed, and TasNetworks provides regional maintenance teams 24/7, so failure of the SCADA and automation service is mostly only out of service for up to 48 hours.

The risk identified to TasNetworks' SCADA and automation equipment is when these devices are unable to be maintained under the normal processes described above. This occurs once the equipment manufacturer ceases support and failures leads to a depletion of dedicated spares. Once dedicated spares have fully depleted, a failure will require a different model of device to be installed in place of the failed device. This requires re-configuration of settings, modifications to design drawings, re-wiring of the panel, and re-commissioning that part of the SCADA system. If this work is performed under emergency conditions, the risk of introducing errors in the installation increase. Additionally, these re-design tasks may require a higher level of engineering skills that may not be available in the short timeframe.

The rushed and potentially inaccurate installation may lead to poor performance of the new SCADA and automation equipment that impacts the network performance and service to customers. Additionally, when higher skilled resources are required at short timeframes, higher costs are incurred.

Although this is a low level consideration due to the critical purpose of SCADA and automation equipment within a power network, if the SCADA and automation equipment was not being

maintained and was left in a failed state, the risk would be the inability to provide remote control of circuit breakers, isolators, correct monitoring information and compliance with the NER that govern the requirement to monitor the transmission network. Due to this statement, the risk of not maintaining SCADA and automation schemes in substations is medium and requires capital investment to mitigate that risk.

Risk Identification		**Risk Analysis**				
Asset	**Risk Description**	**Category**	**Likelihood**	**Consequence**	**Risk Rank**	**Treatment Plan Yes / No**
Gateway RTUs	Loss of gateway RTUs from remote stations will cease remote control and monitoring of the substations. This may result in sub-standard power system constraints on the network and potentially a financial penalty, increasing the risk to field crews, having to locally operate EHV equipment. Requiring the substation to be 24/7 manned increasing cost to TasNetworks and, in turn, customers. A non-conformance may also be issued due to TasNetworks not meeting AEMO data and communication standard, and AER rules 4.11.1 Remote control and monitoring device; and NER sections 4.11.2 Operational control and indication communication facilities increasing network performance and regulatory compliance.	Safety and People	Rare	Major	Medium	Yes
		Financial	Rare	Moderate	Low	
		Customer	Rare	Moderate	Low	
		Regulatory Compliance	Unlikely	Moderate	Medium	
		Network Performance	Unlikely	Moderate	Medium	
		Reputation	Rare	Minor	Low	
		Environment & Community	Rare	Minor	Low	
Substation firewalls	Having devices of this age with no manufacturer support (i.e. software patches) will increase TasNetworks' cyber security risk and has the potential for a hacker to take control of our network causing incorrect network operations and major customer/s impact to supply. Not upgrading will be indirect conflict with internal cyber standard, and not align to NERC CIP, ACSC E8 and does not follow good industry practice.	Safety and People	Rare	Major	Medium	Yes
		Financial	Rare	Moderate	Low	
		Customer	Rare	Moderate	Low	
		Regulatory Compliance	Unlikely	Moderate	Medium	
		Network Performance	Unlikely	Moderate	Medium	
		Reputation	Rare	Minor	Low	

Risk Identification		**Risk Analysis**				
Asset	**Risk Description**	**Category**	**Likelihood**	**Consequence**	**Risk Rank**	**Treatment Plan Yes / No**
		Environment & Community	Rare	Minor	Low	
Engineering PCs	Having devices of this age with no manufacturer support (i.e. software patches) will increase TasNetworks' cyber security risk and has the potential for a hacker to change setting in protection relay gateway RTU's etc. causing no or incorrect network operations and major customer/s impact to supply. Not upgrading will be indirect conflict with TasNetworks' regulatory obligations, increase return to service times due to having to drive to site, and increase risk of operational staff having to locally operate primary equipment putting themselves at a safety risk.	Safety and People	Rare	Major	Medium	Yes
		Financial	Rare	Moderate	Low	
		Customer	Rare	Moderate	Low	
		Regulatory Compliance	Rare	Moderate	Low	
		Network Performance	Unlikely	Moderate	Medium	
		Reputation	Rare	Minor	Low	
		Environment & Community	Rare	Minor	Low	
Other SCADA and automation equipment	Loss of other SCADA and automation devices will prevent network operations to plan and manage network operations correctly. Failure of SCADA and automation devices that provide high speed data to the real time state estimator to optimise the network performance. Controllers prevent some parts of the substation to be not monitored and controllable potentially putting network constraints on parts of the network and unlikely putting operational staff at risk during some operations of equipment.	Financial	Rare	Moderate	Low	Yes
		Customer	Rare	Moderate	Low	
		Regulatory Compliance	Rare	Minor	Low	
		Network Performance	Rare	Moderate	Low	
		Reputation	Rare	Moderate	Low	

Risk Identification		**Risk Analysis**				
Asset	**Risk Description**	**Category**	**Likelihood**	**Consequence**	**Risk Rank**	**Treatment Plan Yes / No**
	After a system fault, TasNetworks needs data from SCADA and automation devices to provide a report to AEMO and/or AER, and not having this data will see the business potentially issued with a fine.	Environment & Community	Rare	Severe	Medium	

6 Whole of life management plan

6.1 Preventive and corrective maintenance (Opex)

6.1.1 Non-routine, corrective maintenance

Corrective maintenance of transmission SCADA and automation is in line with the RIN reporting categories. This program covers SCADA and automation equipment failures at transmission substations: items such as gateway RTUs, Ethernet switches, engineering PCs, bay controllers, automatic voltage regulators, data communication devices, power quality meters, phasor data concentrators, phasor measuring units and Global Positioning System clocks.

The process to rectify a failed SCADA and automation device is to remove the failed device and replace it with an identical spare. When a microprocessor device locks up or communications error occur, similar to a “frozen” computer, a software shut down-cycle is attempted first which usually rectifies the lockup. If the lockup continues, the power-cycle is attempted, however if the lock up continues the microprocessor device is replaced with a spare.

The replaced devices will be replaced firstly with a like-for-like spare, which should be able to be achieved if the spares policy is followed. However, if these spares are not available from the TasNetworks store then the latest standard devices will be used, as per the transmission SCADA and automation standard.

For all SCADA and automation equipment in this part of the network a patching processes may be required and will be a risk based approach following Substation Asset Strategy Engineer risk identifications process. Industry standard indicates patching high risk operational assets such as gateway RTUs, engineering PCs (**HMIs**) and substation firewalls once per year should be considered. This will increase the operational cost over the R24 regulatory control period.

6.1.2 Routine maintenance

SCADA and automation systems have not previously had dedicated routine maintenance programs. The SCADA and automation system are tested during protection routine testing as the alarms and events are checked back to the NCOS. A recent strategy change to the protection routine testing has seen a decrease in this testing. With an increase in cyber-attacks on businesses, the Australian Department of Home Affairs and AEMO have provided guidance on best practice for power utilities, which indicates some form of risk assessment and potentially routine work (outlined below) on these assets may be required.

For R24 a new functional area has been created for this routine maintenance in line with the RIN reporting categories and this program covers all secondary assets within transmission substations, including protection relays.

With increasing cyber security attacks on Australian based companies, to help mitigate these threats the SCADA and automation routine maintenance program will include:

- Performing vulnerability assessments of secondary assets;
- Reviewing and updating access privileges to substation operational technology, to ensure validity, every 12 months;
- Audits of asset inventory will be manually spot-checked every 12 months;
- Logging requirements from gateway RTUs, firewalls and engineering PCs will be continually monitored and reviewed, with reporting every three months to the Asset Strategy team and Substation Asset Strategy Engineer;

- Indicators of anomalous activity will be defined and monitored across the operational environment. Continuous monitoring will be performed across the operational environment to identify anomalous activity, with reviews and reports every three months to the Asset Strategy team and Substation Asset Strategy Engineer;
- A complete and current register of identities (users) with privileged access will be maintained and checked every 12 months with review and reporting every 12 months to the Asset Strategy team and Substation Asset Strategy Engineer;
- Asset data is stored in SAP with the software settings stored in StationWare. New products installed will use baseline templates which include all required cyber security settings. Baselines and templates are reviewed and updated every six months with any changes to baselines tested prior to deployment and all changes logged in StationWare;
- Having this program will reduce the cyber security risk to TasNetworks but having to meet the legislation requirement will increase the cost to TasNetworks for the five year R24 regulatory period; and
- For all SCADA and automation equipment a patching process may be required following a risk assessment from a Substation Asset Strategy Engineer. Industry standard indicates patching high risk operational assets such as gateways, engineering pcs and substation firewalls once per year should be considered. This will increase the operational cost over the R24 regulator period.

Table 2: Summary of programs and risks – OPEX

Project/ Program	Func. Area	Program Data									
		Financial year	FY20	FY21	FY22	FY23	FY24	FY25	FY26	FY27	FY28	FY29
Non Routine - maintenance	CMPSS	Expenditure ($m)	0.21	0.32	0.32	0.32	0.42	0.45	0.45	0.45	0.45	0.45
Routine maintenance of devices	PSCPC	Expenditure ($m)	0.01	0.12	0.0	0.0	0.13	0.13	0.13	0.13	0.13	0.13

6.2 Reliability and quality maintained (Capex)

6.2.1 Planned renewal of gateway RTUs

This program is focused on substation gateway RTUs (including site Ethernet switches) only, with projects at selected sites based on network site criticality, equipment age, spares availability, and hardware and software support availability from the manufacturer.

The gateway RTUs being replaced must be older than 15 years of age and they must be no longer supported by the manufacturer. Approved equipment, as identified in the TasNetworks standards, must be used along with the approved TasNetworks software applications.

Updating this equipment will move TasNetworks towards its business objectives, by implementing IEC 61850 and cyber security technology in existing and new substations, which includes:

- Network climate change resilience and adaptation strategy by reducing our environmental footprint through reduced control building size, less cabling and cable trays, etc.;
- Moving towards a digital future/digital strategy, data driven decisions, faster return to service times and skills of the future;

- Cyber security strategy, improved cyber security threats, alerts and monitoring;
- Network operations systems strategy for improving the visibility and modelling of the network to identify areas for improvement; and
- Alignment of technology including cyber security with other distribution network service providers and transmission network service providers.

Any new secondary device must have installed TasNetworks' (cyber security) baseline configuration that will align to TasNetworks' internal cyber standards and good industry practice.

6.2.2 Planned renewal of firewalls and engineering PCs

This equipment includes substation firewalls and engineering PCs only, with projects at selected sites based on equipment age, spares availability, and hardware and software support availability from the manufacturer that limits TasNetworks' ability to maintain site security to an acceptable standard.

The firewalls and engineering PCs being replace must be older than five years of age and have hardware or software that is no longer supported by the manufacturer. Each site renewal must use approved baseline configurations aligning to TasNetworks' internal cyber standards, aligning with NERC CIP, ACSC E8, and good industry practices. The outcome of this program is expected to see an improvement in equipment technology that will reduce cyber security risks, and a reduction in asset failures of engineering PCs and firewalls that will reduce opex costs and improve network performance.

6.2.3 Renewal of other SCADA and automation equipment

The latest renewal strategy is for TasNetworks to adopt the planned 'just in time' renewal of obsolete SCADA and automation equipment, where equipment is mined from the field to maintain sufficient quantities of spares for the remainder of the commissioned equipment model. This mining will continue until the obsolete model of equipment is fully removed from the network to the latest standard models.

The intent of this planned 'just in time' renewal strategy is to remove some of the youngest of the equipment model from the field to replenish spares quantities for ongoing maintenance of the rest of the asset fleet.

Based on historical failure rates of equipment, as defined in the RIN, which has shown an average of 60 replaced assets per annum for the last three years, and this will increase based on the age of the rest of the equipment.

If spares for certain devices reach 30 per cent or less the manufacturer of that equipment will be contacted if a new model of that device is available, and if this is the case, then a like-for-like replacement will be used. However, if a direct replacement is not available, then a standard device must be used as confirmed by the Substation Asset Strategy Engineer. Foxboro devices are an exception to this rule, as Foxboro gateway RTUs will be replaced with Cooper gateway RTUs and for Foxboro bay controllers will be replaced with TasNetworks' standard Siemens bay controllers.

The new strategy for renewal of SCADA and automation equipment has been in place since the start of 2019, which involves monitoring the availability of dedicated spares of obsolete equipment and undertaking planned replacements to replenish spares to enable the ongoing maintenance of future equipment failures.

6.2.4 Transmission SCADA and automation augmentation

Where new SCADA and automation equipment is installed in the network due to network augmentation, TasNetworks provide standard designs and standard equipment to ensure that TasNetworks' maintenance teams are able to manage spares and maintenance procedures. Where standard designs are not available, the last installation should be used as a template design.

6.2.5 Details of future capex projects/programs

Table 3: Program/project details

Project/Program description	Functional area	Link to Copperleaf
Renewal of Gateway RTU's, FW and engineering PC's	RENSC	https://tasnetworks.c55.copperleaf.cloud/PROD/Modules/Expenditures/Expenditure.aspx?id=50115
Planned just in time replacement	RENSC	https://tasnetworks.c55.copperleaf.cloud/PROD/Modules/Expenditures/Expenditure.aspx?id=50116

6.3 Spares management

Sufficient spares are required to be maintained within the northern and southern regions of Tasmania, to enable replacement relays to be installed within the restoration times defined in the AEMO operating procedures.

Spares are to be kept at an 8:1 in-service to spares ratio, based on region (either north or south), to a maximum of three of each type per region.

Devices are to be kept as compete units, together with sufficient replacement parts to meet all credible contingencies.

If a project introduces a relay of unique design to the system, or increases the quantity of a given relay type beyond the maximum 8:1 ratio, additional devices shall be purchased as a part of that project to enable the quantity of spares on hand to remain compliant with this policy.

6.4 End of life management

The latest renewal strategy is also intended to provide full utilisation of the SCADA and automation equipment by only disposing of a relay once it fails and cannot be repaired. Once the relay cannot be repaired, it is disposed of by sending the relay to e-waste with TasNetworks' IT equipment.

7 Related standards and documentation

The following documents have been used in the development of this asset management plan, or provide supporting information.

Description
TasNetworks Towards 2030
TasNetworks Corporate Plan
TasNetworks Business Plan
TasNetworks Risk Management Framework
National Electricity Rules (NER)
Cyber Aust Gov essential eight maturity model
Tas economic regulator codes
Power System Security Guidelines (aemo.com.au)
Power System Data Communications Standard - FINAL (aemo.com.au)