AMS – Electricity Transmission Network

Communication Systems

Document number	AMS 10-56
Issue number	9
Status	Approved
Approver	J. Dyer
Date of approval	13/10/2015

ISSUE/AMENDMENT STATUS

Issue Number	Date	Description	Author	Approved by
0.1	23/09/11	Initial 2011/2012 updates.	D. Ots	
0.9	13/11/12	ICT Review.	D. Ots	T. Ton
1.0	20/11/12	Final for NSD editorial review.	D. Ots	T. Ton
1.1	03/12/12	Final – Modified as per review comments.	D. Ots / D. Postlethwaite	T. Ton
1.2	20/05/15	Initial 2015 updates incorporating latest template.	D. Ots	T. Ton
1.3	17/07/15	Draft version for comment.	D. Ots	T. Ton
9	13/10/15	Final – Modified as per review comments.	T. Ton	J. Dyer

Disclaimer

Contact

This document is the responsibility of the Asset Management Division, AusNet Services. Please contact the indicated owner of the document with any inquiries.

John Dyer
AusNet Services
Level 31, 2 Southbank Boulevard
Melbourne Victoria 3006
Ph. (03) 9695 6000

Table of Contents

List of Tables

List of Figures

Glossary

Abbreviation	Description
ACMA	Australian Communications and Media Authority
ADG	Asset Data Gathering
ADSS	All Dielectric Self Supporting
AEMO	Australian Energy Market Operator
AMI	Advance Metering Infrastructure
AMS	Asset Management Strategy
CEOT	Customer & Energy Operations Team
CWDM	Corse Wave Division Multiplexing
DWDM	Dense Wave Division Multiplexing
EDAMS	Electricity Distribution Metering Asset Management Strategy
EHV	Extra High Voltage
EMI	Electromagnetic Interference
HV	High Voltage
ICT	Information Communication Technology
IED	Intelligent Electronic Device
IP	Internet Protocol
IPVPN	Internet Protocol Virtual Private Network
IS	Information Security
LDT	Line Despatch Terminal
MPLS	Multi-Protocol Label Switching
NBN	National Broadband Network
NOC	Network Operations Centre
ODN	Operational Data Network
OMN	Operational Management Network
OPGW	Optical Fibre in Ground Wire
OSS	Operational Support Systems
OTN	Operational Telephony Network
PDH	Plesiochronous Digital Hierarchy
POTS	Plain Old Telephone Service
PSTN	Public Switching Telephony Network

Communication Systems

Abbreviation	Description
QoS	Quality of Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SIEM	Security Information and Event Managers
TDM	Time Division Multiplexing
TMR	Trunk Mobile Radio
TS	Terminal Station
U/G	Under Ground
VFRB	Very Fast Runback
VOIP	Voice Over Internet Protocol
VRLA	Valve Regulated Lead Acid
VSWR	Voltage Standing Wave Ratio
ZSS	Zone Sub Station

1 Executive Summary

The AusNet Services transmission network employs communications systems primarily to provide:

- Electrical protection signalling between generating stations and terminal stations;
- Electrical protection signalling between terminal stations and other terminal stations;
- Monitoring and control signalling between AusNet Services' Customer & Energy Operations Team (CEOT), generators, terminal stations, and the Australian Energy Market Operator (AEMO);
- Operational voice and business communication between NOC, offices, depots, terminal stations, generating stations, distribution zone substations, connected interstate transmission and generating stations and AEMO.

These services are enabled through various telecommunications technologies, including:

- Bearers(optical, copper, power line and microwave radio) interconnecting sites;
- Wireline technologies (SDH, PDH, WDM, routing, switching, etc);
- Telephony systems (OTN, CEOT console systems, mobile radio, etc);
- Gateways (interconnections to external / 3rd parties);
- Supporting Facilities (e.g. battery systems, radio towers).

The asset and technology drivers are outlined in this document, including the need to ensure reliability and performance requirements outlined in the National Electricity Rules (NER), challenges associated with technology lifecycles, obsolescence and legacy / new services, and the growing threat to physical and cyber security.

This AMS outlines various communications related strategic aims to enable the strengthening of the transmission electricity network, the modernisation of ICT systems to efficiently deliver existing and future communication services, and transforming systems and practices that enhance operational efficiencies, security and safety practices. The key asset strategies are:

- Replace end of life products / platforms;
- Establishing redundant (independent) communications bearers where justified;
- Establishing "next generation" communications architecture to economically support current and future communications services;
- Enhancing communications service performance and (cyber) security monitoring.

Bearers

- Ensure a minimum of 2 independent communications bearers to each EHV Terminal Station site, in line with EHV plant protection scheme and NER regulatory requirements;
- In line with functional and regulatory requirements, selection priority for new and/or replacement communications bearers to be as follows (where economically justified):
    - Where applicable, establish and/or maintain a 3rd (independent) communications bearer to select transmission sites where excessive operational risk and repair / restoration times justify.
    - Where justified, install OPGW in conjunction with planned EHV ground wire replacement programs.
    - Install OPGW fibre on new EHV line construction or refurbishments:
        - Formulate common requirements and standards with AEMO that best enable the establishment of optical communications bearer(s) between stations during new EHV line works or network augmentations.
- Upgrade end-of-life radio links to enable both native TDM and packet based (Ethernet / IP) communications traffic where economic.

- Maintain and/or replace existing ADSS based on end-of-life and/or physical / optical condition degradation when economic.
- Identify ongoing suitability of digital Power Line Carrier technology for long distance (regional) power lines when other alternatives cannot be justified.
- Consider mechanisms to monitor and report optical fibre performance over time. Complete migration of services from copper supervisory cables to suitable bearers.

Wireless Technology Strategy

- Migrate existing 2G (GPRS) services to equivalent wireless service (3G/4G) prior to service termination date (end of 2016).
- Migrate / 3G wireless technology to equivalent (wireless) service when required.

1.1 Wireline Technologies Strategy

- Identify opportunities for Wireline Networks consolidation where feasible and justified.
- Operational Data Network (ODN):
    - Identify and standardise suitable next generation SDH and PDH platform(s) replacement platforms that satisfies existing mission critical (legacy) TDM and (future) packet applications and interfaces;
    - Implement EMS and NMS capability for next generation (ODN) equipment in line with OSS strategy;
    - Progressively migrate teleprotection function onto new generation equivalent (e.g. IEC61850) or replace digital teleprotection (end-of-life) equipment with technology equivalent.
- Operational Management Network (OMN):
    - Identify and standardise suitable network solution(s) that best enables consolidation (where economic) of non-mission critical legacy and future applications and interfaces:
        - This includes assets associated with (but not limited to) Asset Data Gathering, Corporate and AMI networks.
    - Implement EMS and NMS capability for OMN equipment in line with OSS strategy;
    - Implement user access control system for users and devices;
    - Replace end-of-life Routers, Switches and Serial Servers in line with next generation solution(s).
- Communication Design Standard shall be amended to support IEC 61850 applications within and between Terminal stations.
- Develop a centralised network management system capability for both the OMN and ODN network devices.
- Reduce the number of network layers and devices through consolidation where economic.
- 3rd Party Leased Services:
    - Migrate ISDN (data) services to NBN equivalent (when required);
    - Migrate Business DSL (data) services to NBN equivalent (when required).

Communication Systems

Gateway Technologies Strategy

- At time of asset replacement, identify opportunities (where feasible) to consolidate separate network gateways (that access 3rd party services), including:
    - Internet;
    - SCADA (3G services);
    - Metering (3G services);
    - Cloud Services (if / when required).
- Consolidate multiple Inter-Data Centre link (Richmond and Rowville) gateways.

Telephony Technologies Strategy

- At time of telephony system replacement, identify opportunities for system consolidation to minimise total cost of ownership, system complexity and feature inconsistency. Identify alignment of business wide requirements / features in line with telephony system capability.
- Operational:
    - Replace end-of-life Operational Telephony Network assets with suitable next generation solution that best satisfies operational (CEOT and Incident / Emergency Response) processes and requirements – Tadiran first generation F-series as initial priority;
    - Replace the End-of-Life CEOT Control Room BT-Console System and mobile radio Line Despatch Terminals to enable consolidated handling and head-end abstraction of all operational (voice) communications (including landline, mobile phone and mobile radio) – identify opportunities for integration with CEOT Outage Management System and other systems to maximise efficient outage management practices, operations and co-ordination of activities;
    - Replace end-of-life mobile radio (field) handsets in line with service and/or technology transition;
    - At time of asset replacement, identify opportunities to leverage and/or integrate CEOT Outage Management System(s) to maximise efficient outage management practices and activity co-ordination;
    - Migrate traditional Plain Old Telephony Services (POTS) to NBN service equivalent (where required) to maintain alternative voice services (for operational purposes) to Terminal station sites (in line with NER requirements).
- Enterprise:
    - Identify opportunities to integrate unified communications (mobility and collaboration) workforce capability during enterprise/office telephony replacements / refresh.
- Customer:
    - Improve network outage notification capability to network customers to improve call cue loading, customer wait times and call centre performance;
    - Simplify customer call (performance) reporting capability in line with regulatory requirements.

Supporting Infrastructure Strategy

- Replace batteries at risk of failure within the next five years.
- Enable extended back-up power capability through use of external diesel generator capability (or alternative technologies) to ensure uptime during extended (mains) power outages.
- Replace air conditioning systems based on (temperature) performance and asset condition.

Operational Support Systems Strategy

- Replace end-of-life network management systems hardware and software, including DR capability, in line with enterprise server architecture principles.
- Existing supporting applications to be kept current in line with vendor software version upgrades and associated vendor support framework.
- Integrate overarching OSS capability into enterprise OSS System(s) where practical and cost effective. Adopt OSS capability in line with efficient service delivery, monitoring and reporting practices.

Security Strategy

The AusNet Services' Information Security Strategy aims to:

- Align ICT initiatives with the NIST Cybersecurity Framework – Identify, Protect, Detect and Respond;
- Improve and enhance existing information and cyber security capability (in line with industry best practice) commensurate with the risk and potential impact.

The following security initiatives are outlined in the context of the overarching IS strategy.

1.1.1 Implement and Integrate SIEM visibility to ICS field deployments

- Implement Network Security Monitoring (NSM) and allow for remote forensic investigation and reporting by SOC and InfoSec teams.
- Implement anti-tamper alerts on all cabinets or rooms that house ICS equipment, Satellite, 3G/4G or radio gear used for ICS.
- Implement Passive Vulnerability Assessment toolsets specifically for the ICS environment.
- Install sensors at selected terminal stations and zone substations for un-authorised RF communication to detect and alert on potential "drop bots" or un-authorised communications devices for un-authorised access at remote sites.
- Configure existing devices to point system logging and all operational system logging and backhaul communications logging into the SIEM solution including cybertec modems, routers and ruggedcom switches in the environment.

1.1.2 Implement centralised Authentication, Authorisation and Audit for ICS environment

The strategy is to uplift the existing zone substations to centralised authentication proxy to capture all device access and configuration for legacy systems that do not support in-built access controls.

- Implement authentication proxy to enforce authentication, and automated revocation / continuous audit of access to any new or legacy ICS device, incorporating lockout policies to reduce risk of brute force attempts.
- Integrate auth-proxy to SIEM with audit tools to govern operational practices to remove, disable or rename default system accounts, enforce account lockout policies, and use of strong passwords and alert to SIEM.

2 Introduction

2.1 Purpose

This document describes the Asset Management Strategies for Communication Systems in the AusNet Services Victorian Electricity Transmission Network.

2.2 Scope

This asset management strategy applies to all communication systems associated with the Victorian electricity transmission network, such as:

- Communications Bearers, including:
  - Fibre optic cables;
  - Copper (supervisory) cables;
  - Microwave Radio systems, and
  - Power Line Carriers.
- Communications Network Technologies, including:
  - Wireline
    - Digital multiplexers e.g. SDH, PDH, WDM;
    - (Operational) packet routers and switches;
    - VF and Teleprotection systems.
  - Wireless
    - Telstra 3G Services for Tower Monitoring.
  - Gateway
    - Consolidated routers, switches, firewalls, load balancers, opimisers etc for similar traffic types;
      e.g. Telephony Services Gateway, SCADA Services Gateway, Metering Services Gateway.
  - Telephony
    - Operational voice systems (e.g. PABX's);
    - CEOT head end (answering) systems;
    - Mobile radios;
    - Customer Call Centre system(s).
- Operational Support Systems, including:
  - Telecommunications Network / Element Management Systems;
  - Overarching manager-of-managers.
- Supporting (communications) facilities, including:
  - Radio buildings, towers and connected devices;
  - (Communications) DC battery systems;
  - (In building) communications cabling and interfacing systems, and
  - Communications room/building air conditioning systems.

2.3 Objectives

The objective of this asset management strategy is to provide an overview of:

- AusNet Services' existing communications technology and associated services;
- Existing assets, their service age and condition;
- Key issues and drivers; and
- Strategic initiatives to address the issues and to meet the business requirements and regulatory obligations.

2.4 Reference Documentation

This asset management strategy forms part of a suite of documentation that supports the management of AusNet Services' assets, which include the following:

- AMS 10-56 – Communications Systems – Transmission (ver. 1.1, developed in 2012);
- AMS 10-01 – Asset Management Strategy – Transmission Network;
- AMS 10-68 – Asset Management Strategy – Secondary Systems;
- AMS 10-107 – Asset Management Strategy – Communications Sites;
- AHR 10-56 – Communication System Asset Health Report – Transmission;
- Information Security Strategy 2015 – 2019; and
- Information Security Technology Plan (ISTP): 2016-2020.

3 Communications Services

AusNet Services maintains and operates communications infrastructure and technologies for a range of operational applications and services that are critical to the effective and economic operation of the Victorian extra high voltage (EHV) electricity transmission network.

The range of applications supported by Communication services can be generally categorised into the following categories:

- Tele protection;
- Control and monitoring;
- Real Time Monitoring and Control (SCADA);
- Operational Voice (substation and customer systems);
- Asset Data Gathering;
- Engineering Access;
- Video Surveillance & Security systems;
- Smart Grid applications;
- Business systems.

These services are enabled through various telecommunications technologies, including bearers, wireline and wireless, connecting communications network equipment, supporting infrastructure (e.g. battery systems, radio towers) and back-end IT systems such as operations support systems (OSS). An overview of how these various segments fit together is shown in Figure 1 below.

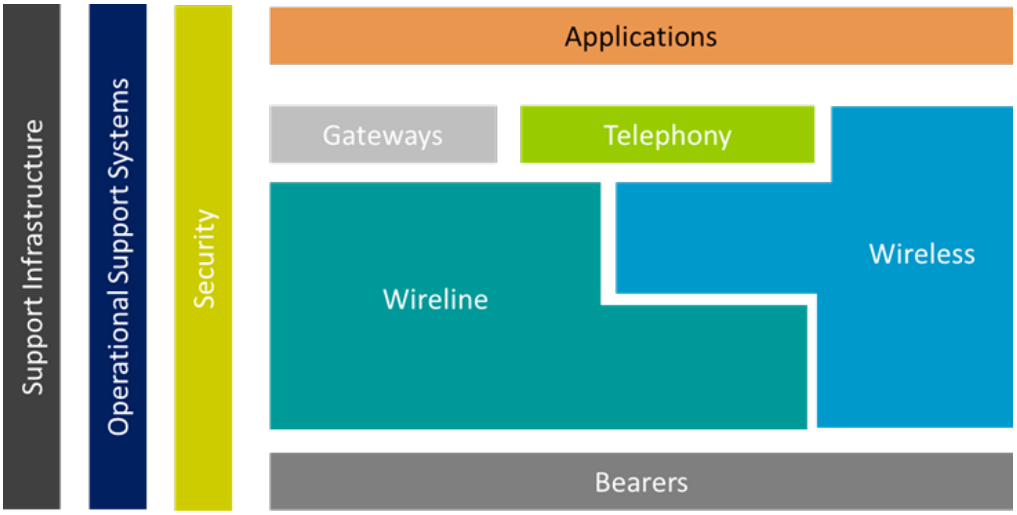

Figure 1 – Overview of the AusNet Services Communications Segments

Bearers	:	Fibre Optic Cable, Microwave Radio
Wireline	:	WDM, SDH, PDH, MPLS, IP, Ethernet
Wireless	:	3G, 4G, WiFi
Telephony	:	PABX, Mobile radios, Voice head End Systems, Call Centre System
Gateways	:	Consolidated Routers, Switches, Firewalls, Load balancers, Wan Optimisers
Security	:	Firewalls, SIEM
Operational Support Syst.	:	Element Management Systems (EMS), Network Management Systems (NMS)
Supporting Facilities	:	Battery, Cabinets, Air Conditioners

Communication Systems

Communications services have a range of technical and functional requirements, some of which are unique to the power utility industry. In general, the requirements associated with communication services are differentiated by four main "quality" factors – reliability/availability, (end-to-end) performance, bandwidth and security as illustrated in Table 2 below.

Figure 2 – Requirements for Communications System

Each communications service application may have varying requirements that place different levels of significance or reliance on the four factors outlined in Figure 2 – Requirements for Communications System. For example, *protection services* typically require high end-to-end channel performance (e.g. latency), are highly critical (i.e. reliability), require robust security measures to ensure correct operation, but at the same time typically require little bandwidth (in comparison to other communications services).

Figure 3 attempts to illustrate the relative difference of the various application requirements on the communications systems (indicative only), where highly critical and end-to-end performance sensitive applications are located in the upper right hand quadrant, low criticality / performance applications in the lower left quadrant, and "bubble" size indicating relative bandwidth requirements (per application).

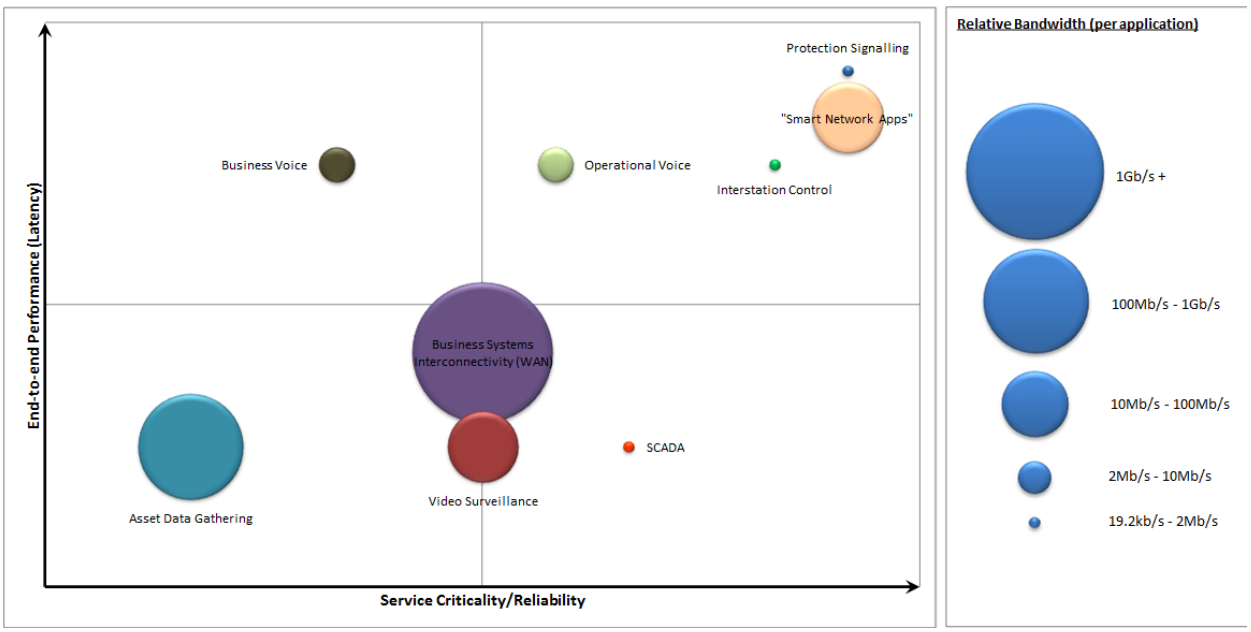

Figure 3 – Comparison of communications service application requirements

4 Asset Summary

AusNet Services' communications network assets span all transmission network sites within Victoria, interconnecting telecommunication between various electricity transmission assets, including Victorian transmission network market participants (e.g. generators) – see Appendix A: Current and Future Communications Network Map. Additionally, interconnectivity is extended interstate to other Transmission Network Service Providers (TNSP's) in South Australia, New South Wales and Tasmania.

In total, AusNet Services owns and/or operates communication related assets at 110 different geographical locations (see Table 1), including terminal stations, Control Centres, administrative offices, mountain top (radio) sites and other market participant locations.

Transmission Communications Sites		Quantity
AusNet Services' sites	Terminal Stations	46
	Radio Sites	30
	Data / Control Centres	2
	Office / Administrative	6
Non-AusNet Services' sites	Other Authorities	26
	Total Communications Sites	110

Table 1 – Transmission Communications Sites

The communications assets, located at the various (transmission related) communications sites, are grouped into the following technology domains:

- Communications Bearers;
- Wire Line Technologies;
- Wireless Technologies;
- Telephony Technologies;
- Gateway Technologies;
- Supporting Facilities;
- Operational Support Systems (OSS).

Security technologies deployed in these communications sites are an overlay to the communications network, and cover the same locations. All groupings of communications categories include a security element in their implementation, with specific security related assets and services discussed in section 4.8 of this AMS.

4.1 Communications Bearers

Communication bearers are the telecommunications interconnectivity medium that provide the "highways" on which individual communication services can be transported from one physical location to another.

The AusNet Services transmission telecommunication system consists of the following bearer technologies:

- Optical Fibre Cable:
  - Optical Ground Wire (OPGW);
  - All Dielectric Self Supporting (ADSS);
  - Underground (U/G).
- Copper Supervisory Cable:
  - Underground (U/G).

- Radio:
  - Point-to-point Microwave (M/W) radio.
- Power Line Carrier (PLC)
- 3rd party Telecom Services (ISDN, ADSL, BDSL, Frame Relay, 3rd Party Fibre).

Table 2 and Table 3 provide a summary of Communication Bearer by type and length.

Cables		Qty	Total Length (km)
Optical	ADSS	35	278
	OPGW	57	1,819
	U/G	153	47
Copper	U/G	148	

Table 2 – Communications Bearers Asset Summary

Other bearer systems	Quantity
Point to point Radio	45
Power Line Carrier	47

Table 3 – Other Communications Bearer Technologies

4.1.1 Optical Fibre Cable

Optical fibre cables provide benefits over other telecommunications bearers due to the:

- Increasing predominance and maturity of optical communications (interfaces) in the telecommunications and utility equipment markets;
- Inherent opto / electrical isolation and EMI resilient properties of optical fibre glass;
- High data bandwidth/throughput capabilities (relative to other alternatives) provided by optical and laser technologies;
- Relative immunity to environmental conditions (e.g. rain events, electrical noise, etc.)

Use of optical bearer technology within AusNet Services (and its predecessors) began in the late 1980's. Its use has continued to grow as legacy bearer technologies such as supervisory (copper) cable and power line (carrier) have required replacement and end-devices have evolved from analogue to digital equivalents.

4.1.1.1. OPGW

OPGW bearers are the predominant optical bearer cable technology currently utilised within AusNet Services. OPGW has benefits over other bearer alternatives through the leveraging of existing electrical network ground-wires and EHV towers (as a physical bearer) and contributing high availability / low failure rates that is characteristic of the physical infrastructure. OPGW installations are typically driven by operational telecommunications requirements (for electrical network purposes) and/or condition based replacement of existing ground-wires. Recent OPGW initiatives have facilitated new installations in the Latrobe Valley (various lines) and in the metro area on the ROTS-RTS 220Kv line. These works have enabled end-of-life replacement of copper supervisory cables (in the Latrobe Valley) and ADSS cables (between MTS and RTS on electricity distribution poles).

4.1.1.2. ADSS

ADSS bearers are strung on distribution electricity poles (both within and without AusNet Services' Distribution region) to provide optical bearer(s) between transmission sites. ADSS provides particular benefit when OPGW (or other) bearers cannot satisfactorily provide the (redundant) bearer requirements of a particular site. Some ADSS cables have progressively been replaced by equivalent OPGW fibre cable when the opportunity has arisen.

4.1.1.3. U/G OFC

Underground optical fibre cables provide the interconnection of equipment in adjacent buildings or sites, and enable the connection to other optical bearer assets on distribution poles (ADSS) and EHV towers (OPGW). These cables total approximately 47 km in length.

4.1.2 Copper cable

Copper supervisory cable use within the transmission network is largely limited to the Latrobe Valley region, between power stations and terminal station sites. The cable has not been extended or added in over 30 years due to technology migration / obsolescence.

Recent projects have installed optical fibre cable as a replacement technology for copper supervisory. The installation of optical fibre (OPGW) bearers in the Latrobe Valley has been completed. Full decommissioning of copper cable will be completed when migration of remaining legacy services (off the copper onto equivalent optical technology) is completed.

4.1.3 Point-to-point Microwave radio

Point to point microwave radio bearers typically provide digital communications bearers to sites in regional areas where the distances and/or viable alternatives necessitate. For sites with mission critical protection services, radio links are not relied upon as the sole bearer technology due to the risk / likelihood of correlated/simultaneous failures (e.g. radio path fading due to weather events). For this reason, radio bearers primarily provide supporting bearers (to other bearer technologies) for redundant (route) purposes. It is anticipated that some radio bearers will be decommissioned when suitable redundant (optical) alternatives become available (in line with network redundancy requirements).

4.1.4 Power Line Carrier

Power Line Carrier (PLC) systems modulate communication signals onto EHV lines to enable signalling between the two ends of a line. They are a narrowband technology enabling low data rate (e.g. 9600 bps) and voice signals between sites and only suitable as a bearer choice when data rate, protection scheme or other application requirements permit. They remain the sole means of (operational) communications to transmission sites in north western Victoria, across the South Australian border (from Heywood) and across the NSW border at Redcliffs (Mildura). Wind farm network connections in the north western region and over the South Australian border are currently driving some PLC replacements and/or reconfigurations to accommodate the requirements associated with generator interconnections to the transmission network.

4.2 Wireline Technologies

Wireline technologies enable services to physically access the communications bearers and can be considered as telecommunications "highway on-ramp" for communications services and applications.

Within the AusNet Services environment, there are three Wireline networks that support the various applications of Tele-protection, Asset Data gathering and monitoring, SCADA and Corporate Communications. They are:

- Operational Data Network (ODN);
- Operational Management Network (OMN);
- Corporate Network.

4.2.1 Operational Data Network (ODN)

The Operational Data Network (ODN) is the new name for the communication network which was previously referred to as the Operational Network. ODN is the most critical communication network for AusNet Services' operations. The ODN provides carriage for the following three key applications:

- Tele-protection Systems;
- SCADA control traffic;
- Operational Telephony Network (OTN) for electricity network operations.

The ODN carries Protection and SCADA data traffic for the EHV transmission electricity network at Terminal and Generator stations. The current ODN is based on a combination of Time Division Multiplexing (TDM) and Wave Division Networking (WDM) technology.

The TDM layer is split into two layers using Plesiochronous Digital Hierarchy (PDH) as its access network, and Synchronous Digital Hierarchy (SDH) as its aggregation & transport network.

Wavelength Division Multiplexing (WDM layer) is typically used to augment the transport (TDM) layer to either extend the geographical distance between the SDH nodes or address optical fibre capacity limitations. There are two types of WDM technology implemented by AusNet Services. These are Coarse Wavelength Division Multiplexing (CWDM) & Dense Wavelength Division Multiplexing (DWDM).

In some cases, Teleprotection equipment is required to provide the interface between the application (e.g. protection) and the ODN, enabling the reliable transmission of discrete protection controls end-to-end between (remote) IED's. Voice frequency (VF) signalling systems that interface some legacy signals (e.g. controls and alarms) to a voice frequency equivalent (300-3400Hz) have been replaced by their digital equivalents in all locations except where PLC bearer technology requires VF transmission for signalling purposes. These will be maintained until associated PLC bearers are replaced.

Table 4 provides a summary of Operational Data Network (ODN) assets.

Multiplex (Digital) Network		**Quantity / Nodes**
WDM	DWDM	20
	CWDM	10
SDH		150
PDH		409
Teleprotection Systems		297

Table 4 – ODN Technology Asset Summary

4.2.2 Operational Management Network (OMN)

The Operational Management Network (OMN) is the new name for the communication network which was previously referred to as the Asset Data Gathering (ADG) network. In the AusNet Services environment, the OMN provides engineering access to staff for remote management and interrogation of various power network and communication devices and carries sensitive information about power network management settings. Other networked applications include on-site corporate system access for field staff, video monitoring of stations and assets, and secure (electronic) access and logging to sites. This network has been built based on Packet Switched technology and consist of switches and routers. OMN spans 44 locations and connects to over 1300 IED's at terminal station sites. The sites are predominantly connected via AusNet Services' owned bearers and communications infrastructure. Where there is no AusNet Services' bearer or communication infrastructure, or existing infrastructure is technologically unsuitable, other 3rd Party bearers and services (e.g. Telstra services) have been used to connect OMN sites.

The OMN supports the following key applications:

- Remote engineering access to power system intelligent electronic devices (IED's);
- Asset data gathering information from intelligent electronic devices (IED's) and systems;
- Management access to communications access devices (e.g. management of communication network switches, routers & serial servers);
- Video monitoring of terminal station sites and associated assets;
- On-site field worker access to corporate IT systems.

Table 5 provides a summary of OMN Assets.

Operational Management Network (OMN)		Quantity / Nodes
Managed IED's / Devices		2456
Network Elements	Routers	4
	Switches	107
	Serial Servers	126

Table 5 – Operational Management Network Asset Summary

4.3 Wireless Technologies

Wireless technologies are currently limited to mobile (GPRS and 3G) 3rd party services at remote weather/environmental monitoring stations located on EHV towers. These devices (approximately 10 in total) relay relevant weather and status information to the master SCADA system for monitoring and system loading purposes.

Similarly AusNet Services has recently rolled out tablets for operation staff as part of the mobility offering under Project Workout. This solution is based on a combination of Telstra 3G (when not on site) and WiFi (when onsite).

It is anticipated that telecom service providers will focus their investment into 4G and carrier Ethernet, resulting in eventual migration away from 3G services, estimated at around year 2020.

4.4 Gateways Technologies

Gateways can be seen as a collection of services and functions that are required when traffic comes into (and going out) AusNet Services from (and to) external 3rd parties. The concept of a gateway is to group / consolidate similar individual external services/links (and associated equipment), into a common shared service/link (and associated equipment).

Following this approach it is envisaged that a simplification of the service and equipment landscape can be implemented which will result in operational efficiency and savings.

The following gateways have been planned to consolidate the multiple individual services that exist today:

a) Telephony Services Gateway;
b) Internet Services Gateway;
c) Cloud Services Gateway.

4.5 Telephony Technologies

AusNet Services heavily relies on voice communications (aka telephony) for communicating between staff, external parties and customers. The telephony domain currently includes:

- Operational Telephony Systems;
- Business (Enterprise) Telephony Systems;
- Customer Telephony System (e.g. Call Centre).

4.5.1 Operational Telephony Systems

Operational telephone systems are intended to provide high reliability telephony (voice) capability to operational sites and staff for the purpose of operating and maintaining the electricity network. Being a combination of AusNet Services' owned and 3rd Party service provider solution (Telstra's StateNet Mobile Radio Network), the Operational telephony systems can usually be relied upon during electricity network events.

Table 6 provides a summary of Telephony Assets.

Telephony		Quantity / Nodes
Operational Systems	PBX's/exchanges	43
	BT Console ITSp41 (head-end) System	1
	BT Consoles (turrets)	5
	Mobile Radio end-points	50

Table 6 – Telephony Technology (Operational) Summary

Operational telephony consists of the following:

Operational Telephone Network (OTN) – consists of Tadiran Coral IPx PABX and handsets at terminal station sites. Gateways are provided to AusNet Services' control room (CEOT) front end (BT console) and other controlling authorities that have interconnecting interests to AusNet Services' electricity transmission network. It is designed to provide voice communications under typical operational scenarios (for example when carrier services are adversely impacted by a power outage).

Control Room (CEOT) Console systems – the BT trading console system and mobile radio Line Despatch Terminals (LDT) provide a front end (via turret interfaces) to voice and mobile radio communications within the Control Room (CEOT) environment, enabling features that best enable the managing and prioritising of operational calls to/from the control room. These systems interface with the OTN, PSTN (public carrier) and mobile radio networks.

Mobile Radio – the StateNet Mobile Radio (SMR) network is a Telstra public wireless network service providing emergency radio (voice and data) communications to 95% of the state. Field staff largely use this network for critical remote voice communication and where service coverage or performance is limited with other mobile services (e.g. mobile phones).

Public Voice Services – the PSTN network is used to communicate with stakeholders not on the OTN network, or as an alternative/back-up means to AusNet Services' internal / private systems (e.g. PSTN phones at Terminal Stations). Mobile phone services (e.g. 3G) are also used by field staff for operational purposes, supported by other dedicated systems (e.g. mobile radio) when circumstances (e.g. mobile phone coverage and/or channel capacity) require.

4.5.2 Business and Customer Telephone Systems, Public Carrier & Other Telephony

Business and customer (call centre) telephony, public carrier land lines (non-Network related), mobile phones, desktop unified communications and video conferencing all form part of and are included in the ICT Strategy[1].

4.6 Supporting Facilities

Communications facilities consist of assets that are essential to supporting the communications system, but do not actively carry or transport communications traffic themselves.

These can include:

- Antenna towers and associated attachments;
- Radio site buildings, fencing, security systems;
- Batteries, chargers, dc-dc converters and solar panels;
- AC mains power systems and diesel generators;
- Air Conditioning systems.

Table 7 provides a summary of communication facilities.

Communications Facilities		Qty
Radio Infrastructure		
Radio Sites*		24
Radio Towers	Lattice type	30
	Pole type	6
Battery Systems		
	12V	3
	24V	20
	48V	175
Battery Chargers		251

* *Dedicated radio sites not shared with electricity site*

Table 7 – Communications Facilities Summary

4.7 Operational Support Systems

Operational Support Systems (OSS) assist in the monitoring, maintenance, administration and operation of the telecommunications network. These include:

- Telecommunications Network and/or Element Management Systems (EMS/NMS) – providing network status, fault and performance information on (vendor specific) telecommunications components that form the telecommunications network;
- Overarching “manager-of-manager” – provides an overarching network wide view for fault and event management across various vendors and network technologies;

[1] Information and Communication Technology Strategy CY2017 – CY2021 Electricity Transmission Network which forms part of the Non-Network section of the overall TRR Submission.

Table 8 provides a summary of OSS assets.

Communications OSS Systems	Qty
Element or Network Management Systems	6
Event / Fault Monitoring Systems	3
Mediating / Aggregating Devices	5

Table 8 – Communications OSS Systems Summary

4.8 Security Systems

From a Wireline perspective, currently transmission sites are secured by:

- Configuration of Access Control Lists (ACL's) of on-site (OMN) networking equipment for all connections on backhaul infrastructure, or on a carriers' private cloud service;
- Use of 802.1x on all on-site networking equipment such as switches.

More recent site implementations have seen embedded firewalls configured in some operational networking devices to further secure data traffic to/from operational station sites. Further enhancements to (network) cyber security is planned as part of, and in line with wider enterprise ICT security initiatives

As part of the evolution of both the Operational Data Network (ODN) and the Operational management Network (OMN), security capabilities and enhancements will be rolled out as part of replacement projects. This is particularly important as new packet (IP/Ethernet) based technology is introduced.

5 Service Age and Condition

Evaluation of communications asset "condition" is largely based on two major factors:

- **Fleet Condition Factors** – There are three factors that contribute to the 'Fleet Condition':
  - Ability of the fleet of assets to meet the Health & Safety Regulations and Code requirements;
  - Ability of the fleet to enable Regulatory Requirements to be met on an ongoing basis;
  - Ability of the manufacturer to continue supporting the fleet of assets (particular technology or model).
- **Component Factors** – These are the factors that identify the technical capability and mechanical / electrical integrity of the asset to perform its expected functionality and capacity.

Fleet Condition factors are particularly important for the communication assets in which we typically interoperate multi-vendor network devices and vendors give little lead time for product end-of-life. While there may be no immediate failure indications in "Component Factors" that justify an asset repair / replacement, vendor declared end-of-life of a particular fleet pose a significant challenge to:

- Augment and/or add to the network (when required) due to a finite quantity of compatible hardware and software / firmware components for existing network elements;
- Repair and/or replace existing components due to limited spares and vendor support.

Taking these factors into consideration, a matrix of condition scores has been derived to classify the Asset condition. The scores are as of year 2015. Table 9 provides the Asset Condition matrix used in this document. More details related to calculation of "C" values can be found in the AHR 10-56- Communication System Asset Health Report.

Condition Score	Condition Description	Summary of details of condition score	Remaining Service Potential
C1	Very Good	- Assets are generally less than 20% of average asset life old and in good operating condition with no history of significant defects or failures. - Manufacturer support and spares are readily available. - Routine maintenance and continued condition monitoring is recommended.	95%
C2	Good	- Assets are in better than average condition for the service age and technology type. - Assets do not require intervention between scheduled maintenance. - No trends of serious deterioration in condition or performance have been recorded. - Manufacturer support and spares available.	70%
C3	Average	- Assets with an average condition for the respective service age and technology type. - Assets typically require increased maintenance or monitoring. - Spares are being used to replace damaged components. - Manufacturer support is becoming limited. - Assets are showing signs of deterioration in condition or degradation / constraint of performance.	45%

Condition Score	Condition Description	Summary of details of condition score	Remaining Service Potential
C4	Poor	- Assets are in worse than average condition. - Manufacturer support and spares is typically not available. - Reverse engineering, salvaging parts from retired equipment or in situ repair has become the most practical solution. - Specialist targeted maintenance is required to manage specific known defects.	25%
C5	Very Poor	- Assets are typically maintenance intensive and have a history of significant failures. - Assets are approaching the end of economic life. - Maintenance to restore acceptable condition is very limited due to lack of spare parts and lack of experience and skill required to maintain the asset. - Assets are no longer supported by the manufacturer. - Maintenance of assets is typically no longer economical compared to asset replacement.	15%

Table 9 – Asset Condition Scoring Matrix

5.1 Communications Bearer Links

Figure 4 provides the condition summary of the communication bearer links.

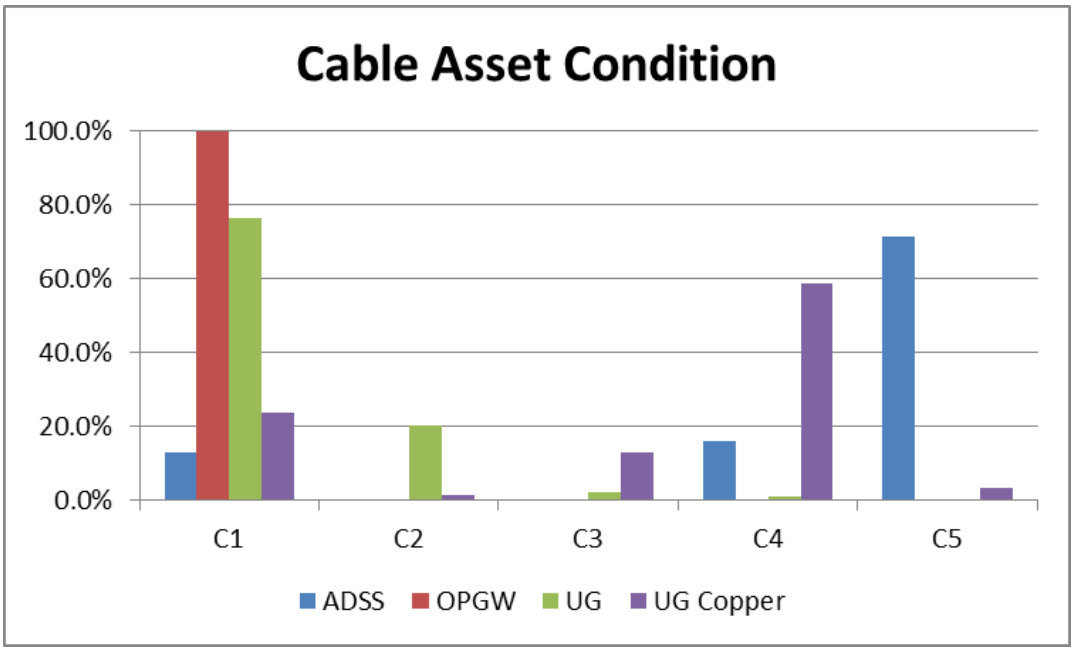

Figure 4 – Cable Asset Condition Summary

5.1.1 OPGW

OPGW fibre optic cables were first installed on AusNet Services' EHV transmission towers in the early 1990's, and continue to be installed as the preferred inter-station optical fibre medium. OPGW cable has proven to be a very reliable and resilient communications medium, with only a once incidence of mechanical failure recorded (due to lightning strike) in the life of AusNet Services' OPGW asset base. The properties of (OPGW) fibre cable will continue to provide the performance and throughput requirements of the underlying applications for the foreseeable future, particularly as operational technologies increasingly migrate to optical equivalents.

There are currently no identified structural or optical condition issues identified with installed OPGW assets that may indicate a requirement for asset works prior to the estimated 35 year asset life. It is expected that ongoing optical and physical condition monitoring will provide the basis for further asset life estimates and works as the earliest installed OPGW assets begin to approach their estimated end of life (at around 2025).

Identified EHV ground wire (non-OPGW) asset replacements (due to physical condition degradation) will be identified and analysed for opportunities in OPGW establishment at the time of planning / business case approval.

Spares are stocked and maintained for OPGW cable (by AusNet Services) to best enable the timely repair in the instance of cable / fibre failure. Repair and/or replacement of OPGW cable is time intensive and expected to be in excess of 8 hours due to the specialised skills, apparatus and planning required in EHV/OPGW line work. For this reason redundant (alternative) bearer routes are established where the risk and impact justify.

5.1.2 ADSS

ADSS cable bearer assets currently total about 280 km of cable length throughout the bearer network. The original install base from the early 1990's is beyond the expected life of 18-20 years, and has experienced comparatively high failure rates (to OPGW) due to its vulnerability to damage from environmental factors such as vehicle accidents and vegetation encroachment. The number of repairs to a particular ADSS cable can have an accumulative adverse impact on the end-to-end optical performance that is dependent on the number and quality of fibre joins / repairs. The use of end device technologies such as Dense Wave Division Multiplexing (DWDM) and higher bandwidth optical components has required more stringent optical fibre parameters, making (the end-to-end) optical performance more critical in modern technology applications. On this basis, the effective life of ADSS cables are in line with estimated asset life expectancy (e.g. approximately 20 years).

The current ADSS replacement program (commenced in 2014/15FY) has identified initial replacements that are prioritised on cable state / condition and on cables that are reliant/suspended on non-AusNet Services' distribution poles. Where possible, OPGW cable (either new or existing) is the preferred replacement/alternative technology (where justified) due to the increased reliability (in line with transmission infrastructure criticality) and reduced ongoing maintenance. Future planned works aims to complete the replacement of identified ADSS cables with new and/or replacement alternatives.

5.1.3 Point-to-point Microwave radio

The current point-to-point microwave radio asset population is made up of various generations of equipment manufactured by NEC, Siemens, Ceragon and 4RF. NEC (2500 model) and Siemens (SRAL) equipment were originally installed around the year 2000 and are no longer supported by their respective vendors. The remaining NEC systems are planned to be replaced prior to 2018, while the sole Siemens system is not currently targeted for replacement as the service is anticipated to be decommissioned. Ceragon and 4RF systems are projected for replacement beginning in 2022/23.

Figure 5 provides the condition summary of the point-to-point radio assets.

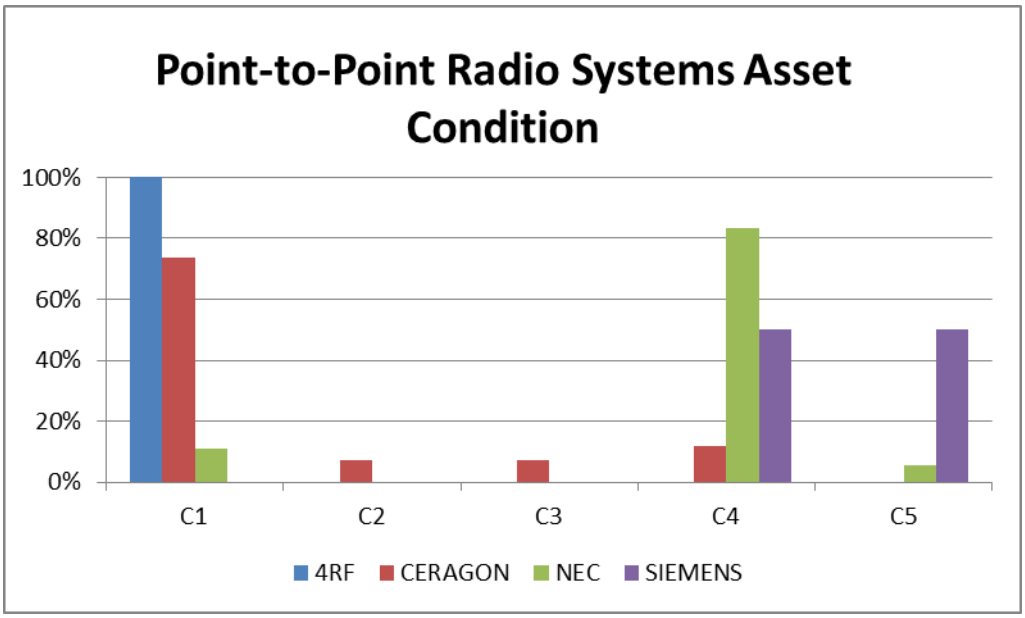

Figure 5 – Point-to-point Radio Asset Condition Summary

5.1.4 Power Line Carrier

Power Line Carrier systems in the NW region are Dimat types (OPC120, OPC180) with sufficient spares and current support from the vendor. Replacement of these systems is expected to commence around 2021/22 to best enable ongoing support and spares availability. Older types (Fuji Denso) have been in service for more than 25 years with increased failure rates and limited spares impacting ongoing serviceability. These systems are targeted for replacement over the next 5 years, including systems at HYTS, MBTS, and RCTS.

Figure 6 provides the condition summary of the power line carrier assets.

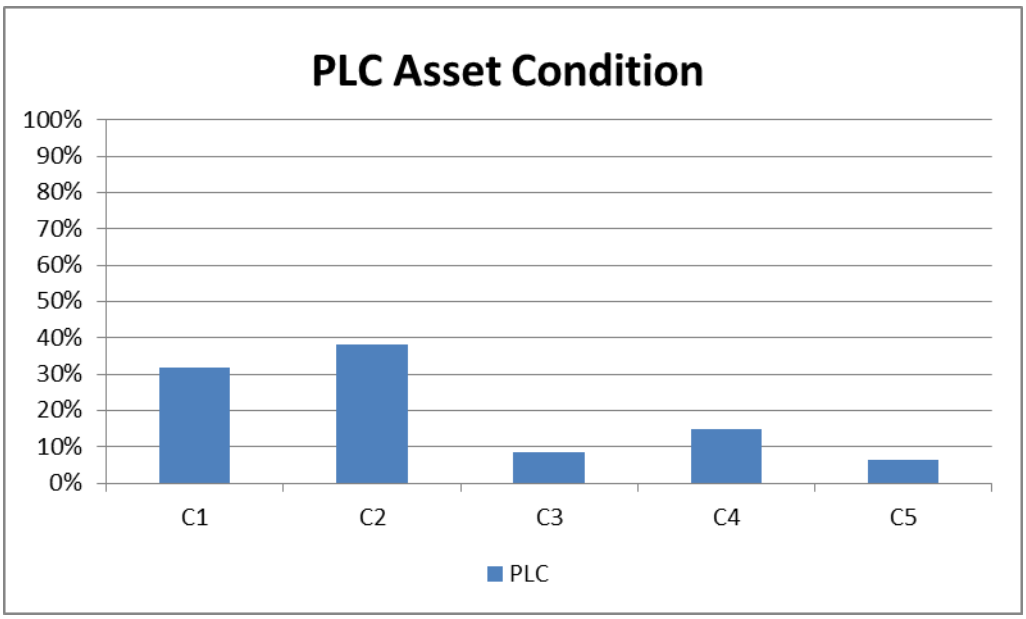

Figure 6 – Power Line Carrier Asset Condition Summary

5.2 Wireless Technologies

5.2.1 Mobile (2G/3G) services

The Telstra 2G (GPRS) network is targeted for switch off by the end of 2016, requiring services to be migrated to alternative networks some time prior to this end date. Current remote devices (e.g. weather monitoring stations) utilising GPRS modems/services are being migrated as part of remote system upgrades. There is currently no projected or announced switch off date for 3G services – based on historical technology lifecycles, projected 3G service end-dates are estimated around 2021/22.

5.3 Wireline Technology

5.3.1 Operational Data Network (ODN)

Operational Data Network (ODN) consists of PDH, SDH, WDM and Tele-protection equipment. PDH equipment manufactured by Nokia has already reached the end of its practical service life and is no longer supported by manufacturers. This asset has a condition score of C5 and the PDH fleet will need to be replaced within the next five years.

Nokia Dynanet PDH assets have been in operation for 25 years. The vendor has notified end-of-support for the Dynanet platform at the end of 2016. Some node replacements have commenced as part of technology replacement programs to enable suitable spares holding for life extension. Follow up replacement programs will aim to replace remaining nodes with suitable (next generation) technology.

The current SDH asset population consists of Nokia, Siemens, Ericsson and ZTE vendor technology. Nokia and Siemens equipment is currently end-of-support, and is maintained through the use of internal spares. Ericsson (OMS 1200) SDH assets can no longer be purchased (last time buy) and will be end-of-support in 2019. ZTE (S200) nodes continue to be supported by the vendor, with no end-of-support dates currently identified by the vendor. Current replacement program(s) aim to complete the replacement of Nokia and Siemens with next generation equivalent(s) over the next 3 years, while a percentage of the Ericsson SDH population will be replaced to reclaim spares for life extension beyond 2019.

WDM assets are currently the ZTE M600 (for CWDM) and the MRV LambdaDriver range (for DWDM). The M600 range is approaching end-of-supply (last time buy) in Q4 2015, and projected to be end-of-support in 2017. Similarly the MRV LambdaDriver is end-of-supply December 2015, with End-of-support notified as end of December 2018. Commencement of WDM asset replacement (with next generation equivalent) is planned in 2018/19.

Digital Teleprotection assets are manufactured by Dewar Electric (DM1200) and currently have no identified support / condition issues. Recent vendor product announcements identify new models that are likely to make the current unit obsolete. Replacement is expected to require some like-for-like (legacy) teleprotection and future IEC61850 functionality.

The following diagram illustrates the condition of the various PDH, SDH, WDM and Tele-protection equipment within the electricity transmission business.

Figure 7 provides the condition summary of the operational data network assets.

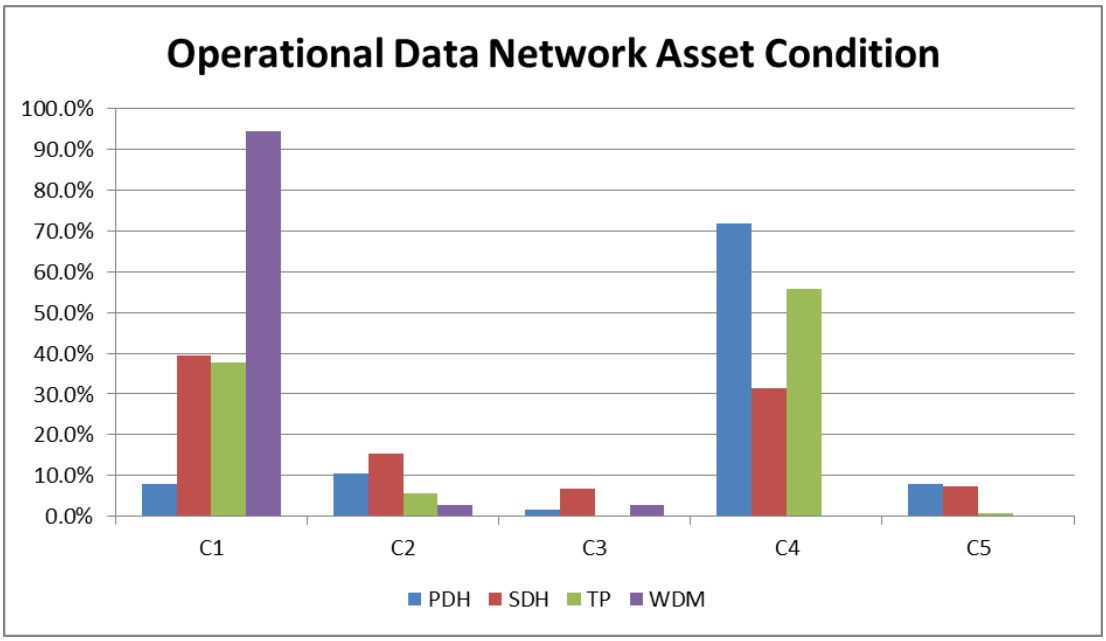

Figure 7 – Operational Data Network Asset Condition Summary

5.3.2 Operational Management Network (OMN)

The OMN predominantly consists of Routers, Switches and Serial Servers manufactured by Cisco, Siemens (RuggedCom) and Lantronix. Typical OMN technology life-cycles are in the 5-7 year range, largely influenced by product support periods maintained / outlined by the vendor. Continued use of out of support equipment in the operational / SCADA environment is identified as a significant risk to the business.

Cisco has announced end-of-support for the 3750 series of switches which will result in a requirement to progressively replace these devices in the next five years. Lantronix serial servers are already end-of-support with approximately 50% of the population already replaced with RuggedCom equivalents. The remaining Lantronix population will be replaced as part of a follow up program. Other OMN assets are projected to be progressively replaced in line with vendor supportability, spares holdings and associated risk.

The OMN asset population and its condition is illustrated in Figure 8.

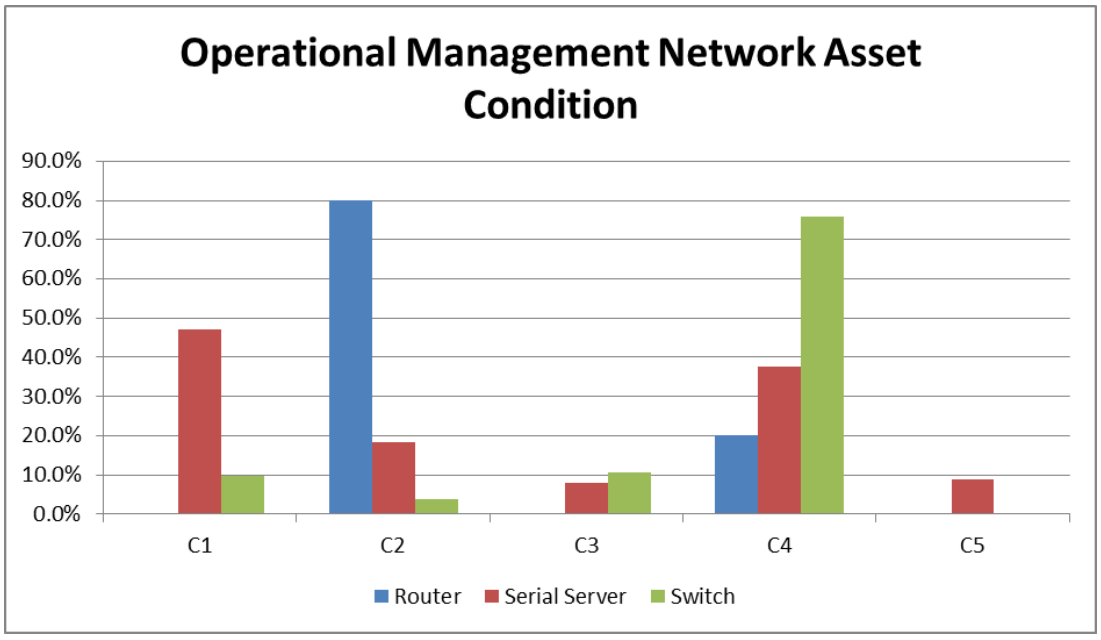

Figure 8 – Operational Management Network Asset Condition Summary

5.4 Telephony Technologies

5.4.1 Operational Telephony Systems (OTN)

The OTN network within terminal stations and depot sites is predominantly based on the Tadiran F series platform, which is based on legacy PBX technology installed in 2004/05. This platform has been superseded by the vendor with the IPx and (more recently) Aeonix platforms, which adopt latest generation IP based telephony functionality. Key hardware components within the F series system are no longer readily available, while software/firmware elements are not supported or updated by the vendor. It is anticipated that the F-series and IPx components of the OTN will require replacement over the next 2-3 years due to limited spares availability and ongoing supportability. Replacement will aim to consolidate disparate voice systems and versions where economic and feasible.

Figure 9 provides the condition summary of the OTN assets.

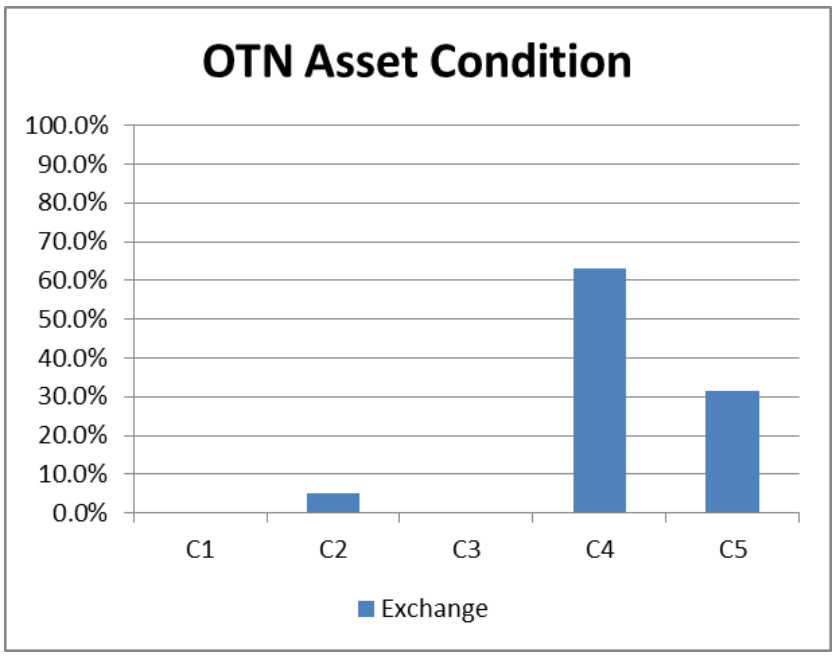

Figure 9 – OTN Asset Condition Summary

5.4.2 Control Room (CEOT) Console Systems

The BT control room console system (Turrets & Head-end) have been in operation since 2005, and is fundamentally based on similar TDM technology to the OTN network to which it interfaces. There are similar support and end-of-life issues relating to key components of the console system, with replacement anticipated in line with a similar time frame to the underlying OTN network. The StateNet mobile radio LDT units are also end-of-life, with replacements co-ordinated with BT console replacement to simplify features and functionality across the CEOT systems.

5.4.3 Mobile Radio (StateNet)

The StateNet mobile radio network is maintained by Tait communications on behalf of Telstra. The network is based on MPT1327 mobile radio technology, and was originally installed for the purpose of shared emergency services use (Police, CFA, SES) throughout regional Victoria. There is currently some uncertainty regarding the medium term future of the network given:

- the supportability of MPT1327 as a technology given the prevalence and market acceptance of newer and more feature rich mobile trunking technologies / standards; and
- Key network users (e.g. CFA) migrating onto alternative (private) mobile radio systems.

Mobile radio (end-point) replacement will have to occur for any change in alternative mobile service technology or provider. It is anticipated that this will likely be required and/or justified in the next 2-5 year time period, either as a result of service provider migration and/or high service cost (to maintain) . Corresponding mobile radio LDT replacements should allow interoperation with multiple mobile radio technologies and should therefore be agnostic to radio technology and service provider.

5.4.4 Public Voice Services

The federal NBN rollout program is currently impacting POTS (Plain Old Telephone Service) services at various sites which currently utilise the service for telephone, (dial-up) modem, fire alarming and fax functionality. The NBN rollout status currently identifies 4 Terminal Station sites (SMTS, BATS, FTS and SHTS) impacted prior to the end of 2016. Migration of existing services at those and future locations (to like-for-like NBN services or alternative solutions) is required to avoid disconnection of those services. The remainder of the NBN program (beyond 2016) is anticipated to impact most POTS services at Terminal Station sites throughout Victoria. These services will require migration to a suitable alternative solution.

Mobile phones and other business related voice services are categorises as Non-Network and are included as part of the ICT strategy.

5.5 Supporting Facilities

Figure 10 provides the condition summary of the supporting facilities assets.

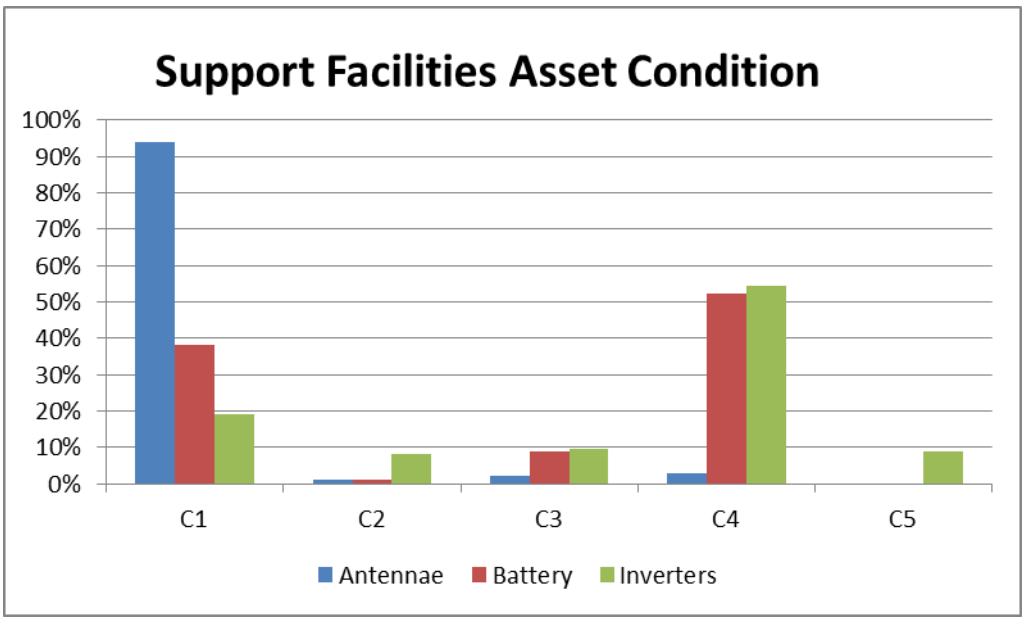

Figure 10 – Supporting Facilities Asset Condition Summary

5.5.1 Radio Towers

Dedicated communication (radio) sites, buildings and antenna structures are generally in good physical condition. Some sites are anticipated to require physical security hardening given their remote nature and lack of modern key access and site monitoring. Recent bushfire experience has also identified bushfire hardening measures for some high-risk mountain top sites that would minimise the risk of building/infrastructure loss during bushfires. Bushfire hardening (of identified sites) has been completed in line with the established standard.

5.5.2 Battery Systems

Over the next 10 years, approximately 70% of communications DC battery systems are expected to require replacement either due to degradation/end-of-design life or requirement to meet increased charge capacities for equipment uptimes. This will be co-ordinated with the decommissioning of fixed remote diesel systems and the introduction of "plug-in" transportable emergency diesel generator set capability.

5.5.3 Air Conditioning

Modern telecommunications technology housed within dedicated communications room/buildings is typically rated up to a maximum temperature of 50 to 55° C, requiring fan-forced cooling and air conditioning systems to maintain optimal operating temperature. Some associated air conditioning systems are expected to require replacement within 5 years due to both age and cooling performance. Room/building temperature monitoring will enable further identification of temperature / cooling performance.

5.6 Operational Support Systems

The condition of OSS systems is related to 3 interdependent elements – server hardware, server operating system (OS) and version of application (management system) software. The majority of current hardware and software elements within the communications OSS environment are at or approaching end-of-support. Most (software) systems also share virtual machine hardware/infrastructure, increasing the impact of potential hardware failure(s). Current support issues within the OSS domain include:

- Server OS:
  - Windows 2000 Server end-of-support (2 instances);
  - Window Server 2003 R2 end-of-support (5 instances).

- OSS Applications:
  - Castle Rock (overarching) event / fault manager approaching end-of-support;
  - Siemens TNMS end-of-support;
  - Ericsson MV36 EMS end-of-support;
  - ZTE EMS/NMS (E300) end-of-support.

Current initiative(s) aim to update hardware and software to latest versions (where feasible) to mitigate risk associated with hardware failures and software (vendor) support and licencing issues. The Ericsson (MV36) function will be migrated to an existing supported instance of the management software. The Siemens TNMS will no longer be required and be decommissioned as part of the ODN replacement programme.

5.7 Security Systems & Services

5.7.1 Network Access Controls (NAC)

802.1x Network Access Control (NAC) was deployed by AusNet Services in 2004. It leverages supplicants on devices, and authenticators reside in the switch functionality to perform a basic Virtual Local Area Network (VLAN) allocation based on device privileges.

While switch hardware and software have been refreshed over this time, the current security technologies have advanced significantly, and now capabilities for network quarantine, system health checks, user-based authentication and dynamic service profiles for users are available to provide higher security capabilities, as well as the option of moving into a vendor supported and standardised deployment. As an early adopter of wired 802.1x network access control, much of the solution deployed at AusNet Services was built for purpose and thus is a custom solution.

5.7.2 Human Machine Interface (HMI)

The HMI's deployed at substations have been refreshed, however the secure configuration of these remote desktops have been in service since 2008. While this configuration was locked-down significantly as a kiosk style deployment at that time, there are significant improvements in security technologies that are required to be installed on this infrastructure to better protect them from remote or physical malicious attackers.

6 Keys Issues and Drivers

Issues and drivers that influence the decisions around technology changes and/or asset replacement are multi-fold. There are specific drivers for each technology category and these are described in general terms in the following sections.

6.1 Regulatory Requirements

The National Electricity Rules (NER) outlines particular performance and redundancy requirements for the electricity transmission assets and associated systems of a Transmission Network Service Provider (TNSP). Requirements that directly impact communications systems include:

- ***Performance*** *– maximum fault clearance times are outlined (S5.1a.8) for systems protecting each particular electricity transmission network voltage, and include times for local and remote end event initiations. These specified times include total end-to-end operation times, of which communications operation and signal transmission times are a component;*
- ***Redundancy*** *– specifies that the system must operate within the performance constraints with any single communications element out of service (S5.1.9d)*;
- ***Availability*** *– all electrical protection systems, of which communications signalling forms a part, are to be available at all times, apart from a maximum period of 8 hours. Otherwise known as the "8 hour rule" (S5.1.2.1d);*
- ***Availability*** *– of a back-up telephone facility independent of commercial telephone service providers (S5.2.6.2).*

The Electricity Safety Act (section 98(a)) requires AusNet Services to "design, construct, operate, maintain and decommission its supply network to minimise as far as is practicable the hazards and risks to the safety of any person arising from the supply network; having regard to the:

a) severity of the hazard or risk in question; and

b) state of knowledge about the hazard or risk and any ways of removing or mitigating the hazard or risk; and

c) availability and suitability of ways to remove or mitigate the hazard or risk; and

d) cost of removing or mitigating the hazard or risk".

In order for AusNet Services to meet above requirements, the transmission network relies on availability of Communications Network for protection, control & monitoring. Hence communications from CEOT to terminal stations, switchyards and SCADA communication need to be maintained with a high degree of reliability and availability.

High reliability and availability drive the need to maintain communication assets in a healthy operating condition, with adequate levels of ongoing maintenance and vendor support.

AusNet Services adopts the ISO27001 framework for security management and governance, and aligns people, process and technology to this international standard. In regard to ICT systems, consideration has been given to NERC-CIP and IEC62443 (ISA99) to ensure that current best practice thinking on securing critical infrastructure is taken into account.

6.2 Technological issues & drivers

6.2.1 Supportability

Adequate and satisfactory support and supply of spare parts from vendors and manufacturers on an ongoing basis is critical to the communications network in order to guarantee the required high level of availability. Due to the rapid advancements in communication technology some product lines are being replaced by modern equivalents on short timeframes. This drives regular technology refreshment.

Support and spare parts for legacy systems quickly become scarce and often requires a long term financial commitment to a supplier to secure spare parts. This is not always economic considering the age of those technologies and hence regular technology refreshment is required. Existing PDH, SDH, WDM and Cisco (3750 & 3550 models) fall into this category.

Rapidly changing technologies and vendors declaring end-of-support, introduce an increasing risk to the Communications Network, which is an influencing factor in this Asset Management Strategy.

6.2.2 Legacy Systems

The communications network is made up of devices from multiple vendors and interoperability challenges arise between different vendors due to proprietary protocols, vendor specific features and evolution of technologies. As a result, changes in one product line may limit the interoperability of the overall network forcing technology refresh and asset replacement. Managing multiple network technologies from different vendors has become increasingly challenging and generally does not provide the necessary economies of scale in the longer term. A strategic objective of AusNet Services is to build efficient automated and integrated processes and systems to support a dynamic business model.

PDH & SDH are now considered legacy technologies and the majority of the (non-utility) users have already migrated away from these technologies. AusNet Services is planning to gracefully migrate these networks and associated services to next generation equivalent technologies.

IEC 61850 is an International Standard for Substation Automation and heavily dependent on Communication System needs outlined in ten broad categories (Ref: Annex – I). AusNet Services is currently analysing suitable IEC 61850 practices and standards for substation automation and requires the Communications systems to be aligned to IEC 61850 requirements and standards. In its current format, the Communication system cannot accommodate the IEC 61850 requirements and changes need to be made in the wireline domain. The forward looking ODN & OMN networks are being developed to provide a suitable pathway for these capabilities.

On the telephony side, TDM based telephony systems (e.g. PABX) are becoming increasingly difficult to maintain as these technologies are migrating to packet based VoIP equivalents. Similarly analogue signal based ‘Plain Old Telephone Services’ (POTS) are also becoming increasingly difficult to support as systems are replaced by the likes of NBN and VoIP service. Office locations and operational sites are being impacted by the reduced maintenance support and require migration of existing analogue Telecom services to digital NBN based equivalents.

6.2.3 Performance

[C.I.C]

This is in contrast to requirements for typical (packet based) enterprise/business IT networks and applications, which are less sensitive to data delay and loss, but require many orders of magnitude greater bandwidth/data throughput. Traffic prioritisation (e.g. QoS marking) is expected to be fundamental to future packet network design and operation, particularly where performance sensitive and business critical applications are required to contend with other “bursty”, high bandwidth network traffic/applications.

Some (legacy) systems present on-going challenges in meeting end-to-end performance requirements. Current Power Line Carrier (PLC) systems introduce a 10ms (approximate) delay to the transmit time of any relayed signal. For the Very Fast Runback (VFRB) scheme, which requires the end-to-end repeating of control signals over a number of PLC systems, the total communications transmit time is approaching the application limit of 100ms. Any further sectioning of the PLC communications will further impact transmission time (and delay the scheme).

6.2.4 Availability / Reliability

To meet regulatory codes (e.g. NER), protection schemes and their communications channels need extremely high availability/reliability performance, which effectively requires two completely independent schemes to operate at all times (when protected plant is in service), except for an 8 hour window for maintenance. When factoring in other plant and equipment unavailability figures, the associated communications systems require an availability of 99.9993%, with a probability of 99.38% for any one circuit operating without failure in a given year.

Systems also need to remain operational during significant transmission network events or outages, assuming momentary or complete (and possibly long-term) AC supply outages. All high availability or critical operational transmission communications traffic is therefore powered off dual DC communications batteries, independent of other system DC supplies. Battery capacity/sizing needs to factor equipment uptime requirements for disaster recovery (after AC system failure), including sufficient battery charger rating for recharging (under full load) on power restoration.

6.3 Information Cyber Security Drivers

6.3.1 Cyber Security Risk

Security threats to critical infrastructure may arise from "hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, natural disasters as well as malicious or accidental actions by insiders"[2] according to the US National Institute of Standards and Technology (NIST). Recent reports indicate that Cyber-attacks on Industrial Control Systems (ICS) are increasingly prevalent, with a high proportion targeting the energy sector. In 2012, ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) reported that 41% of cyber-security incidents across critical infrastructure sectors involved the energy sector, particularly electricity.[3]

For AusNet Services this poses the challenge of building sufficient resilience to withstand cyber-attacks that may impact the integrity of systems and services required for the transmission and distribution of power in an increasingly threatened and sophisticated information security environment. Threats targeting personally identifiable information present similar challenges in maintaining the confidentiality of customer information and securing communication with customers appropriately to protect financial and reputational interests of AusNet Services and its customers.

6.3.2 Security Compliance

The Australian Securities & Investment Corporation released a "Cyber Reslience Health Check, Report 429" in March 2015 overviewing existing legal and compliance requirements for organisations which may require positive steps to be taken with respect to cyber risk, including risk management and disclosure requirements. The report emphasises the importance (for ASX listed companies) to have "..the ability to prepare for, respond to and recover from a cyber-attack"[4]. The suggested framework is based on the U.S. National Institute of Standards & Technology's (NIST) 'Cyber Security Framework for Critical Infrastructure'.

The United States is also addressing specific electricity grid cyber asset security concerns through compliance requirements that are in line with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. These standards have undergone ongoing refinement, with CIP version 5 becoming enforceable (for U.S. utilities) by the end of 2015. Given the current gap in equivalent

2 National Institute of Standards & Technology, *Cyber Security Framework for Critical Infrastructure*, USA, 2014.

3 Industrial Control Systems Cyber Emergency Response Team, *ICS-CERT Monitor (Oct-Dec 2012)*, USA, 2012.

4 Australian Securities & Investment Corporation (ASIC), *Cyber Resilience Health Check, Report 429*, Australia, 2015.

Communication Systems

Australian standards that specifically relate to electricity grid critical infrastructure, AusNet Services identifies the NERC CIP framework as current (electricity) industry best practice and a prudent basis for cyber security enhancement within its mission critical grid systems. Alignment with the NERC CIP framework will also ensure compliance with ISO27019 '*Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry*', and IEC62443 '*Industrial communication networks - Network and system security'.*

The Australian federal government has also highlighted 'telecommunications security sector reforms' (Attorney General, 26 June 2015) that will aim to introduce new law(s) impacting Telecommunications providers that aim to manage national security risks associated with unauthorised access and interference with Australia's telecommunications networks. The (potential) laws may impact AusNet Services' obligations as a Communications Service Provider (CSP) under the Telecommunications Act. Insufficient detail on the proposed Bill currently makes it difficult to assess this impact.

7 Strategies

This AMS contributes to the strategic objectives outlined in the Corporate Business Plan 2015-18. The strategies to be adopted for each component of the communications network are shown in the following section.

7.1 Bearers

- Ensure a minimum of 2 independent communications bearers to each EHV Terminal Station site, in line with EHV plant protection scheme and NER regulatory requirements;
- In line with functional and regulatory requirements, selection priority for new and/or replacement communications bearers to be as follows (where economically justified):
    - AusNet Services' owned fibre (OPGW preferred);
    - AusNet Services' owned Point-to-Point Digital Radio;
    - 3rd Party Fibre Swap (2nd and/or 3rd communication bearer routes);
    - 3rd Party Leased service (2nd and/or 3rd communication bearer routes);
    - AusNet Services' owned Power Line Carrier (where suitable).
- Where applicable, establish and/or maintain a 3rd (independent) communications bearer to select transmission sites where excessive operational risk and repair/restoration times justify;
- Where justified , install OPGW in conjunction with planned EHV ground wire replacement programs;
- Install OPGW fibre on new EHV line construction or refurbishments;
    - Formulate common requirements and standards with AEMO that best enable the establishment of optical communications bearer(s) between stations during new EHV line works or network augmentations.
- Upgrade end-of-life radio links to enable both native TDM and packet based (Ethernet/IP) communications traffic where economic.
- Maintain and/or replace existing ADSS based on end-of-life and/or physical/optical condition degradation when economic;
- Identify ongoing suitability of digital Power Line Carrier technology for long distance (regional) power lines when other alternatives cannot be justified;
- Consider mechanisms to monitor and report optical fibre performance over timeComplete migration of services from copper supervisory cables to suitable bearers.

7.2 Wireless Technology Strategy

- Migrate existing 2G (GPRS) services to equivalent wireless service (3G/4G) prior to service termination date (end of 2016).
- Migrate / 3G wireless technology to equivalent (wireless) service when required.

7.3 Wireline Technologies Strategy

- Identify opportunities for Wireline Networks consolidation where feasible and justified
- Operational Data Network (ODN):
    - Identify and standardise suitable next generation SDH and PDH platform(s) replacement platforms that satisfies existing mission critical (legacy) TDM and (future) packet applications and interfaces;
        - Complete replacement of end-of-life Siemens SDH equipment with next generation equivalent;
        - Commence replacement of Ericsson SDH equipment with next generation equivalent commencing in 2019/20 – establish spares to satisfy ongoing network maintenance and operation prior to complete technology replacement (beyond 2021/22);
        - Continue replacement of end-of-life Nokia Dynanet PDH equipment with next generation equivalent technology in line with SDH replacement program;
        - Commence replacement of end-of-life MRV and ZTE WDM equipment with next generation equivalent.
    - Implement EMS and NMS capability for next generation (ODN) equipment in line with OSS strategy;
    - Progressively migrate teleprotection function onto new generation equivalent (e.g. IEC61850) or replace digital teleprotection (end-of-life) equipment with technology equivalent;
- Operational Management Network (OMN):
    - Identify and standardise suitable network solution(s) that best enables consolidation (where economic) of non-mission critical legacy and future applications and interfaces:
        - This includes assets associated with (but not limited to) Asset Data Gathering, Corporate and AMI networks;
    - Implement EMS and NMS capability for OMN equipment in line with OSS strategy;
    - Implement user access control system for users and devices;
    - Replace end-of-life Routers, Switches and Serial Servers in line with next generation solution(s).
- Communication Design Standard shall be amended to support IEC 61850 applications within and between Terminal stations.
- Develop a centralised network management system capability for both the OMN and ODN network devices
- Reduce the number of network layers and devices through consolidation where economic.
- 3rd Party Leased Services
    - Migrate ISDN (data) services to NBN equivalent (when required);
    - Migrate Business DSL (data) services to NBN equivalent (when required);

7.4 Gateway Technologies Strategy

- At time of asset replacement, identify opportunities (where feasible) to consolidate separate network gateways (that access 3rd party services), including:
    - Internet;
    - SCADA (3G services);
    - Metering (3G services)
    - Cloud Services (if/when required).
- Consolidate multiple Inter-Data Centre link (Richmond and Rowville) gateways;

7.5 Telephony Technologies Strategy

- At time of telephony system replacement, identify opportunities for system consolidation to minimise total cost of ownership, system complexity and feature inconsistency. Identify alignment of business wide requirements/features in line with telephony system capability.
- Operational:
    - Replace end-of-life Operational Telephony Network assets with suitable next generation solution that best satisfies operational (CEOT and Incident/Emergency Response) processes and requirements – Tadiran first generation F-series as initial priority.
    - Replace the End-of-Life CEOT Control Room BT-Console System and mobile radio Line Despatch Terminals to enable consolidated handling and head-end abstraction of all operational (voice) communications (including landline, mobile phone and mobile radio) – identify opportunities for integration with CEOT Outage Management System and other systems to maximise efficient outage management practices, operations and co-ordination of activities.
    - Replace end-of-life mobile radio (field) handsets in line with service and/or technology transition;
    - At time of asset replacement, identify opportunities to leverage and/or integrate CEOT Outage Management System(s) to maximise efficient outage management practices and activity co-ordination.
    - Migrate traditional Plain Old Telephony Services (POTS) to NBN service equivalent (where required) to maintain alternative voice services (for operational purposes) to Terminal station sites (in line with NER requirements).
- Enterprise:
    - Identify opportunities to integrate unified communications (mobility and collaboration) workforce capability during enterprise/office telephony replacements / refresh.
- Customer:
    - Improve network outage notification capability to network customers to improve call cue loading, customer wait times and call centre performance.
    - Simplify customer call (performance) reporting capability in line with regulatory requirements.

7.6 Supporting Infrastructure Strategy

- Replace batteries at risk of failure within the next five years;
- Enable extended back-up power capability through use of external diesel generator capability (or alternative technologies) to ensure uptime during extended (mains) power outages;
- Replace air conditioning systems based on (temperature) performance and asset condition.

7.7 Operational Support Systems Strategy

- Replace end-of-life network management systems hardware and software, including DR capability, in line with enterprise server architecture principles;
- Existing supporting applications to be kept current in line with vendor software version upgrades and associated vendor support framework;
- Integrate overarching OSS capability into enterprise OSS System(s) where practical and cost effective. Adopt OSS capability in line with efficient service delivery, monitoring and reporting practices.

7.8 Security Strategy

The AusNet Services Information Security Strategy aims to:

- Align ICT initiatives with the NIST Cybersecurity Framework – Identify, Protect, Detect and Respond;
- Improve and enhance existing information and cyber security capability (in line with industry best practice) commensurate with the risk and potential impact;

The following security initiatives are outlined in the context of the overarching IS strategy.

7.8.1 Implement and Integrate SIEM visibility to ICS field deployments

- Implement Network Security Monitoring (NSM) and allow for remote forensic investigation and reporting by SOC and InfoSec teams;
- Implement anti-tamper alerts on all cabinets or rooms that house ICS equipment, Satellite, 3G/4G or radio gear used for ICS;
- Implement Passive Vulnerability Assessment toolsets specifically for the ICS environment;
- Install sensors at selected terminal stations and zone substations for un-authorised RF communication to detect and alert on potential “drop bots” or un-authorised communications devices for un-authorised access at remote sites.
- Configure existing devices to point system logging and all operational system logging and backhaul communications logging into the SIEM solution including cybertec modems, routers and ruggedcom switches in the environment.

7.8.2 Implement centralised Authentication, Authorisation and Audit for ICS environment

The strategy is to uplift the existing zone substations to centralised authentication proxy to capture all device access and configuration for legacy systems that do not support in-built access controls.

- Implement authentication proxy to enforce authentication, and automated revocation / continuous audit of access to any new or legacy ICS device, incorporating lockout policies to reduce risk of brute force attempts;
- Integrate auth-proxy to SIEM with audit tools to govern operational practices to remove, disable or rename default system accounts, enforce account lockout policies, and use of strong passwords and alert to SIEM.

Appendix A: Current and Future Communications Network

[C.I.C]