



Asset Management Plan

Network Operations

Record Number: R299400

Version Number: 1.2

Date: November 2022

Authorisations

Action	Name and title	Date
Prepared by		25/11/2022
Reviewed by		3/12/2022
Authorised by		12/12/2022
Review cycle	5 Years	

Responsibilities

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

Please contact the Network Operations Leader with any queries or suggestions.

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

© Tasmanian Networks Pty Ltd 2022

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.

Record of revisions

Ver	Details	Name
1	New Document	
1.1	Updated for R19	
1.2	Major update incorporating R24	

Table of Contents

Authorisations.....	2
Responsibilities	2
Disclaimer.....	2
1 Purpose.....	7
2 Scope	7
3 Management Strategy and Objectives.....	7
4 Description of the asset portfolio	8
4.1 Background	8
4.2 Assets	9
5 Changing Industry Requirements.....	11
6 Whole of life management plan	13
6.1 Selection criteria	13
6.2 Strategy (OPEX and CAPEX)	13
6.3 Proactive Monitoring.....	15
6.4 Reactive Monitoring	15
6.5 Defect Management	15
6.6 Technical Support	16
6.7 Triggering events for software and data updates	16
6.8 Spares management	16
6.1 Economic Life	16
6.2 End of life management.....	17
7 Asset Performance	17
7.1 NER and AEMO Compliance	17
7.2 NOCS Asset Condition Summary	17
7.3 System Protection Scheme (SPS).....	18
8 Risk	18
8.1 Business Risks.....	18
9 Financial Summary	19
9.1 OPEX Expenditure	19
9.2 CAPEX Expenditure	19
9.2.1 Investment evaluation.....	19
9.2.2 Recurrent Investment	21
9.2.3 Proposed Non-recurrent investment.....	22
10 Related Standards and Documentation	26

Glossary

ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AC	Alternating Current
AGC	Automatic Generator Control
AMP	Asset Management Plan
AUFLS	Adaptive Under Frequency Load Shedding
DC	Direct Current
DMS	Distribution Management System
DMZ	De-Militarised Zone
DOTS	Distribution Operator Training Simulator
DPF	Distribution Power Flow
DSA	Dynamic Stability Analysis
DSE	Distribution State Estimator
DSO	Distribution System Operator
EMS	Energy Management System
FCAS	Frequency Control Ancillary Services
FEP	Front-End Processor
FLISR	Fault Location, Isolation and Service Restoration
FPA	Fault Protection Analysis
GIS	Geographic Information System
GCS	Generator Contingency Scheme
IBR	Inverter Based Resources
ICCP	Inter-Company Communications Protocol
IP	Internet Protocol
IT&C	Information Technology and Communications
MMI	Man Machine
NAVS	Northern Automatic Voltage Scheme
NEM	National Electricity Market
NOCS	Network Operation and Control System
NWAVS	North-Western Automatic Voltage Scheme
OMS	Outage Management System
OTS	Operator Training Simulator
PABX	Private Automated Branch Exchange
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
RPSS	Residual Power System Security
SAVS	Southern Automatic Voltage Scheme
SCADA	Supervisory Control and Data Acquisition

SLA	Service Level Agreement
SML	SCADA Minutes Lost
SOM	Switch Order Management
SPS	System Protection Scheme
TADCS	Transmission and Distribution Control System
TDM	Time Division Multiplex
TESI	Tasmanian Electricity Supply Industry
TMR	Trunk Mobile Radio
TNOCS	Telecommunications Network Operation and Control System
TRCalc	Thermal Ratings Calculator
TSA	Transient Stability Analysis
VSA	Voltage Stability Analysis
VVC	Volt Var Control

1 Purpose

The purpose of this document is to describe the Asset Management Plan for the software and hardware assets of the Network Operations Control System (NOCS) which provide or support the operation of the Tasmanian power system.

2 Scope

This document covers only the Master Station platform, network data, software applications and hardware assets of the NOCS.

These software applications and network data fall into two broad categories:

- (i) Real time applications and network data residing within the protected control system domain; and
- (ii) Operations support applications and network data residing within the corporate IT domain.

This plan excludes the following:

- IT Infrastructure compute and storage;
- Operating System and SQL Server licensing;
- Telecommunications bearer and wide area networking;
- Desktop computers and telephones; and
- Substation SCADA and protection physical assets i.e. RTU and relays outside of the Network Operations Control System.

TasNetworks' Operational Systems are dependent on assets not included in this plan; these are identified here because of their criticality to this plan. They are:

- control centre buildings physical security;
- heating, lighting and ventilation (including air-conditioning systems);
- uninterruptible power supplies (UPS) and backup diesel generation;
- battery systems (primarily telecommunications);
- voice and data communications infrastructure;
- IT infrastructure – compute, storage and desktop;
- Smart Field Devices (reclosers, fuse savers, regulators etc); and
- RTUs and relays in TasNetworks' substations.

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 strategy and programs undertaken to manage the NOCS and associated systems.

The asset management objectives are to:

- present an overview and high level catalogue of the NOCS non-physical assets;
- manage and meet the strategic goals, measures and initiatives outlined in the TasNetworks Business Plan;
- achieve reliable system performance consistent with prescribed services standards;
- comply with relevant legislation, licenses, codes of practice and industry standards;

- achieve high system availability targets and disaster recovery objectives for critical systems;
- protect the NOCS non-physical assets from cyber security and other potential security threats;
- continually adapt, benchmark, improve asset management strategies and practices, and apply contemporary asset management techniques consistent with industry best practices; and
- define future operation and capital expenditure requirements of the systems.

4 Description of the asset portfolio

4.1 Background

TasNetworks owns and operates the electricity transmission and distribution network in Tasmania and is required to meet Australian Energy Regulatory (AER) National Electricity Rules (NER), Australian Energy Market Operator (AEMO) standards and local legislation, specifically for the Transmission and Distribution Control System (TADCS) this includes but not limited to:

- AEMO power system data communication standard;
- AEMO power system security guidelines;
- NER section 4.3 Power system security;
- NER section 4.5 Control of power system voltage
- NER section 4.9 Power system security relation market operations;
- NER section 4.11.1 Remote control and monitoring devices;
- NER section 4.11.2 Operational control and indication communication facilities
- NER section 4.15 Compliance with performance standards; and
- Tasmanian Electricity Code (TEC)

The primary components of the NOCS comprises of a SCADA master station, Energy Management System (EMS), Distribution Management System (DMS), and Outage Management System (OMS), encompassing hardware and proprietary software from core industry vendors. The NOCS is designed to provide uninterrupted service to both Transmission and Distribution operations as well as the interfaces to AEMO and Tasmanian market participants. Connections to AEMO and Hydro Tasmania (ICCP links), data communications (provided under Telecommunications Bearer Network AMP (R0000032671) to remote assets are key components of the NOCS and centralised protection and control Schemes.



This SCADA platform was commissioned in 2002 to manage the complexity of the Tasmanian transmission system and its interconnection to Victoria. In 2014, it was expanded to perform distribution network monitoring and control functions when TasNetworks formed to own and operate both the transmission and distribution networks in Tasmania. Additionally, in 2019 the platform was further expanded to implement DMS functionality to support TasNetworks transformation roadmap 2025.

4.2 Assets

[REDACTED]. The most recent upgrade of the core software platform was conducted in October 2021. In addition to updates to the software described here, system size and license increases are required to support the Network Program of Work (PoW), along with hardware upgrades to ensure reliable and performant operation. The NOCS is an operational system utilising, where applicable, commodity hardware. The design, configuration and lifecycle management of these assets are to align with the operating philosophy of the NOCS.

At a high level the assets consist of:

[REDACTED]

- **Energy Management System (EMS).** Comprising:
 - the EHV transmission network, load and generation data models specifying the connectivity and electrical parameters required to simulate the transmission system in real-time.; and
 - the real-time network analysis software utilised for on-line security analysis, short-term operations planning and on-line engineering studies. Features include:
 - network topology processor;
 - power flow and state estimation;
 - contingency analysis;
 - short circuit analysis;
 - automatic generator control;
 - voltage stability; and
 - available transfer capacity.
- **Distribution Management (DMS).** Comprising:
 - the HV and LV distribution network, load and generation data models specifying the connectivity and electrical parameters required to simulate the distribution system in real-time; and
 - the real-time network analysis software utilised for on-line switching analysis, outage planning, and on-line engineering studies. Features include:
 - network topology processor;
 - power flow and state estimation;
 - short circuit analysis;
 - load drop analysis;
 - protection reach analysis; and
 - safety pre-operational check analysis.
 - Fault Location, Isolation and Service Restoration (FLISR). Automation software to detect faults on the distribution network and rapidly restore power to customers.
- **Switch Order Management (SOM).** Software to efficiently manage the request, writing, validation, and execution of switching steps required to remove electrical plant from service. This includes analysis to support the due regard for safety, customer service and network reliability on both the transmission and distribution networks.
- **Outage Management System (OMS).** Software utilising the DMS network model to manage outage calls from customers, predict location of outages and manage customer notifications;

- **Historian, data analysis and reporting.** [REDACTED]
[REDACTED] Historical data and analysis tooling is provided to users via a number of web applications and reporting tools accessed via both the corporate and secure control system networks.
- **Logging.** Electronic logging facilities have been implemented for both Distribution and Transmission Control Rooms.
- **Custom applications, control and protection schemes.** To manage system security issues, improve network utilisation, and manage contingent events a number of custom application and control schemes have been implemented. The significant applications include:
 - *TRCalc*: Dynamically calculate the thermal ratings of transmission lines;
 - *NWAVS, NAVS, SAVS*: Automation schemes which control generators, capacitor banks and transformers to manage voltage levels at key nodes within the transmission network;
 - *Residual Power System Security (RPSS) tools*: Suite of tools to assist in generator dispatch and secure management of the Tasmanian power system at the request of, or in the absence of, the market operator (AEMO). RPSS is a TasNetworks license obligation;
 - *Distribution protection suppression*: Suite of tools to suppress or re-instated substation and Smart Field Assets (SFA) protection for vegetation management and during periods of high fire risk;
 - *Generator and Load Contingency Schemes (GCS and FCSPS)*: Suite of protection schemes to manage the contingent loss of either loads or generators of sufficient size to breach the frequency operating standard
 - *Network Control System Protection Scheme (NCSPS)*: Protection scheme which enables significantly higher utilisation of key transmission lines. This scheme rapidly ramps down or disconnects generators after a contingent event to remove violations of terminal or thermal ratings of transmission lines;
 - *Anti-islanding and overload schemes*: Control schemes to disconnect generators or loads to remove electrical islands or overloads on key assets such as transformers;
 - *Adaptive Under Frequency Load Shedding (AUFLS)*: Control scheme to provide FCAS raise services by disconnecting loads at predefined rate of change of frequency or set frequency limits.
 - *DMS GIS interface*: Software to extract the distribution network from TasNetworks ESRI GIS Utility Network Model (UNM) [REDACTED].
 - *System strength dispatch*: Software to monitor the Tasmanian power system to ensure under normal conditions and pre-defined contingent events that there is sufficient system strength, as defined by AEMO system strength requirements. For short falls of either inertia of fault level, the software enables the economic dispatch of generators to resolve the detected system strength shortfall.
- **Training Simulators.** This is a key component of the competency assessment system for real time shift staff. The system simulates the power system as well as mimics the EMS, DMS and OMS platforms. It is used for:
 - training of new personnel on the use of the NOCS;
 - power system restoration and residual power system security exercises;
 - rotational load shedding;
 - scenario based exercises; and
 - test platform for core system upgrades and scheme development.

- **Synchrophasor data concentration and analysis.** This includes software to collect and analyse high speed data from Phasor Measurement Units (PMU). [REDACTED] This data is used for fault analysis, generator commissioning and detecting abnormal network operating conditions.
- **Cyber security and System management.** This includes end point protection and application white-listing, network monitoring, intrusion and abnormality detection software. Additionally, this also includes management and monitoring software to manage the IT infrastructure, applications and cyber security products.
- **Hardware.** This includes:
 - *Remote Terminal Units (RTUs):* Used for protocol conversion and data concentration for a small subset of Smart Field Devices;
 - *Teleprotection units:* Used to provide signalling for the various contingency and control schemes listed above;
 - *Network equipment:* This includes switches for the control system Local Area Networks as well as firewalls to segment and protect the control system;
 - *GPS clocks:* Used to provide millisecond time synchronisation as well as system frequency and time deviation measurements; and
 - Terminal servers: Utilised to connect RS232 or RS485 serial interfaces to an Internet Protocol (IP) network as required by the Front End Processor.

5 Changing Industry Requirements

In 2017, to facilitate the safe and secure operation of the power system with increasing levels of inverter based resources (IBR), the Australian Energy Market Commission (AEMC) created a framework and obligations for the management of system strength. These changes sought to provide system strength through the management of fault levels and inertia. TasNetworks implemented an innovative, although tactical solution to dispatch system strength services in 2020 enabling the power system to absorb additional IBR.

The Tasmanian Government’s Renewable Energy Target (TRET) and Renewable Energy Action Plan (TREAP) has set objectives to double the State’s renewable energy-based generation sector and become a major contributor to firming electricity supply across the NEM. The TRET also demonstrates Tasmania’s opportunity to become a leader in the emerging global renewable hydrogen industry with the Tasmanian Hydrogen Action Plan¹ citing a 1,000 MW hydrogen production facility supporting 2,000 MW of renewable generation.

The proposed 1,500 MW DC interconnector Marinus link, along with the supporting North West transmission development, will support Australia’s transition to variable renewable generation and pumped hydro energy storage within Tasmania.

The installed capacity of IBR, made up of PV generation (~173 MW at Sept. 2020), Basslink interconnector (500 MW export, 480 MW import), and wind generation (567.7 MW) is operational on a system with a long term demand minimum of 929 MW and maximum of 1522 MW, as per Table 1.

- Table 1 Tasmanian Demand (MW)

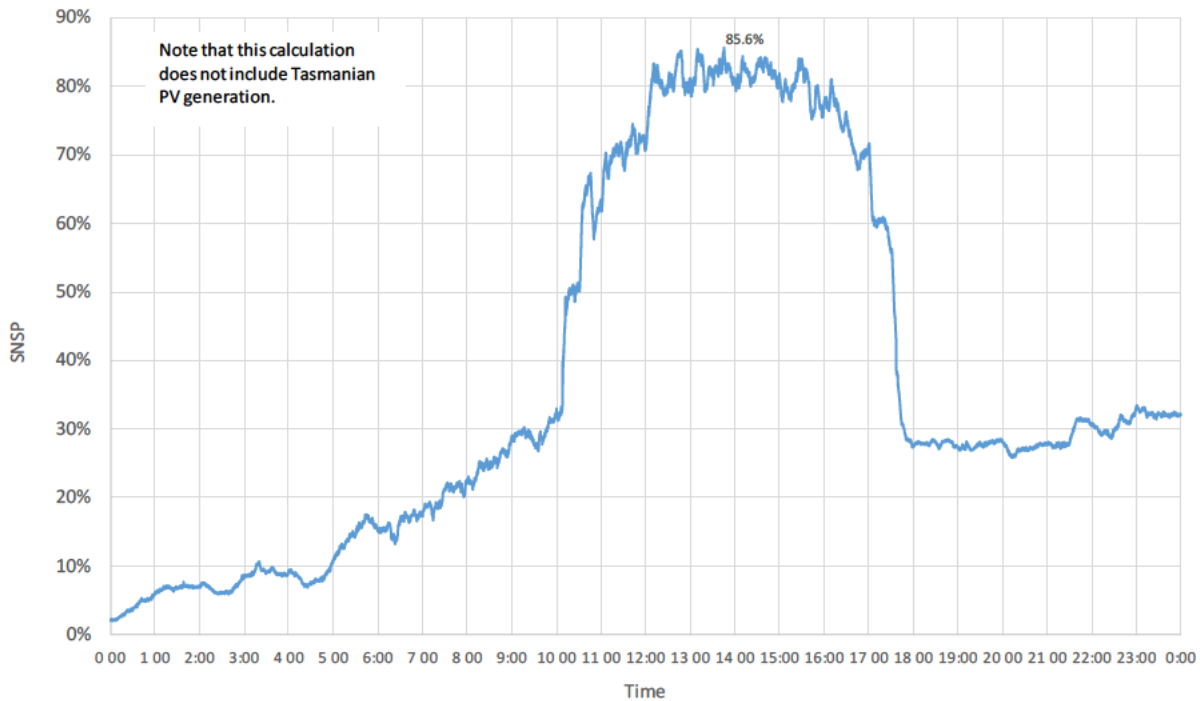
<u>Excluding Basslink</u>	<u>1 Percentile</u>	<u>5 Percentile</u>	<u>50 Percentile</u>	<u>90 Percentile</u>	<u>99 Percentile</u>
<u>Outage</u>					

¹ [Link to Hydrogen action plan](#)

Minima	888	964	1121	1330	1486
Long term average	929	986	1144	1367	1522
Maxima	980	1023	1175	1401	1566

Due to these two factors Tasmania experiences periods of large system non-synchronous penetration (SNSP) as demonstrated by the chart below.

Tasmanian System Non Synchronous Penetration (SNSP) Ratio
Sunday 13 September 2020



On the distribution network, changing customer behaviour and the predicted consumer uptake of disruptive technologies such as rooftop PV, battery storage, electric vehicles and demand response solutions at an accelerating rate, is resulting in power flows and voltage levels that existing networks were not designed to operate with. This disruptive technology, generally referred to as “Distributed Energy Resources” or DER will need to be orchestrated to manage network constraints in real-time. As the industry moves towards the paradigm of a Distribution System Operator (DSO) to actively manage the distribution electricity network quality stability and constraints, several key capabilities will need to be delivered by operational systems. Although this will require investment in technology, process improvement, data capture and data remediation it has been demonstrated in other jurisdictions that the capital cost of implementing new capabilities will be significantly less than the cost of addressing issues using traditional network augmentations and upgrades.

Regardless of the DSO model chosen by the industry the following base capabilities will be required:

- **Integration of Internet of Things (IoT) and Advanced Metering Infrastructure (AMI):** extend the control, reach, granularity and breath of information into network operations;
- **Open APIs:** enable staff, suppliers, consumers and market participants to gain direct access to data and capability locked within our core systems;

- **Adaptive Cyber Security:** as the connectivity and exposure of core controls systems is required by a DSO, increased capability to protect mission control network control systems from cyber-attack will be mandatory;
- **Real-time and forecast Network constraint detection:** utilise highly accurate network models, telemetry, and historical data to forecast and detect in real-time the likely violations of thermal and equipment ratings within the network.
- **Network service aggregators:** contract to customers to provide operational envelopes to manage periods of peak or minimal demand within the network. This is likely to also include the management of third party energy providers using equipment such as community batteries.

The points raised in this section, along with TasNetworks' Future Distribution System (FDS) roadmap and 2030 vision require continued augmentation of the NOCS. Section 9.2.3 details proposed projects which facilitate the delivery of the additional capability required in a timely and prudent manner.

6 Whole of life management plan

6.1 Selection criteria

Real time systems are selected to provide reliable service for an expected 10 year life. Systems should allow for future expansion, technical support and flexibility. The major issues identified in the management of the NOCS are:

- reliable performance for expected life of product;
- manufacturer support over the life of the product and consequential "lock in" through support agreements;
- vendor proprietary software;
- obtaining outages to upgrade systems;
- firmware version control;
- configuration software support; and
- cyber security design for integrated transmission and distribution operation.

These criteria can also be applied to Operations support software but with a 5 year expected life. Operations support can tolerate a lower level of availability for some software applications. This factor is taken into account in this management plan.

6.2 Strategy (OPEX and CAPEX)

The NOCS and its availability is a critical component of TasNetworks real-time operation of its transmission and distribution systems. Support of NOCS utilises these asset management strategies:

- TasNetworks maintaining sufficient internal knowledge and expertise to rectify the vast majority of operational issues that may arise and to ensure that it is not totally dependent on the suppliers of that hardware and software;
- TasNetworks maintains support agreements with the suppliers of the software and hardware on which these systems run to ensure access to technical support when required. For critical software, source code escrow provisions are required within supplier contracts;

- [REDACTED]
- where possible, procure vendor support contracts at a level which provide a mechanism to implement regular software updates;
- every 12 to 24 months TasNetworks upgrades core NOCS software components with current releases. Production software versions should be no more 1 major version behind a vendor's latest release. Software versions need to be field proven prior to implementation on production systems within the NOCS;
- ad-hoc software upgrades will occur to remedy security deficiencies and software defects;
- apply a continuous improvement and security by design methodology to cyber security. Review and utilise new security measures during upgrades.
- TasNetworks regularly upgrades the core components of the NOCS IT infrastructure hardware including servers, storage and workstations. See also the Corporate IT Asset Management Plan;
- TasNetworks regularly upgrades the networking and telecommunication components of the NOCS. See also the Telecommunications Bearer Network Asset Management Plan;
- changes made to customise core operational software undergo system testing using the development and quality assurance systems prior to releasing the changes into the operations environment;
- continually enhance operational systems in line with good industry practice and evolving needs;
- database management, including the historical and SCADA databases, is a key responsibility of NOCS and those databases are significant corporate assets and must be kept secure and in an operational state at all times;
- database changes and upgrades are only applied to the NOCS weekly and scheduled using the same rigor as planned network outages
- provide systems that enable network planning and operating decisions to be made based on high quality, holistic information about the network and assets;
- provide systems that enable existing assets to be fully utilised and efficiently operated and maintained;
- strictly control both physical and technical access to the operational environment;
- assess emerging technologies, standards and practices – implementing these as and when appropriate to provide a modern, effective and efficient information technology environment and removing manual intervention and opportunities for manual intervention;
- continually assess system capacity and licensing of the various software and hardware components to support transmission and distribution network augmentation;
- maintaining alarm levels less than or equal to “stable” alarm rate in accordance with the Engineering Equipment and Materials Users Association (EEMUA) to avoid overloading operators with too many alarms; and
- general and external access to the operational systems and their data is via information servers with high levels of access security.

Network support assets can tolerate a lower level of availability for most applications. The principles above are also applied in the asset management strategy commensurate with the 5 year asset life and criticality.

TasNetworks has adopted a strategy of implementing both proactive and reactive condition monitoring of software assets and physical assets. Proactive monitoring practices actively checks

the conditions of assets to identify developing condition issues before failure. Reactive monitoring detects failures once they have occurred so that normal service can be restored.

6.3 Proactive Monitoring

The goal of proactive monitoring is to predict likely incidents with sufficient notice and information to enable staff to take corrective action and avoid the incident. TasNetworks has implemented condition monitoring for software assets to detect defects and provide early warning of developing issues. Many systems have in-built diagnostic capability and report application and server status via SMS or email. TasNetworks has several operational monitoring systems that display system and infrastructure statuses and alerts within the NOCS environment. Systems are monitored in office hours by NOCS staff and are monitored by both power system coordinators and automatic processes after-hours.

Staff undertake daily check of systems to ensure operation and address any areas of concern. All issues or incidents are logged in a service management tool.

6.4 Reactive Monitoring

Reactive monitoring aims to detect incidents affecting assets as quickly as possible during or after they occur, to capture sufficient information for the incident to be rectified in the shortest practical timeframe and to provide that information to operational staff. The NOCS systems self-diagnose and present information to responding staff. At this stage, staff assess the impact of the incident and undertake corrective action

To manage after-hours incidents, an on-call roster is maintained on a 365/24 basis. On-call staff have training and expertise in all NOCS systems and subsystems. In some cases, operations support software 'first response' is provided by personnel on the on-call roster. Interdependencies between the NOCS, DMZ and corporate network sometimes require diagnosis of failures to be performed by the on-call specialists. Remedial action may be referred to corporate IT or TNOCS networking specialists.

6.5 Defect Management

Software defects are prioritised, logged and entered into the service management tool. Due to the complex nature of software defects, high level support is contracted with the vendor. Service impacting defects are addressed in accordance with vendor Service Level Agreements (SLAs). If not service impacting, the vendor will resolve by patching the software or add it to a list of possible enhancements for the next software release.

6.6 Technical Support

Other operational costs which are not able to be classified as corrective maintenance are allocated to the general NOCS budget. These tasks include:

- system fault analysis and investigation;
- preparation of asset management plans;
- standard and procedure management;
- management of the service providers;
- resources management, particularly professional and technical skills availability;
- training;
- group management; and
- general technical advice.

6.7 Triggering events for software and data updates

These events commonly trigger the need to update NOCS or operations support software and data:

- network augmentation of the transmission or distribution system;
- new customer connections;
- new generation projects;
- violations to power system security criteria due to demand changes;
- change to field technology;
- NER compliance;
- Change or additional National Electricity Market (NEM) requirement;
- continuous improvement to customer service;
- increased cyber security risk or vulnerability; and
- loss of vendor support where systems become obsolete.

As the NOCS control systems has expanded to include rich process based functionality to manage planned and unplanned outages, and to automate key functions such as fault restoration, it is anticipated that functional requirements of business stakeholders will also drive the requirement for more frequent and complex upgrades, including significant training and change management.

Proposed network augmentation projects identified in the 'Annual Planning Report' will include the installation of primary and secondary assets. This will grow the number of assets within the network, resulting in increased use of operational systems resulting in higher operational and maintenance costs.

6.8 Spares management

Fore hardware utilised within the NOCS, sufficient replacement parts are to be kept to meet all credible contingencies which would result in an outage impacting the operation of the NOCS. This includes maintaining vendor agreements to ensure adequate and timely delivery of spares to restore redundancy within 24 hours of a failure.

6.1 Economic Life

The NOCS software assets have an economic asset life of 10 years as defined by Sinclair Knight Merz (SKM) in its "Assessment of Proposed Regulatory Asset Lives" report prepared in August 2013.

Assets related to Operations support software is considered to have an economic asset life of 5 years.

Network data, network models and procedures are updated as required

6.2 End of life management

The latest renewal strategy is intended to provide full utilisation of the assets deployed within the NOCS. Key software components are to be reviewed every 10 years to ensure:

- alignment to business requirements;
- adequate and economic support mechanisms exist; and
- the risks of operating these systems fall within the business risk appetite.

Hardware equipment, once reaching end of life, is disposed by sending to e-waste in alignment with TasNetworks asset disposal policies.

7 Asset Performance

Performance levels of TasNetworks NOCS assets are assessed using a combination of internal performance monitoring measures and external benchmarking.

AEMO call for a target NOCS availability of 52 SCADA Minutes Lost (SML) per rolling year average. This equates to 99.99% availability with no distinction between unplanned or planned outages. Whilst this target is non-binding, TasNetworks has adopted this target as key performance indicator. Currently the NOCS is within the AEMO metric and is comparable to other Australian TNSPs.

There are no performance measures that apply to network support applications.

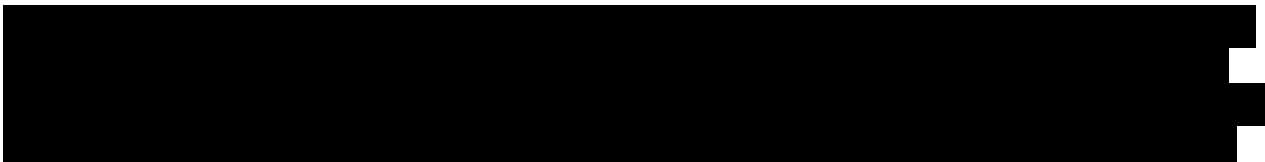
7.1 NER and AEMO Compliance

The NOCS is required to meet the compliance requirements set out in section 4.11 of the National Electricity Rules (NER) and the AEMO Standard for Power System Data Communication version 3.0, effective 3 April 2023. These obligations require that SCADA systems are designed and installed to meet minimum levels of:

- redundancy;
- security;
- latency of data; and
- reliability and accuracy of data.

7.2 NOCS Asset Condition Summary

Network Operations manages a wide range of operational software packages which could be considered to exist in good condition due to the evergreen asset management philosophy. Assets are kept functional and their effective lifecycle extended through the application of appropriate updates. Due to the critical nature of the NOCS, core assets are updated according to the management philosophy detailed above in section 6 Whole of life management plan.





7.3 System Protection Scheme (SPS)

The introduction of the SPS required increased performance of operational systems. This includes the requirement of a sub 3 second data latency from digitisation for effective operation. Failure of the NOCS may cause the SPS not to operate correctly under fault conditions. There is also a risk of triggering a SPS event when work is being carried out on the NOCS. The full set of performance standards for the SPS can be found in the SPS Performance Standard V1.4 (D11/96135) and the SPS Operational Requirements V1.3 (D11/96133). The documents outline the following requirements:

- SPS central trip box availability;
- SPS central trip box telecommunications availability;
- circuit breaker SCADA latency;
- timing of key process within NOCS;
- fault response; and
- allowed outages and duration.

Introducing and maintaining the skills required for Network Operations control room and support personnel require well designed documentation, procedures, and training scenarios.

8 Risk

The threat of mal-operation and the inability to control the power system are the greatest risks for the operational systems. Redundancy and communication diversity at key sites is of paramount importance to maintain system availability and compliance. It is important to have local in-house support, on-site spares, and access to vendor high-level support to ensure timely repair to return the systems to normal operating state after a failure.



The main risk associated with the NOCS is the corruption of data or inadvertent misconfiguration by staff. A regimented back-up and change management process has been implemented to address the aforementioned.

8.1 Business Risks

The following key business risks have been identified:

- Significant failure of NOCS occurs resulting in disrupted power supply and potential penalties and reputation loss to TasNetworks.
- Telecommunications Network Management platform failure resulting in inhibited ability to monitor system outages and performance, resulting in reduced service and delays in responding to failures.
- System Black, greater than 12 -24 hours, effects on Communication System leading to loss of service.
- Withdrawal of supplier support, e.g. hardware replacements and support escalation.

A full breakdown of risk and associated mitigation can be found in the NOCS Risk Management Plan and Management.

New risks in the operations support area:

1. NECF breaches
2. Loss of reputation with customers due to poor planning and coordination of network outages.
3. Inefficient deployment of mobile generation or incorrect application of demand side initiatives.
4. Ineffective contingency plans arising from incorrect/incomplete network studies.

9 Financial Summary

9.1 OPEX Expenditure

Budgets for operational expenditure are derived from corrective maintenance and technical support estimates. These budgetary figures are prepared by the Network Operations department for the operational activities of the entire population of assets. Key contributors to operational expenditure are:

- labour;
- vendor support;
- provision of on-call rosters;
- Process and documentation maintenance;
- training of in-house support staff; and
- telecommunications charges.

A full breakdown of the Network Operation's department budget can be found in TasNetworks finance systems

9.2 CAPEX Expenditure

For the development of TasNetworks' Corporate Plan, rolling 7 year capital works program capital expenditure for the proposed NOCS enhancement program, is estimated as a level 1 by the Project Services team.

Closer to the project initiation phase, the projects are more accurately estimated by the Project Services team as a level 3A estimate and are compared and consolidated with the project Contractor's submission to create a level 3B estimate which is included in the business case for expenditure approval.

9.2.1 Investment evaluation

For each program or project to be included within TasNetworks revenue proposal(s), an Investment Evaluation Summary document is prepared describing the condition, performance, risk, options and strategies identified within this asset management plan and a Net Present Value (NPV) summary for each identified option is also presented to support the need for capital expenditure.

The Investment Evaluation Summary documents for this asset management plan's proposed capital program are:

- NOCS Transmission System Enhancement Program Investment Evaluation Summary


- NOCS Distribution System Enhancement Program Investment Evaluation Summary

These are stored within the Revenue Reset Program of Work.

9.2.2 Recurrent Investment

Table 2 provides the schedule for recurrent investment required to maintain the systems as outlined in section 6 whole of life management plan.

Table 2 Recurrent investment

<i>year</i>	2023/24	2024/25	2025/26	2027/28	2028/29	2029/30	2030/31	2031/32
<i>Network</i>				Renew				
<i>Firewall</i>	Renew					Renew		
<i>GPS Clocks</i>					Renew			
<i>RTUs</i>			Renew					
<i>Historian</i>	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade
<i>PDC Software</i>		Renew*				Renew		
<i>PMU Analytics</i>	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade
	Upgrade		Upgrade		Upgrade		Upgrade	
<i>Simulators</i>		Upgrade			Upgrade			Upgrade
<i>Infrastructure (OS, AD, DB)</i>		Upgrade			Upgrade		Upgrade	
<i>Security & Sys Mgt</i>	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade	Upgrade



9.2.3 Proposed Non-recurrent investment

Detailed below is a proposed list of significant Operational System projects for the current and 2024-29 regulatory control periods. The intent of the information given below is to give some brief context and justification of the project.

System strength Management Update 2025-2026 (unbudgeted)

It is expected system strength requirements will continue to change as IBR increase and new loads connect to the Tasmanian power system. This project is to provide updates to the EMS and custom system strength application to support the changing requirements in the monitoring and dispatch of system strength services. This includes the ability to embed inertia and fault level calculations in contingency analysis, on-line engineering studies and outage planning.

Short term outage planning and scheduling 2024-2026 (unbudgeted)

The development of Northwest network projects, along with the Marinus interconnector, will require the management of extensive equipment outages on an increasingly dynamic and volatile network. This will require the capability to coordinate generator, load and network equipment outages in a manner that safety manages network constraints, system strength issues, automation and protection schemes, dispatch patterns and changing weather patterns. The project is to provide the outage scheduling, conflict, look-ahead contingency and engineering analysis to assist short-term outage planners so that they can ensure outages occur efficiently and with minimal disruption to market participants.

RPSS 2027-2029 (unbudgeted)

This project is to update the suite of tools enable TasNetworks meet its license requirements to manage the Tasmanian power systems in the absence of AEMO. These tools will require a significant redevelopment to support the increase penetration of IBR and potential introduction of new major loads and interconnectors into the Tasmanian power system.

Synchrophasor 2024-2029 (Unbudgeted)

The application uses real-time phase angle and voltage measurement data from phasor measurement units (PMUs) located in key positions within the network to facilitate more accurate network modelling of the power system. PMU data will provide operational staff with a more accurate view of power flows within the power system allowing more precise modelling and analysis of system security (power flows). This project is to deploy PMU and PDCs at key network locations to ensure full visibility of the transmission system including major industrials and generators.

Transient Stability Analyser (TSA) 2027-2029 (Unbudgeted)

TSA provides analysis of the power system to determine the ability for it to remain in a stable state with small fluctuations in load and generation. TSA will allow early detection of issues with system security associated with changes to load and/or generation.

Defensible Architecture 2024-2025 (partially funded)

The core architecture of the NOCS will need a significant uplift to manage increased cyber security requirements and the ongoing requirement to connect to new untrusted market participants. These new connections range from large wind farms owned by international organisations to mini

generators within the distribution system as well as system aggregators communicating over the internet. This project is to implement the appropriate network segmentations, isolation and cyber security controls to manage the risks these connections propose to a critical TasNetworks function. The project will provide a mechanism to reduce and scale capability inline with the cyber security risk facing the business at any given time.

Remote Access 2023 -2024 (partially funded)

The breadth and depth of technologies implemented within the NOCS as outlined in section 4 make it unviable, non-cost effective and ineffective for a small on-call roster to provide adequate 24/7 support. Failure of key system is likely to necessitate the remote access for vendors and support staff not on call to resolve issues in a timely fashion. Additionally, there is a requirement to provide flexible work arrangements for a limited pool of skilled engineers to support the real-time systems. This project is to implement the requisite cyber security controls, privileged access management and security review to minimise the risks associated with remote access.

Tasmanian Integrated System Protection Scheme (TISPS) 2024-2026 (funded)

The main driver of the NCSPPS is to facilitate the delivery of increased energy through key transmission corridors to enable additional export through the Basslink interconnector. This protection and control scheme entered service in 2005, as such, its key hardware assets are reaching 20 years of age and the end of their economic life. Although owned by TasNetworks, the NCSPPS is currently a non-regulated asset and provided as a service to Basslink. As new loads and generators connect to the Tasmanian power system the NCSPPS/TISPS will need to be modified to handle the new connections and changing power flows on the system. It is expected the NCSPPS functionality will become regulated reflecting the shared benefit it provides to several market participants.

As the TISPS is based on the NCSPPS its assets will need to be renewed and modified to support changes in energy flows resulting from new interconnectors, loads and generators. It will also need to scale to support the number of generators expected to connect to the Tasmanian power system. This project is to replace the NCSPPS with the TISPS. This will include a redesign and technology review phase along with an implementation phase.

Forecasting 2024-2025 (funded)

As DER and IBR penetration increases within Tasmania, it will become increasingly important to be able to generate short-term forecasts of both loads and various types of generation such as solar and wind. This requirement will likely exist within both the transmission and distribution networks to enable the prediction of network constraints ahead of time. [REDACTED]

[REDACTED] This project is a requirement for a number of projects within this Program of Work (PoW) to obtain their full benefit.

Distributed Energy Resource Management System (DERMS) 2028-2030 (funded)

There has been a steady and continued growth of rooftop PV and embedded generation on to the Tasmanian distribution network. Other technologies such as battery storage, electric vehicles and demand response solutions will result in power flows and voltage levels that existing networks were not designed to operate with. This project is to implement a DERMS solution integrated into the ADMS to visualise and manage these Distribution Energy Resources (DER) to avoid violating network thermal and voltage constraints.

Network Constraints/Operating envelopes 2025-2027 (funded)

This project is to modify the existing ADMS state estimator to detect current network violations and predict future probable constraints. This will need to occur for the nominal network configuration, as well as planned and unplanned network outages. Additionally, the solution will calculate relevant operating envelopes which would resolve the network violations. Integration into the DERMS module will enable the envelopes to be dispatched and monitored.

AMI integration 2025-2026 (funded)

AMI meters provide a wealth of features and data which would greatly support several ADMS features to improve customer outcomes. The ability to receive notifications such as last gasp and service restoration will assist in detecting and managing unplanned network outages. The capability for fault centre staff and field to ping meters will reduce truck rolls and verify planned outages for critical customers such as those designated as life support customers. Additionally, being able to query power quality data for select meters will drastically improve the ability to detect and manage parameters such as voltage levels. This project will implement an AMI gateway to interface metering providers within Tasmania into the ADMS.

Volt/Var control 2028-2029 (funded)

The increased penetration of DER within the power system will result in increased volatility of voltage levels across the distribution system. This will make it difficult for control room staff to coordinate and manage the large number of reactive devices and transformers throughout the state. This project will implement an automation solution to provide centralised monitoring and control of voltage and reactive power flow. The solution will issue controls to capacitor banks, voltage regulators, Load Tap Changer (LTC) transformers to resolve violations detected by the DMS state estimator.

FCS/PCS/AUFLS replacement 2023-2025 (non-regulated)

The NOCS contains several System Protection Schemes (SPS) to manage defined contingent events which would result in a deviation outside the frequency operating standard. All these schemes have been built on top of the original SPS hardware which entered service in 2005. This hardware is reaching the end of its economic life and will require replacement. These contingency schemes are non-regulated assets which are provided as a service to several generators. This project is to review the existing designs and implement a solution that will renew the assets and scale to manage the new generators and loads expected to connect to the system. Due to the meshing of hardware, this project will need to occur alongside the TISPS project.

Advanced Distribution Management System (ADMS) (funded – in progress)

An ADMS is a software platform that supports the full suite of distribution management and optimisation. It includes functions that automate outage restoration and optimise the performance of the distribution grid. ADMS functions available for electric utilities include fault location, isolation and restoration, Volt/Var ampere reactive optimisation, conservation through voltage reduction, peak demand management and support for microgrids and electric vehicles.

A fully functioning ADMS provides real-time information and situational awareness to locate exactly where a fault is and expedite deployment of a crew to fix the problem if required. This results in reduced outage times, more efficient use of resources, improved system reliability, improved asset life and reduced risk to public safety. This project is to deliver an integrated DMS and OMS.

Historian renewal & enhancements (partially funded)

The NOCS captures and maintains a large amount of operational historical information relating to various aspects of the Tasmanian power system. This information is used to demonstrate

compliance with obligations such as those defined in the National Electricity Rules, TNSP operating agreement, AEMO standards and customer connection agreements. Historical operational data is also utilised within TasNetworks to effectively plan, develop, manage, and report on the transmission system. Although this asset is regularly upgraded to ensure vendor support there is an increased need to store additional information such as AMI data, power system parameters calculated from both the DMS and EMS, and high-speed data fault data from relays. The requirements will result in not only increased licensing but also a redesign to support business and cyber security needs. This project is to deliver an operational historian, a renewed enterprise historian and licensing to support the business through the 2024-2029 regulatory control period.

10 Related Standards and Documentation

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

Description	URL
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)	
Future Distribution System Vision and Roadmap	

