Asset Management Plan

Network Operations

Record Number: R299400

Version Number: 1.0

Date: October 2017

Authorisations

Action	Name and title	Date
Prepared by	Adrian Merkel, NOCS Team Leader	25/10/2017
Reviewed by	Chong Ong, Network Operations and Control Team Leader	30/10/2017
Authorised by	Jason King, Network Operations Leader	30/10/2017
Review cycle	2.5 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.

Disclaimer

UNCONTROLLED WHEN PRINTED

This document has been prepared and made available solely for information purposes. Whist 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

Name	Details
A. Merkel	New Document
A. Merkel	Updated for R19

Table of Contents

Glossary

AEMO	Australian Energy Market Operator
AC	Alternating Current
AGC	Automatic Generator Control
AMP	Asset Management Plan
DC	Direct Current
DMS	Distribution Management System
DMZ	De-Militarised Zone
DSA	Dynamic Stability Analysis
EMS	Energy Management System
GCS	Generator Contingency Scheme
GRC	System to manage governance, risk and compliance
ICCP	Inter-Company Communications Protocol
IP	Internet Protocol
IT&C	Information Technology and Communications
MMI	Man Machine
NEM	National Electricity Market
NOCS	Network Operation and Control System
OSI	Open Systems International
OTS	Operator Training Simulator
PABX	Private Automated Branch Exchange
PMU	Phasor Measurement Unit
RPSS	Residual Power System Security
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SML	SCADA Minutes Lost
SPS	System Protection Scheme
TDM	Time Division Multiplex
TESI	Tasmanian Electricity Supply Industry
TMR	Trunk Mobile Radio
TNOCS	Telecommunications Network Operation and Control System
TRCalc	Thermal Ratings Calculator
VSA	Voltage Stability Analysis

1 Purpose

The purpose of this document is to describe the Asset Management Plan for software assets managed and coordinated by Network Operations which provide or support the operation of the Tasmanian power system.

2 Scope

This document covers only the Master Station platform, network data and software applications managed and coordinated by Network Operations.

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

i. Real time applications and network data residing on the Open Systems International (OSI) Monarch platform and

ii. Operations support applications and network data residing on the corporate IT platform.

This plan excludes the following:

- IT Infrastructure except the Monarch SCADA platform and associated software;
- Telecommunications bearer and networking;
- Desktop computers and telephones; and
- Substation SCADA and protection physical assets i.e. RTU and relays.

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

- control centre building physical security;
- heating, lighting and ventilation (including air-conditioning systems);
- uninterruptible power supplies (UPS);
- battery systems (primarily communications);
- voice and data communications infrastructure;
- IT infrastructure and firewalls;
- Smart Field Devices (reclosers, fuse savers, regulators); and
- RTUs in TasNetworks' substations.

3 Strategic Alignment and Objectives

This asset management plan aligns with both TasNetworks' Asset Management Policy and Strategic Objectives. Its framework is set out in Fig 1.

The objectives of this plan are to:

- Present an overview and high level catalogue of these non-physical assets;
- Manage business risk presented by the systems;
- Achieve reliable system performance consistent with prescribed services standards;
- Quantify the risk specific to the systems and identify corresponding risk mitigation strategies;
- Ensure the effective and consistent management and coordination of asset management activities relating to the assets throughout their life-cycle;
- Demonstrate that the systems are being managed prudently throughout their life-cycle;

- Ensure asset management issues and strategies are taken into account in decision making an planning; and
- Define future operation and capital expenditure requirements of the systems.

3.1 Background:

Details of the OSI Monarch platform are provided in section 4. An overview of the software applications and network data is provided below.

i) Real time assets residing on the OSI Monarch platform

The formation of TasNetworks extended the use of the OSI Monarch platform to support Distribution real time functions. Network Operations and Control Systems (NOCS) now provides SCADA, EMS, DMS and Operator Training Simulator functionality across the two disciplines.

The NOCS requires significant configuration and customisation to enable its functions for TasNetworks. This work is the intellectual property of TasNetworks and is a non-physical Network Operations asset.

The assets are:

a) Configuration of database, contingency analysis lists, scan lists and data polling methodology;
b) Design of Man Machine Interface (MMI) including station one line diagrams, alarm configuration, network state summaries and user interfaces to custom and propriety applications;
c) Network model specifying the components, connectivity and characteristics of the electricity network including the customisations that account for special control schemes and custom applications.
d) Custom applications - NWAVS, NAVS, SAVS, TRCalc, TFB tool, Vegetation tool, NCSPS & FCSPS (generically called SPS), Load shedding, SynchroWAVe, RPSS tools, Historian and market systems. Descriptions and specifications for these applications can be found in the Network Operations Collaboration Zone.
e) Operator Training Simulator training room, configuration and scenarios.

ii) Operations support software and network data residing on the corporate IT network:

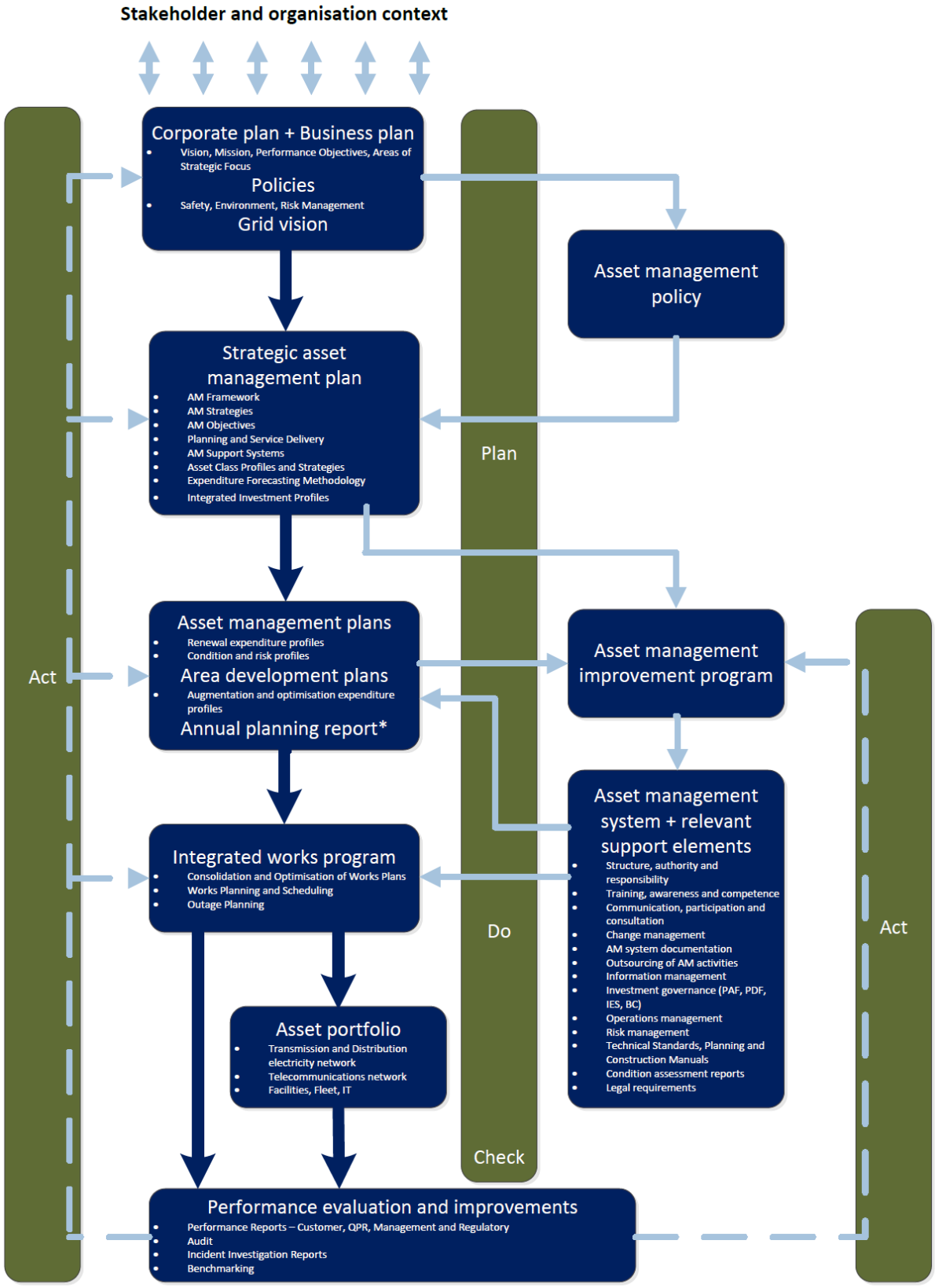
a) Network Study tools and associated data: Network study tools are required to find the best solutions to network problems such as voltage, thermal or stability constraints. These tools minimise adverse customer and market impacts from planned and unplanned network outages in both the Transmission and Distribution networks. These tools are used in association with market systems to forecast the impact of network activity on the market.
b) Reporting: TasNetworks utilises two historians (eDna and PI) to manage network data. The historians are used for reporting network performance, incident investigations and investigating network issues. Also, web applications provide access to real time information on a 'read only' basis via the corporate network.
c) Logging: Electronic logging facilities have been implemented for both Distribution and Transmission Control Rooms.
d) Network Access for maintenance or project work: Network Operations administer and optimise planned outages and access to the Distribution and Transmission networks. The objective is to maximise customer service while achieving the required maintenance or

project schedule. Software tools are in use for both Distribution and Transmission outage planning.

e) Switch order management: Network operations is responsible for producing switching instructions that provide the switching steps required to remove electrical plant from service with due regard for safety, customer service and network reliability. Software packages that assist the production of switching instructions are in use across both the Distribution and Transmission groups.

f) Operational procedures: An extensive database of operating procedures is maintained by Network Operations to support both Transmission and Distribution real time operations.

Figure 1 – TasNetworks Asset Management Documentation Framework



* The Annual Planning Report (APR) is a requirement of sections 5.12.2 and 5.13.2 of the National Electricity Rules (NER) and also satisfies a licence obligation to publish a Tasmanian Annual Planning Statement (TAPS). The APR is a compilation of information from the Area Development Plans and the Asset Management Plans.

4 Detail of the Assets

i) **The Master Station platform**:

The SCADA, EMS, and DMS, comprises computer hardware and OSI proprietary software. NOCS is designed to provide uninterrupted service to both Transmission and Distribution operations as well as the interfaces to AEMO and Tasmanian generators. Connections to AEMO and Hydro Tasmania (ICCP links), data communications (provided under Telecommunications Bearer Network AMP (R0000032671) are key components of the NOCS and System Protection Scheme (SPS).

The platform is a dual redundant set of assets which are housed in Maria Street and Chapel Street to achieve the availability required for 24/7, mission critical operations and control. The platform is supported under contract with OSI whilst configurations, station displays, network models and applications are supported by a TasNetworks team of SCADA engineers.

This SCADA platform was commissioned in 2002. The core NOCS application is provided by an OSI Monarch platform, upgraded annually. The most recent upgrade of the core software platform was conducted in October 2016. Updates to the software described here are usually required with hardware upgrades to ensure reliable operation after the updates.

a) Configuration of databases, contingency analysis lists, refresh rates and data polling:

This suite is critical to the correct functioning of all other application software residing on the Monarch platform. They enable the Monarch platform to provide Tasmanian electricity network SCADA and EMS functions. The data is maintained by a TasNetworks team of SCADA specialists.

b) Design of MMI including station one line diagrams, alarm configuration, network state summaries and user interfaces to custom and propriety applications:

A correctly designed MMI maximises the utility of the Monarch platform for TasNetworks users. This design effort represents a significant investment in its initial design, maintenance and continuous improvement.

c) Network model specifying the components, connectivity of the electricity network and model customisations for special control schemes and custom applications:

The electrical characteristics and connectivity of the network must be specified within the Monarch platform to enable its real time EMS functions. For example, OpenNet is a product from OSI that provide a network security analysis system for on-line security analysis, operations planning and off-line engineering studies. Features include:

- network topology processor;
- power flow;
- contingency analysis;
- state estimation;
- optimal power flow;
- short circuit analysis;
- automatic generator control;
- voltage stability; and
- available transfer capability.

Custom applications such as SPS and TrCalc also require network characteristics to be built in NOCS.

d) Custom applications - TrCalc, NWAVS, NAVS, SAVS, TFB tool, Vegetation tool, NCSPS & FCSPS (generically called SPS), Load shedding tool, SynchroWave, RPSS tools, Historian and market systems.

NWAVS, NAVS, SAVS: These are tools for state-wide network voltage and overload control. They provide automatic control under routine conditions.

TFB tool, Vegetation tool: These are labour saving tools to perform repetitive controls in bulk. The tools manage reclosers, fuse savers and loop automation schemes.

System Protection Scheme (SPS): The SPS is a suite of hardware and software. The Frequency Control SPS manages the effect of a Basslink loss of link by disconnecting load or generation to bring system frequency within required technical limits. The Network Control SPS manages the impact of loss of a key transmission circuit by automatically reducing generation and removing overloads on transmission circuits. A backup Network Control SPS hardware/software system is also provided at critical substations to protect against failure of the NOCS. NCSPS availability is such that energy transfer into or out of Tasmania would be severely constrained should the function fail. Hardware for the SPS is outside the scope of this plan.

RPSS Tools: TasNetworks licence obligations require TasNetworks to perform AEMO's security function should all communications be lost with AEMO. This suite of tools facilitate the capture of market data and the network state such that TasNetwork can perform this security function in AEMO's absence. Automatic Generator Control (AGC) is a requirement of this suite of tools.

Historian: Both eDNA and Pi are real-time data historians for acquiring, storing, and displaying large amounts of operations and engineering information. Historians collect data from a number of sources, including the central SCADA platform and store it in a highly compressed format, allowing decades of high-frequency, time-series data to be stored online in its original resolution. The historians enable accurate and timely provision of historical information. The historian tool is used by both operational and corporate users. It is provided in a redundant configuration. The historians reside in the 'de-militarised Zone' (DMZ) between the SCADA and corporate network environments.

Market Systems: This is a suite of systems which sit on the DMZ, comprising the info-server suite of applications. These applications give access to market information for power system coordinators and operational engineers.

Synchro phasor Data Concentrator: concentration of PMU data streams for usage in fault analysis and energy management systems.

e) Operator Training Simulator (OTS) training room, configuration and scenarios.

OTS is a key element for training on the NOCS platform. It is part of the competency assessment system for real time shift staff. It is also used for:

- Training of new personnel in the use of NOCS;
- black start and residual power system security exercises;
- rotational load shedding;
- scenario based exercises; and
- Test platform for core system upgrades.

OTS requires adjoining training rooms. One allows an instructor to play out training scenarios and mimic interactions with external parties (eg field staff, major customers and TasNetwork managers). The other mimics the control room environment and facilities used by shift staff. Significant investment is required to write and maintain training scenarios.

ii) Operations support software and network data residing on the corporate IT network:

a) Network Study tools and associated data:

NEO, Ezy2View are supported by Operational Systems department but funded by Corporate IT under the Corporate IT Asset Management Plan – Applications Program.

TasNetworks use two proprietary software packages, NEO and ezy2view, and custom applications to provide market intelligence for network study. These reside on the corporate IT network. Both rely on data from the info-server operating on the DMZ.

The study tools are used to optimise deployment of mobile generator units as a short term measure to improve customer outcomes. Demand side initiatives are being developed utilising the emerging battery technology to provide similar relief.

As a TNSP, TasNetworks is required to produce network limit equations that describe the technical envelope of the network. AEMO convert these limit equations into constraint equations for use in their market management system. This fulfils AEMO's system security obligation. Software tools are required for the production of limit equations and subsequent administration of constraint equations in a library. Network study models and associated software tools are required to perform these functions.

TasNetworks is subject to transmission performance incentive schemes that are linked to market outcomes. Market tools provide the anticipated market prices, generator participation, inter and intra regional power flows to aid the study and resolution of network voltage, stability or thermal problems arising from planned outages in a manner that minimises market impact. Historical market information and bids are also available through the info-server facility.

A suite of software provide access to real-time data but reside in the corporate IT network. These assets include:

- Market Watch System (NEO);
- Ezy2View;
- SynchroWAVe;
- Bid stack viewers;
- Constraint analysis tools; and
- Data querying tools.

b) Reporting:

In addition to the Historians residing in DMZ listed above, a number of web based applications have been deployed in the DMZ to enable ad-hoc reporting of real-time data. Furthermore within the corporate network read only access to the NOCS real time displays and diagrams has been provided to users. These facilities are used in combination with MS Office products for reporting.

c) Logging:

SMELT and Daily Log are the two automated power system coordinator log-sheets used in the Transmission and Distribution Control Rooms respectively.

d) Network Access for maintenance or project work:

Request to Alter Distribution System (RADS), Plant Restriction and Outage Management System (PROMS), are owned by Network Operations and supported by external service providers or internal resources for smaller changes. RADS is the Distribution outage planning tool while PROMS is the transmission outage planning tool.

e) Switch Order management:

Switching Operations (SWOPS), Schedule of Planned Operations (SOPO) are owned by Network Operations and supported by external service providers or internal resources for smaller changes. SWOPS is the Distribution switching writer. SOPO is the Transmission switching writer.

f) Operational procedures:

Operating procedures comprise Standard Operating Procedures, contingency plans and documentation of custom applications and third party assets connected to the network.

The list of software assets and their update cycle is documented in NOCS Software Resource List (R0000868475).

4.1 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 Economic Lives for Transend Regulatory Asset Classes" report prepared in April 2008.

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.

4.2 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;
- continuous improvement to customer service; and
- loss of vendor support where systems become obsolete.

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.

4.3 Utilisation

The utilisation of the Network Operations Control System has increased dramatically since 2003. The connection and upgrade of substation and telecommunications assets has had an impact on the size and complexity of operational systems. As the need for greater volumes of data from RTUs and monitoring devices increase, there will be a significant growth of connected devices and data point count. With the prevalence of "smarter" solutions, such as dynamic line ratings, the SPS, script calculations, real-time network modelling and analysis and anti-islanding schemes, the complexity of operational systems will also increase.

The complexity of the network and smarter systems can also drive the increase in range of applications required for operations support. For example, demand side initiatives and mobile generator solutions is likely to require new software applications to manage them.

5 NOCS Condition Monitoring Practices

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.

5.1 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 Network Operations Control Systems 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. Within the service monitoring tool the following attributes are recorded:

- asset impacted
- responding staff;
- time reported;
- time attended;
- time repaired;
- description of the incident;
- description of the resolution;
- vendor job ticket (if escalated); and
- time closed.

5.2 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. The NOCS is provided on a redundant co-primary configuration and can accommodate up to three failures. All operational systems are backed up daily and back-ups are stored off site.

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 specialists.

5.3 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.

High level support is managed and budgeted for by Network Operations Control Systems and is provided by the following vendors:

- Open Systems International;
- Schneider Electric;
- OSISoft;
- Schweitzer Engineering Laboratories;
- GE Energy; and
- Microsoft

5.4 Technical Support

Other operational costs which are not able to be classified as corrective maintenance are allocated to the general Network Operations and Control Systems 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 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 Network Operations and Control System 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; and
- configuration software support.

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

The Network Operations Control System 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 internally 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 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;
- for the suite of NOCS applications from Open Systems International (OSI) the highest level of support (Monarch Diamond) is contracted;
- every 12 months TasNetworks upgrades core NOCS software components with current releases;
- ad-hoc software upgrades will occur to remedy security deficiencies and software defects;
- TasNetworks regularly upgrades the core components of the NOCS IT infrastructure hardware including servers and storage. See also the Corporate IT Asset Management Plan;
- TasNetworks regularly upgrades the networking and communication components of the NOCS. See Telecommunications Ethernet Bearer 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. This testing will be undertaken on the pre-production and development servers;
- 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;
- 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 users 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.

6.3 Regulatory Obligations

6.3.1 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 1.2, released 7 April 2005. 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.

Overall, TasNetworks SCADA systems are compliant with the NER and Australian Electricity Market Operator (AEMO) requirements. In 2012 TasNetworks undertook a project to reduce latency of substation data transmission. The core 220kV sites of George Town, Sheffield, Palmerston and Farrell substations now return sub 3 second poll which is within the required AEMO standard of 8 seconds. A breakdown of AEMO timing and outage requirements can be seen in Appendices A and B.

Network support applications do not have these compliance obligations.

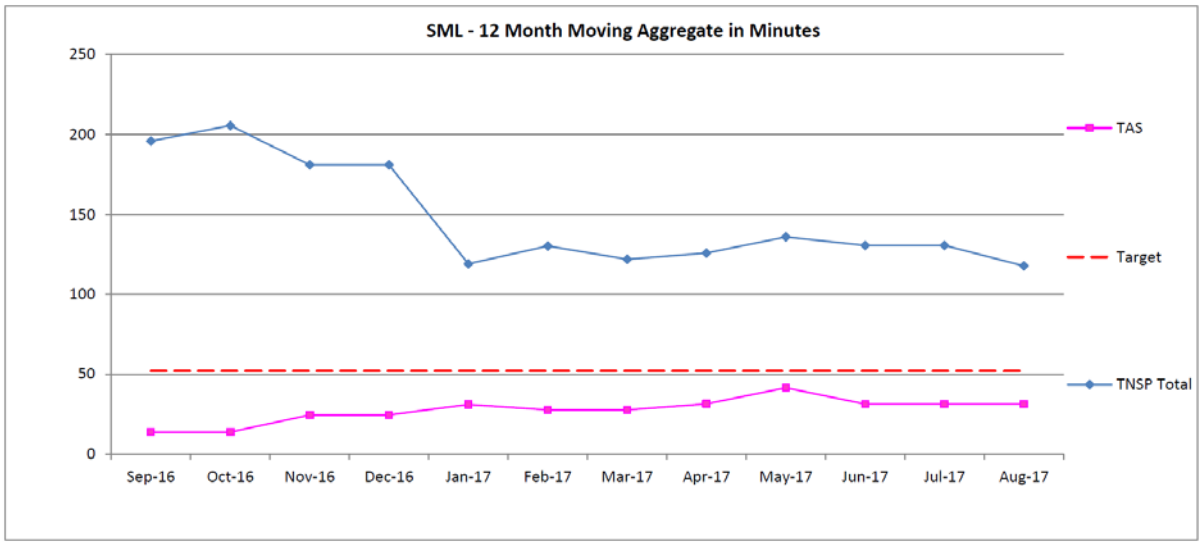
7 Asset Performance

Performance levels of TasNetworks Network Operations Control System 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 a as key performance

indicator. Currently the NOCS is within the AEMO metric and is comparable to other Australian TNSPs. The current year's result can be seen in figure 2.

Figure 2 NOCS SML Performance



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

7.1 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 Management plan.

TasNetworks' SCADA platform provider, OSI, is committed to the Monarch platform and its suite of applications. TasNetworks maintains a close working relationship with OSI to determine the positioning of their product. At this point in time, TasNetworks has had no indication from OSI on the termination of its Monarch platform. Due to TasNetworks' current evergreen management philosophy and the functionality, reliability and useability of the OSI product, it had been decided to continue with the current SCADA platform until the 2019-24 regulatory period. This approach will defer capital expenditure in the order of $10-20 million. Leading up to the next period, an assessment of the OSI platform will be undertaken to determine its condition and if the platform supplies an adequate feature set for TasNetworks' future requirements.

7.2 System Protection Scheme (SPS)

The introduction of the SPS required increased performance of operational systems. For example the AEMO Standard for Power System Data Communication version 1.2A calls for a maximum data latency from field devices to the NOCS of 8 seconds compared to the SPS requirement of a sub 3 second latency 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 in the procedures database and OTS 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 and access to vendor high-level support to ensure timely repair to return the systems to normal operating state after a failure.

The NOCS is delivered on a redundant co-primary infrastructure configuration. The NOCS can withstand a loss of either Chapel Street or Maria Street Operations Building or 3 server failures. 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 TasNetworks' GRC application and NOCS Risk Management Plan (R0000492572) and Management Matrix (R0000728928).

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;
- 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.

9.3 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:

IES01805 - NOCS Transmission System Enhancement Program Investment Evaluation Summary

IES00945 - NOCS Distribution System Enhancement Program Investment Evaluation Summary

These are stored within the Revenue Reset Program of Work Tool.

9.4 Proposed projects

Detailed below is a proposed list of Operational System projects for the 2017-24 revenue periods. The intent of the information given below is to give some brief context and justification of the project. For a more comprehensive description and justification please refer to the associated IES.

Strategy and operaiotnal plans (R numbers)

OpenNet updates/customisations

To provide ongoing improvements to the OpenNet application and includes customisations to better suit the needs of the network, control room and wider business users.

Phasor Measurement integration

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).

Dynamic Stability Analyser (DSA) implementation

DSA 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. DSA will allow early detection of issues with system security associated with changes to load and/or generation.

Training simulator wind generation implementation

To augment the OTS to simulate generation from wind farms within the network so as to provide more realistic simulation of the power system for training purposes.

Annual upgrades

The base platform of the NOCS is centred on the Monarch product from OSI. To ensure adequate vendor support, as well as increased robustness, this platform is renewed every 12 months.

Platform/Architecture Change

Due to the ever increasing amount of data flowing into the NOCS and increased automation requirements, the licensing, database capacity and architecture will have to be modified and increased.

SmartGrid Support

The increased reliance on smart grid technology to provide greater efficiencies in managing the real-time operation of the power system requires underlying systems to handle new technologies and protocols. It is expected that the increased use of Internet Protocol (IP) and protocols such as IEC 68150 in substations will require master station support. Additionally existing Smart Grid technologies such as dynamic line ratings and system wide contingency schemes will need renewal to handle additional requirements and industry standards.

- Short Term Load and Renewable Forecasting – enhance the management of contracts which provide demand management and network support;
- Large scale renewables
- Distributed energy resources
- Integration of new Smart Field Assets
- Switch Order Management – enhancement and review of current paper based switching sheet processes and legacy schedule of planned operations application;
- Mobile access of real-time state of the network – provision of mobile tools to enable field teams to view the current real-time state of the power system;
- Real-time network modelling applications – provision of real-time modelling tools to distribution control room to enable more efficient and reliable operation of the network;
- Strategic Overhead monitoring – selective provision of monitoring of existing network assets to enhance visibility of critical sections the distribution network.
- Improved monitoring of existing metering – selective monitoring of power quality readings from existing metering installation; and

- Cyber security. (new connections and all that)

Advanced Distribution Management System (ADMS)

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.

TasNetworks does not currently have a Distribution Management System (DMS). The current state contains parts of a DMS, however they are not complete or integrated. The roadmap is progressively work towards an integrated ADMS, with investment timed to align with investments in Network technology and Geospatial Systems.

Training & Simulation Systems

The OTS provides a fully simulated environment for the training of power system coordinators to assist in meeting NEM operator training requirements. For this environment to be of practical use it is required to match the NOCS in terms of mimicked functionality. This environment needs to be regularly renewed along with the provision of schemes as they are implemented on the NOCS. Additionally, extending the OTS to mimic the distribution network will provide distribution operators an environment to train and enhance their ability to manage advanced distribution automation.

Historian upgrades & enhancements

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. This asset is regularly renewed to ensure vendor support and augmented such that it has the capability to meet the increasing data recording and reporting requirements of the transmission system.

NEM Systems upgrades & enhancements

The NOCS NEM systems consist of a suite of custom built applications to provide reporting on market pricing, power system constraints, and limits. As AEMO systems and the underlying technology are constantly updated it is necessary to renew the NEM systems. Additionally this suite of applications will require enhancements as NEM reporting requirements increase.

Consolidation and integration

Due to the merging of Aurora's Network business and Transend duplicate systems exist within the Network Operations and Control System. A number of projects will need to be initiated to consolidate these tools to provide the company with reduced maintenance and support costs, as well as a consistent tool and data set for both Transmission and Distribution sections of the business. The systems where duplication currently exists or were integration could greatly benefit the business include:

- Operations logging and reporting tools;
- Real-time modelling and GIS integration;
- Real-time Outage Management integration;
- Outage and Network access management tools; and
- Historian and offline modelling tool integration.

10 Responsibilities

Maintenance and implementation of this management plan is the responsibility of NOCS Team Leader, Network Operations.

Approval of this management plan is the responsibility of the Network Operations Leader

11 Related Standards and Documentation

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

1. D02/524 SCADA System Standard
2. AEMO Standard for Power Systems Data Communications
3. NOCS Standard NS001 - Operations Standard (R0000295281)
4. NOCS Operational Systems Strategy 2017-2025 (R0000770686)
5. NOCS Operational Plan 2017-2019 (R0000777305)

12 Appendix A – AEMO Time Interval Requirements for NOCS

Table 1 Time intervals

Column 1	Column 2	Column 3	Column 4
		Time Interval	
Type	Category	Normal standard	Interim standard
analogue value	a high resolution measurement of system frequency or electrical time required by AEMO from a Transmission Network Service Provider for central dispatch	2 seconds	2 seconds
status indication	main dispatch data	6 seconds	7 seconds
analogue value or discrete value	main dispatch data	6 seconds	7 seconds
status indication	main system data or dispatch data that is not main dispatch data	8 seconds	9 seconds
analogue value or discrete value	main system data or dispatch data that is not main dispatch data	14 seconds	15 seconds
status indication	neither main system data nor dispatch data	12 seconds	13 seconds
analogue value or discrete value	neither main system data nor dispatch data	22 seconds	23 seconds

13 Appendix B – AEMO Yearly Outage Allowance for NOCS

Table 2 Critical outages of remote monitoring equipment or remote control equipment

Column 1	Column 2	Column 3
Category of remote monitoring equipment and remote control equipment	**Total period of critical outages**	
	normal standard	**interim standard**
remote control equipment	24 hours	48 hours
remote monitoring equipment not transmitting or receiving main system data or dispatch data	24 hours	48 hours
remote monitoring equipment transmitting main system data or dispatch data but not main dispatch data	12 hours	24 hours
remote monitoring equipment transmitting or receiving main dispatch data for which AEMO has agreed that it has substitute values for that dispatch data	12 hours	24 hours
remote monitoring equipment transmitting main dispatch data for which AEMO has not agreed that it has substitute values for that dispatch data	6 hours	12 hours