Appendix 5.14: Secondary systems-communications ASP

Regulatory proposal for the ACT electricity distribution network 2019-24
January 2018

evoenergy

Reference Documents

Document	Version	Date
National Electricity Rules	104	19/12/2017
National Electricity Law – National Electricity (South Australia) Act 1996	15.12.2016	15/12/2016
ACT Utilities (Technical Regulation) Act 2014	R6	08/11/2017
Electricity Distribution Asset Management Policy PO1101	2.0	01/10/2015
Asset Management Strategy	V5.0	11/01/2018
Asset Management Objectives	V4.0	12/12/2017
Asset Management System Description	V5.0	12/01/2018
Asset Management Governance Framework	V4.0	12/01/2018
Disruptive Technology – EN 10 Year Strategic Direction Plan	V2.19	28/08/2017
ActewAGL Grid Vision 2016-2046		12/2016
Secondary Systems Strategy	2.0	22/01/2018
ActewAGL ICT Security Standard SM4321	1.0	15/02/2017
ActewAGL ICT Security Framework SM4326	1.0	05/05/2016
Media Sanitisation, Destruction and Disposal Standard	1.0	30/01/2017

Table of Contents

Glossary

Term	Description
ACT	Australian Capital Territory
ADMS	Advanced Distribution Management System
ADSS	All-Dielectric Self-Supporting optical fibre cable
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
ArcFM	Asset management system, incorporating GIS (Geographic Information System)
ASD	Australian Signals Directorate
ASP	Asset Specific Plan
BSD	Business Systems Division
CAPEX	Capital Expenditure
CB	Circuit Breaker
CCTV	Closed-circuit television
CT	Current Transformer
DC	Data Centre
DC	Direct Current
DDoS	Distributed Denial of Service – an Internet based attack on a company's network
DDRN	Digital Data Radio Network
DFA	Distribution Feeder Automation
DG	Distributed Generation
DMR	Digital Mobile Radio
DMS	Distribution Management System
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol version 3
DNSP	Distribution Network Service Provider
DRF	Disaster Recovery Facility
DSD	Demand Side Device
DSM	Demand Side Management
DSS	Distribution Substation
DWDM	Dense Wavelength Division Multiplexing – a method of combining multiple optical signals in a single optical fibre using different light wavelengths
EN	Energy Networks
EV	Electric Vehicle
FCI	Fault Current Indicator

Term	Description
FLISR	Fault Location, Isolation, and Service Restoration
FMEA	Failure Mode and Effects Analysis
GIS	Geographic Information System
HMI	Human Machine Interface – local touch screen interface to RTUs and IEDs
HV	High Voltage electricity circuit – generally 132kV in Evoenergy network
ICCP	Inter-Control Centre Communications Protocol – IEC 60870-6/TASE.2
IED	Intelligent Electronic Device – microprocessor controlled multi-function protection device
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
kVA	Kilo Volt Amperes – a measure of power capacity
kW	Kilo Watts
LAN	Local Area Network
LV	Low Voltage electricity circuit
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
MVA	Mega Volt Amperes
MW	Mega Watts
N-1	Security Standard where supply is maintained following a single credible contingency event
NEL	National Electricity Law
NEM	National Electricity Market
NER	National Electricity Rules
NSP	Network Service Provider
OPEX	Operational Expenditure
OPGW	Optical Fibre Ground Wire
OT	Operational Technology
OTDR	Optical Time-Domain Reflectometer
P90	90th percentile
PMU	Phase Measurement Units
PoF	Probability of Failure
PoW	Program of Work
PQM	Power Quality Monitor

Term	Description
PV	Photo-Voltaic panels (solar panel generators)
QoS	Quality of Service – setting of IP network priorities to ensure minimum performance levels of critical infrastructure
RF	Radio Frequency
RIVA DS	Riva Decision Support (proprietary software system that supports analytical modelling to aid asset management decision making)
RPN	Risk Priority Number
RTU	Remote Terminal Unit
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control and Data Acquisition system
STPIS	Service Target Performance Incentive Scheme
TMR	Trunked Mobile Radio
TNSP	Transmission Network Service Provider
UHF	Ultra High Frequency
Utilities Act	ACT Utilities (Technical Regulations) Act 2014
UTR	Utilities Technical Regulations
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
ZSS	Zone Substation

NOTE *All analysis has been undertaken using 2017/18 real dollars unless otherwise stated. Budgeted expenditure for CAPEX & OPEX excludes indirect costs.*

Document Purpose

This document is an Asset Specific Plan (ASP). It specifies the activities and resources, responsibilities and timescales for implementing the Asset Management Strategy and delivering the Asset Management Objectives for a specific asset class. In conjunction with the other ASPs, it forms Evoenergy's Asset Management Plan, which describes the management of operational assets of the electricity distribution system.

Detailed in this document are the systematic and coordinated activities and practices whereby Evoenergy manages the asset class in an optimal and sustainable manner. Associated asset condition data, performance data, risks, and expenditure are presented and assessed over the asset life cycle for the purpose of achieving the organisational strategic plan.

As part of the assessment of asset management options, a recommended asset strategy is presented with associated Capital expenditure and Operational expenditure forecasts, including a 10 year budget forecast, for consideration by Evoenergy management.

This document has been developed based on good practice guidance from internationally recognised sources, including the Global Forum on Maintenance and Asset Management (GFMAM) and the Institute of Asset Management (IAM). It has been specifically developed to comply with the relevant clauses of ISO55001.

Audience

This document is intended for internal review by Evoenergy management and staff. As part of legislative, regulatory and statutory compliance requirements, the audience of this document is extended to relevant staff of the ACT Technical Regulator and the Australian Energy Regulator.

1 Executive Summary

This Asset Specific Plan (ASP) provides details of the asset management plan specific to a particular asset class, and is an important part of the line-of-sight management of assets from the corporate objectives and strategy level down to the work execution level. For details of the asset management strategy, refer to the *Asset Management Strategy* document. For details of how the policies, principles and strategies from the asset management policy and strategy align with the ASPs that form the overall Asset Management Plan, refer to the *Asset Management Objectives* document.

The communications assets covered by this ASP provide services for operating the electrical network for SCADA and the ADMS, network protection, operational voice, and other operational and engineering data services to substations and field devices. Whilst the primary purpose of the communication systems is to provide enhanced communication capabilities for the critical function of electricity network protection, monitoring and control, the system will support other communications users and capabilities, aimed at enhancing a range of Evoenergy business functions.

Communication assets facilitating electricity network protection, monitoring and control must meet the requirements of regulatory authorities such as the Australian Energy Regulator (AER) as outlined in the National Electricity Rules (NER), and the requirements in the ACT Utilities (Technical Regulations) Act 2014.

This ASP adopts a risk-condition based approach in accordance with Evoenergy's strategic direction to determine the optimal strategy to maintain and replace communications assets over their lifetime. With the advent of newer technologies such as numerical protection relays and other IEDs, there is a growing amount of operational data being collected, transferred, stored and analysed. Additionally, with the increasing penetration of disruptive technologies such as grid-connected solar photovoltaic panels and battery storage, the electrical network is changing from a traditional and stable centralised generation model to a dynamic and potentially unstable distributed generation model. Future requirements for more nuanced monitoring, control and balancing of supply and demand in a distributed generation environment is a key driver for improved data collection and analysis, greater system agility and resilience, and finer granularity of control. This will require a deeper penetration of communications assets into the distribution network in order to ensure that quality of supply is maintained for our customers. The asset management approach employed in this ASP considers the evolving requirements of communications assets in the changing distribution network environment. These requirements demand a high throughput communications network to support the need for highly responsive control of the electricity network, and to handle the amount of data generated.

The communications assets are considered on an individual basis due to the differing technologies utilised in each type of asset. Decisions about replacement or upgrade of the assets will be based on the risk-condition criteria and on the assets' ability to provide required functionality, bandwidth and performance in compliance with business and regulatory requirements, rather than replacing assets based on their age alone.

Accordingly, the condition and technical capabilities of communication assets has been determined as the key criteria that underpin risk-condition based scenario planning analysis for the 2019-2024 Regulatory Period to choose the most viable option from:

- Option 0: Do Nothing. This option does not entail any maintenance or replacement and basically is a run to fail strategy.
- Option 1: Periodic Maintenance with Age-Based Replacement. This option focuses on a like for like replacement at asset end of life.
- Option 2: Optimised Maintenance with Strategic Replacement. This option takes into consideration each communications asset type and selects the optimal strategy for maintenance. Where existing assets are not capable of providing functionality, or where

technology advances in media or protocols render existing assets obsolete, strategic replacement prior to asset end of life is recommended. A greater penetration of communications assets into the distribution network is also pursued as a strategic response to the changing nature of the electrical distribution landscape, as detailed in the *Secondary Systems Strategy*. This option also considers and aligns with protection, SCADA and other asset enhancement/replacement programs, and delivers efficiencies through combined implementation.

Based on the cost optimisation benefit and the health of the assets, this plan recommends Option 2 as the strategy that provides the best cost/benefit while controlling the risk and providing the required functionality. The optimised Program of Work budget for Replacement CAPEX and OPEX is presented in Table 1.

Total Budget	2019/20	2020/21	2021/22	2022/23	2023/24
CAPEX	**370,000**	**550,000**	**430,000**	**595,000**	**360,000**
OPEX	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**
Planned Maintenance (OPEX)	126,000	126,000	126,000	126,000	126,000
Unplanned Maintenance (OPEX)	75,000	75,000	75,000	75,000	75,000
Condition Monitoring (OPEX)	36,000	36,000	36,000	36,000	36,000

Table 1: OPEX and CAPEX Optimised Program of Work Budget

This ASP presents a broad-based program of works in terms of CAPEX replacements for communication assets with obsolescence issues in order to provide enhanced communications to meet future business requirements and considers expected asset growth with a greater penetration of communications assets into the distribution network from planned augmentation projects. It provides an optimised program of work approach for maintenance for managing existing assets and assets under management from planned projects.

2 Asset Class Overview

This ASP covers the Communication asset class within the Secondary Systems asset portfolio. The communications assets within this class are responsible for providing enhanced communication capabilities for the critical function of electrical network monitoring and control. For details of the asset groups contained within the Communication asset class, refer to section 2.2.

2.1 Asset Class Objectives

The asset class strategy presented in this ASP follows the overall Evoenergy *Asset Management Strategy* and *Asset Management Objectives*. The asset class strategy is an integral part of the asset management strategy, with the overall objective to provide safe, reliable and cost effective supply of electricity to customers and compliance with regulatory requirements.

This ASP seeks to meet objectives in the following categories:

Responsible

- Achieve zero deaths or injuries to employees or the public
- Maintain a good reputation within the community
- Minimise environmental impacts, for example bushfire mitigation
- Meet all requirements of regulatory authorities, such as the AER as outlined in the NER, and the ACT Utilities (Technical Regulations) Act 2014.

Reliable

- Tailor maintenance and renewal programs for each asset based on asset health and risk
- Meet network SAIDI and SAIFI KPIs
- Record network status, events and alarms accurately to facilitate effective operations and determine the common failure modes and condition of assets
- Successfully deliver the asset class PoW.

Sustainable

- Enhance asset condition and risk modelling to optimise and implement maintenance and renewal programs tailored to the assets' needs
- Make prudent commercial investment decisions to manage assets at the lowest lifecycle cost
- Integrate primary assets with protection and automation systems in accordance with current and future best practice industry standards
- Deliver the asset class PoW within budget.

People

- Proactively seek continual improvement in asset management capability and competencies of maintenance personnel.

That is, the strategy and ASP must be practical in the sense that it can be implemented, must also be flexible enough to satisfy the future requirements of the Evoenergy network, and must be cost effective and efficient with consideration of both technical and human resources.

2.2 Asset Groups

Communication assets are classified in terms of the communications media and technology that they employ. Table 2 provides a broad-based classification of asset groups within the asset class.

Asset Class	**Secondary Systems Communication**

Asset Groups	LAN Devices:
	  Base Station Ethernet Switches
	  Distribution Ethernet Switches
	  Zone Sub Ethernet Switches
	Media Converters
	Optical Fibre Cables:
	  ADSS Optical Fibre
	  OPGW
	  Underground Optical Fibre
	Pilot Cables
	Power Supplies
	Radio Systems:
	  3G-4G Modems
	  Digital Mobile Radio:
	    Base Stations
	    Gateways
	    Mobile Radios
	  Microwave Radios
	  UHF Radios:
	    UHF Base Stations
	    UHF Remotes
	Tele-Protection Devices
	WAN Devices

Table 2: Asset Classification – Communication Assets

Operations for radio systems and WAN devices are currently managed by the Business Systems Division (BSD) communications group, with Energy Networks Division (EN) as the asset owner and end user. The LAN devices, media converters, optical fibre, pilot cables, power supplies and tele-protection devices are managed by EN as part of the SCADA and protection systems at substations and other field locations. The system architecture consists of a number of different media types, having grown over the years on an as-needed basis.

Historically the UHF radio network was the primary communication system used for SCADA and Evoenergy zone substations, and the majority of chamber substations and field reclosers were also linked through this network. An optical fibre network and IP-MPLS core has been established over the period from 2016 to 2018 and currently extends to all 132kV zone substations, data centres and control centres. It is the primary communications for the SCADA/ADMS network to key sites and also supports a range of other communications services. Moving forward, UHF radio systems and 3G/4G modems will be used for SCADA connectivity at the distribution substation level where optical fibre connectivity is neither practical nor economically feasible.

In 2017-18 the voice radio systems are being consolidated from legacy VHF and TMR systems to a unified DMR system for all control room and field staff communications. DMR maintenance requirements have been considered as part of this ASP.

2.3 Asset Functions

The ADMS SCADA master station utilises the communication system to provide telemetry to all SCADA-enabled network field devices. The communication system also enables compliance with the NER requirements for Inter Control Centre Protocol (ICCP) reporting of system status and performance to AEMO and TransGrid. The future communication system will also support other communications users and capabilities aimed at enhancing a range of Evoenergy business functions.

Evoenergy has installed a redundant optical fibre network as the principal communications network between control centres and zone substations, with an IP-based MPLS multiservice network at its core. Resultant increases in bandwidth provide the capacity to meet the primary monitoring and control function, as well as supporting all of the other identified corporate communications needs. These additional corporate communications needs are described in detail in the Evoenergy *Secondary Systems Strategy* document.

The optical fibre carrier network utilising MPLS technology is scalable while protecting mission critical services with Quality of Service (QoS) prioritisation. It has the capacity to support additional network functions without impacting on the primary electricity network protection and SCADA functions of the communications network. The versatility of the IP-based MPLS network allows for the full integration of the capabilities of substation IEDs, allowing for more detailed monitoring and control of the electrical network and equipment, in addition to the core protection function of the devices.

The Evoenergy communications system is required to service a wide range of business needs, including electrical network protection, SCADA, metering, security, telephony, video and corporate data services. The *Secondary Systems Strategy* is developed around providing a unified communications network to provide services while maintaining cyber security and meeting individual system's service performance requirements. As the core of the communications network is based on high speed optical fibre and a multiservice MPLS network, there is the ability to expand the utilisation of the network to include other desirable functionality such as network control functions, providing corporate LAN access, remote monitoring of a CCTV network and extending centralised access control to the zone substation sites.

An important aspect of the IP-based MPLS communications system is the ability to provide much higher levels of security for the network itself, to prevent penetration or hacking of the communications network. By implementing network segregation with the capabilities of the IP MPLS network, VRFs and VLANs can be set up across the communications system, minimising the potential impact if any of the VRFs/VLANs are compromised. Under this design for instance, protection functions, SCADA functions and the corporate network could be on three different virtual networks. Additional functions can easily be added to the communications network through the configuration of a VRF/VLAN for each function.

2.3.1 Asset Function Definitions

The communications network acts as an interface to facilitate communications between:

- Master control centres and network sites, for:
    - System alarms
    - System event logging
    - Data transfer
    - SCADA control

- Network sites and protection devices, for monitoring of device status and relay settings
- Various networked sites involving zone and distribution substations.

The specific functions of assets in this asset class are described in the following sub-sections.

2.3.1.1 LAN Devices

Communication switches are widely used in the Evoenergy substation networks, providing network infrastructure to connect IEDs and RTUs and then to connect to the station router, 3G/4G modem or UHF radio.

2.3.1.2 Media Converters

Media converters are used to connect serial devices (typically RS-422/485) and copper-based Ethernet devices to the optical fibre network.

2.3.1.3 Optical Fibre Cables

The optical fibre network is Evoenergy's primary communications system. A number of different cabling options are employed, depending on geographical requirements:

- OPGW
- Underground optical fibre
- ADSS optical fibre
- Leased optical fibre from telecommunications providers.

2.3.1.4 Pilot Cables

Pilot cables are used as a communication medium for SCADA communications to some chamber substations, and for translay protection for dedicated 11kV distribution cables. The pilot cables are nearing end of life, and will be phased out and replaced with optical fibre, 3G/4G or UHF radio.

2.3.1.5 Power Supplies

DC-DC power supplies installed in the communications panels provide the required DC voltage for communications equipment. These are typically powered from the zone substation DC supply.

2.3.1.6 Radio Systems

A number of digital radio technologies are deployed throughout Evoenergy's network to provide communication links between the control centres and networked sites in the field. The following types of digital radio are used:

- 3G/4G modems
- Microwave radios
- UHF radios.

With the optical fibre installation project completed, the UHF radios (in conjunction with 3G/4G modems) transitioned from being the primary communications network to providing SCADA connectivity at the distribution substation level (e.g. reclosers, switches, chamber and padmount distribution substations).

In addition to these communications media, the digital mobile radio network provides voice communications for Evoenergy fleet vehicles and portable radios for staff.

2.3.1.7 Tele-Protection Devices

Tele-Protection is a form of protection where devices are located at both ends of an electricity feeder. They are connected by a communications link and act as one scheme (unit protection) utilising the interconnection link between them. The devices are triggered only for faults detected in the section of feeder line between the two devices. The protection function is triggered when comparative value differentials are exceeded. Evoenergy tele-protection is implemented via one of the following:

- Optical fibre links utilising OPGW and underground dark fibre
- IEEE C37.94 protocol over the IP MPLS network
- Digital radio
- Copper pilot cable.

2.3.1.8 WAN Devices

WAN devices such as routers and switches provide control of IP traffic throughout the network. They are scoped and sized to allow for the operation of several VRFs/VLANs simultaneously, allowing the Evoenergy communications strategy to be implemented.

The following devices are included in this asset type:

- MPLS routers
- DWDM optical multiplexers
- Access switches and routers in zone substations.

2.4 Needs and Opportunities

The *Core Communications Network* (WAN) connects to Evoenergy zone substations, switching stations, control centres and data centres. It has the primary function of providing communications service for protection, SCADA, ADMS, operational networks and the corporate network. It is implemented as a multiservice MPLS network.

The *Distribution Communications Network* extends to distribution assets such as field reclosers, automated switches, fault passage indicators, chamber substations and other monitoring devices. The *Distribution Communications Network* endpoints use the Digital Radio Network or 3G/4G communications for new sites.

2.4.1 Needs

The most significant element of risk is the reliability consequence associated with communication system failure for one or more sites, resulting in loss of monitoring and control functionality. This risk can result in a number of different outcomes, including catastrophic failure or damage to associated primary assets, cascading outages affecting other parts of the network, extended outages to customers, and offloading generation.

The overarching need of communication asset management is to ensure asset maintenance and asset replacement maintains risk exposure at an acceptable and manageable level, whilst at the same time meeting the requirement for greater communications penetration into the distribution network. The decisions on the upgrade and extension of the communications network are based on balancing the investments against the maintenance costs and the level of risk accepted by the organisation in providing a stable and sustainable electricity supply to its clients.

2.4.1.1 Replacement of UHF Radios

A number of ageing UHF radios will need to be replaced during the 2019-2024 regulatory period. The age of the oldest radios will exceed 20 years with an average age 12 years. In addition these radios are unencrypted and have other cyber security vulnerabilities that necessitate replacement.

The base stations and a number of remote radios will be replaced prior to the commencement of the 2019-2024 regulatory period, with the remaining remote radios due for replacement between 2019 and 2023 as they reach end of life.

The remote radios are proposed be replaced with current model Trio Q series units. These units have adaptive modulation with increased data transmission speeds up to 56kbps (up from the existing 9600bps). Additionally these have improved collision handling, data encryption, Quality of Service, compression, alarm functions, and support for IP based communications. Encryption will be implemented as required to meet cyber security requirements. Increased data transmission speeds and improved collision handling will improve throughput and time between SCADA reports to ADMS offering improvements to operations. These options come at no additional cost with the replacement equipment.

2.4.1.2 Distribution Network Monitoring

As identified in the *Secondary Systems Strategy*, responding to the impacts from disruptive technologies (such as PV, other DER and EVs) will require power quality and SCADA monitoring to be extended to lower parts of the network. The additional network data collected will be provided to ADMS for real-time tactical demand response and stored on a central repository and analysed to enhance network planning and asset management. This will permit improved asset utilisation, more informed decision making on network augmentation and optimised asset maintenance. The *Secondary Systems Strategy* proposes a Distribution Network Monitoring Program and other initiatives that will increase the communications asset base in the *Distribution Communications Network*.

The further expansion of the communications network to the distribution level of the electricity network will become a priority. This will enable monitoring and control of the network at the level where the PV, battery and EV network connections are occurring. The technology used to extend the communications network will vary depending on location, technology coverage and geographical features. RF mesh, 3G/4G networks, or UHF radio may be utilised. Coverage, distance, geography, cost and availability will all be considered for each new site, suburb or region.

2.4.1.3 Additional Zone Substations

There are three zone substations planned to be built by Evoenergy in the 2019-2024 Regulatory Period and beyond. Additionally TransGrid is establishing the new Stockdill substation. In order to provide necessary protection and SCADA for these new substations and transmission lines, extensions to the communications network will be required. The planned expansion to the optical fibre network is contained in the *Secondary Systems Strategy*.

2.4.1.4 Cyber Security

Communications provides a critical role in the cyber security defence in depth approach detailed in the *Secondary Systems Strategy*. Network segmentation, establishing perimeter security and appropriate data encryption over public and radio networks is key to the cyber security strategy. The aim is to reduce the threat exposure of the Evoenergy electrical network to communications disruption or malicious operation of SCADA and protection devices.

The risk of adverse impacts on communications systems from cyber security incursions, either in the form of targeted attacks or unintentional collateral damage, has been increasing in recent years. SCADA communication systems in particular can no longer rely on physical separation in order to maintain security, and there is a need for mature and considered cyber security measures to be in place to protect critical infrastructure.

At the device level, switches, routers, terminal servers, radios, base stations, modems and tele-protection devices must be kept up to date to ensure there are no known security vulnerabilities exposed. This is driven by vendor releases and recommendations for software patches and updates, firmware updates, and driver updates as required. It is critical that communications network devices are supported and operating systems are patched. This is particularly important for devices such as MPLS routers and Ethernet switches in the core of the network. Exploits of vulnerabilities in these devices can lead to compromise of the SCADA and ADMS control systems or protection systems

These core devices (MPLS routers and Ethernet switches) must remain in vendor support. The expected end of support for these devices needs to be factored into replacement programs.

Devices in the *Distribution Communications Network* (UHF radios and 3G/4G radios) provide SCADA communications to devices such as field reclosers and automated switches. These devices operate over public networks and encryption is required to be implemented and maintained.

> NOTE *The reader is encouraged to refer to the Cyber Security Strategy section of the Secondary Systems Strategy document for further details.*

2.4.2 Opportunities

With the advent of newer technologies being deployed in the network, such as numerical protection relays and other IEDs, there is a growing amount of operational data that can be collected.

2.4.2.1 Condition Monitoring

Utilising the reach and capacity of the communications network, Evoenergy can leverage additional monitoring capabilities of modern IEDs, such as condition monitoring of primary and secondary assets. This information can be gathered on a real-time basis for analysis and notification of alarm conditions. The data collected will be used to perform condition analysis to aid in the planning of maintenance, augmentation and the eventual replacement of assets.

2.4.2.2 Remote Access of IEDs and RTUs

One of the capabilities of modern RTUs and IEDs is with remote connection and remote management. This capability can be leveraged by Evoenergy with the ability to log into RTUs and IEDs remotely. This will have the following potential use cases:

- The ability to remotely interrogate devices and ensure operation at the designed and configured values.
- The ability to download event and disturbance reports remotely. More timely investigation of into the cause of faults, and the avoidance of travelling to site.
- The ability to access and leverage condition monitoring information collected by the devices remotely and store/analyse information into central asset management systems.

The ability to monitor and configure the RTUs and IEDs remotely will improve the management of the devices significantly. Updates and changes to settings will be able to be performed without the need for site visits to carry out the work. This will mean quicker turn-around on operational investigations at a reduced cost (avoidance of travel time to site). This will result in faster turn-around and less exposure to the zone substation sites.

Configuration tasks are subject to thorough testing as part of software development best practices, and must be approved in accordance with Evoenergy IT/OT standards before being rolled out to sites. Cyber Security is a major consideration with the implementation of remote access. Please see the *Secondary Systems Strategy* for more information.

2.5 Associated Asset Classes

The communication assets provide services for secondary systems assets including protection relays (IEDs) and SCADA RTUs.

Asset class associations:

- Hardware:
    - Transformers
    - CB Isolators
    - Reclosers
    - Gas Switches
    - RTUs
    - Protection Relays
    - System Monitoring Devices
    - Battery Chargers

- OT/IT Systems:
    - ADMS
    - SCADA
    - RIVA
    - ArcFM
    - Cityworks.

3 Asset Base

This section provides details of Evoenergy’s current asset base for assets that are a part of this asset class, including the current age and condition profiles of the assets and the projected asset count.

3.1 Asset Base Summary

The communication asset data has been built from ArcFM and other sources, with all assets included within RIVA DS.

Table 3 gives details of Evoenergy’s in-service communication assets as at 2017.

Asset Type	Quantity	Design Life (yrs)	Average Age (yrs)	Oldest Age (yrs)
3G-4G Modems	44	7	0	0
ADSS Optical Fibre	2	40	0	0
Base Station Ethernet Switches	4	15	0	0
Distribution Ethernet Switches	40	15	3	10
DMR Base Stations	4	15	1	1
DMR Gateways	3	15	1	1
DWDM Optical Multiplexers	6	7	1	2
Media Converters	28	15	1	4
Microwave Radios	14	10	6	8
Mobile Radios	169	10	4	9
OPGW	12	40	1	2
Pilot Cables	19	30	27	32
Power Supplies	28	15	1	3
Tele-Protection Devices	37	10	12	30
TMR Base Stations	16	10	9	9
TMR Gateways	2	10	9	9
UHF Base Stations	7	10	13	17
UHF Remotes	116	10	8	18
Underground Optical Fibre	29	40	1	2
WAN Devices	22	7	2	6
Zone Sub Ethernet Switches	79	15	2	6

Table 3: In-service Assets

NOTE

Individual optical fibre segment lengths are recorded in Riva/ArcFM.

3.2 Asset Service Life Expectancy

The design life of communications assets varies dependent on the asset type. Refer to Table 3 for asset design life details. The useful life may be less than or greater than the design life, which can depend on quality of manufacturing, installation, maintenance and operational conditions.

3.3 Asset Age Profile

Figure 1 shows the age profile of the communication assets.

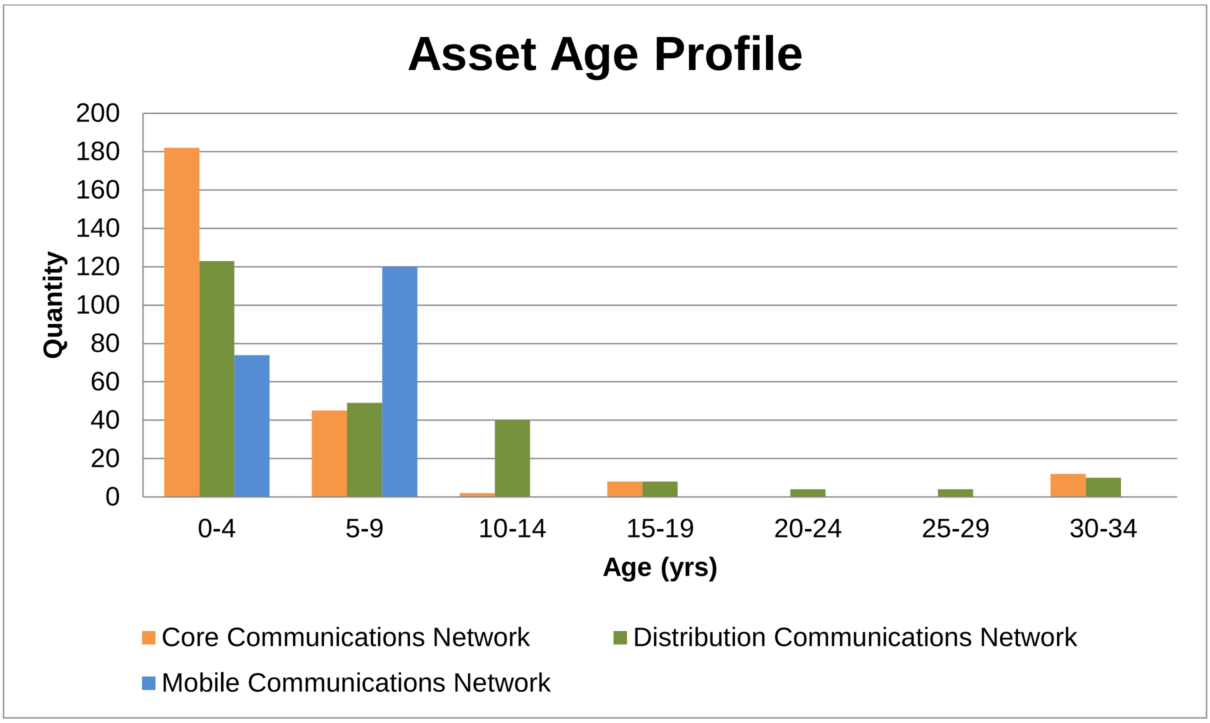

Figure 1: Age Profile of Communication Assets

In order to ensure the presentation of meaningful asset age and health data, the various communications assets have been grouped together as follows:

- *Core Communications Network:*
  - *ADSS Optical Fibre*
  - *OPGW*
  - *Underground Optical Fibre*
  - *DWDM Optical Multiplexers*
  - *WAN Devices*
  - *Base Station Ethernet Switches*
  - *Zone Sub Ethernet Switches*
  - *Microwave Radios*
  - *Power Supplies*
  - *Tele-Protection Devices*
- *Distribution Communications Network:*
  - *3G/4G Modems*
  - *Distribution Ethernet Switches*
  - *Media Converters*
  - *Pilot Cables*
  - *UHF Base Stations*
  - *UHF Remotes*
- *Mobile Communications Network:*
  - *DMR Base Stations*
  - *DMR Gateways*
  - *Mobile Radios*
  - *TMR Base Stations*
  - *TMR Gateways.*

3.4 Asset Condition Profile

The current asset health profile is determined by combining the asset condition rating with its criticality rating. Condition is determined by the asset's age and expected life. Obsolescence is determined by maintenance requirements and availability of support from manufacturers. Criticality is determined from operational, safety and environmental consequences due to asset failure.

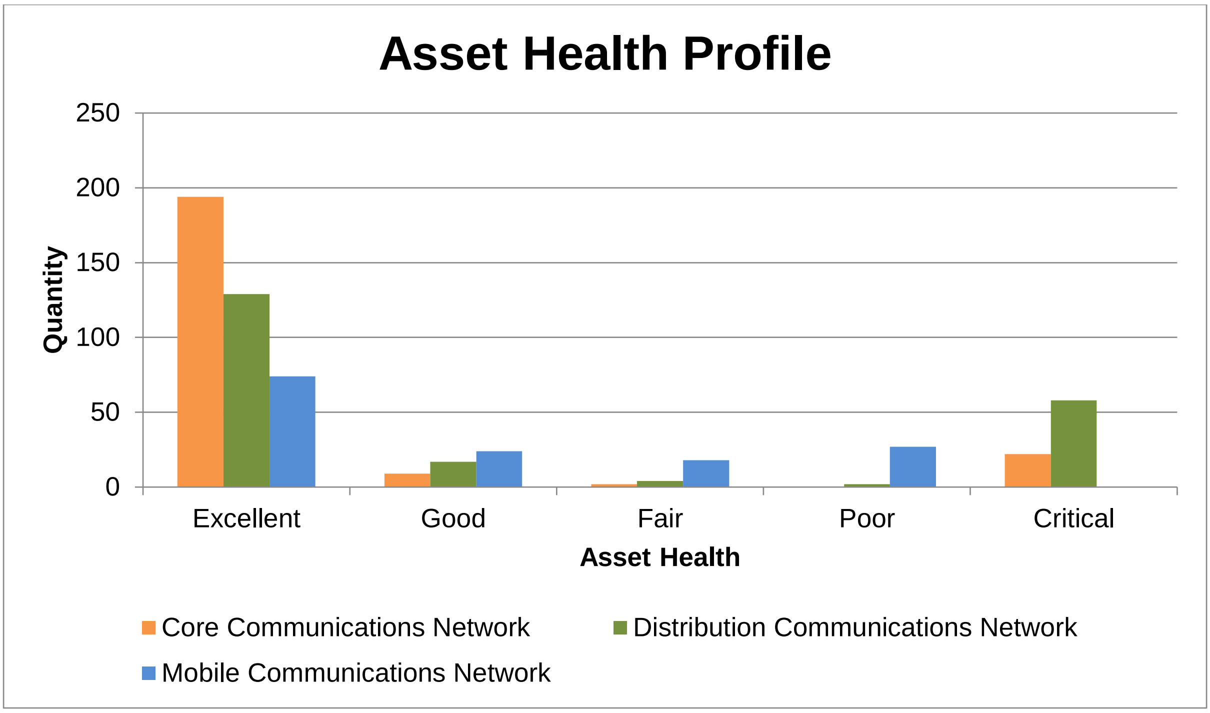

Figure 2: Asset Health Profile of Communication Assets

NOTE *Health Score: Excellent (100-90), Good (90-70), Fair (70-50), Poor (50-30), Critical (30-0)*

Table 4 gives details of the current condition of communication assets.

Asset Type	Manufacturer	Model	Quantity	Average Health
3G-4G Modems			**44**	**Excellent**
	CISCO		**14**	**Excellent**
		IR809	14	Excellent
	MAXON		**30**	**Excellent**
		UNIMAX MA-2025-4G	30	Excellent
ADSS Optical Fibre			**2**	**Excellent**
	(blank)		**2**	**Excellent**
		72c ADSS	2	Excellent
Base Station Ethernet Switches			**4**	**Excellent**
	RUGGEDCOM		**4**	**Excellent**
		RX1500	4	Excellent
Distribution Ethernet Switches			**40**	**Excellent**
	RUGGEDCOM		**40**	**Excellent**
		RS910NC	1	Excellent
		RS8000	23	Excellent
		RS2100	1	Excellent
		RX1500	5	Excellent
		RX802i	10	Excellent
DMR Base Stations			**4**	**Excellent**
	TAIT		**4**	**Excellent**
		TB9315	4	Excellent
DMR Gateways			**3**	**Excellent**
	TAIT		**3**	**Excellent**
		TN9300	2	Excellent
		TN8271	1	Excellent

Asset Type	Manufacturer	Model	Quantity	Average Health
DWDM Optical Multiplexers			**6**	**Excellent**
	smartoptics		**6**	**Excellent**
		M-OADM4-921924	1	Excellent
		M-OADM4-925928	2	Excellent
		M-OADM4-933936	1	Excellent
		M-3817-921936	2	Excellent
Media Converters			**28**	**Excellent**
	MOXA		**28**	**Excellent**
		ICF-1150-M-SC-T	26	Excellent
		TCF-142-M	2	Excellent
Microwave Radios			**14**	**Good**
	CERAGON		**14**	**Good**
		IP-10 1500P 11Ghz	1	Good
		IP-10 RFU-CX 15Ghz	1	Good
		IPMAX 1500P 13Ghz	2	Excellent
		IP-10 RFC-CX 18Ghz	1	Good
		IP-10 RFU-CX 18Ghz	2	Excellent
		IP-10 RFU-CX 13Ghz	4	Excellent
		IP-10G RFU-CX 18Ghz	1	Good
		IPMAX 1500P 18Ghz	1	Good
		IP-10 1500P 13Ghz	1	Good
Mobile Radios			**169**	**Good**
	TAIT		**169**	**Good**
		(blank)	119	Good
		TM9355	25	Excellent
		TP9360	25	Excellent
OPGW			**12**	**Excellent**
	(blank)		**12**	**Excellent**
		72c OPGW	6	Excellent
		24c OPGW	3	Excellent
		48c OPGW	3	Excellent
Pilot Cables			**19**	**Poor**
	(blank)		**19**	**Poor**
		(blank)	19	Poor
Power Supplies			**28**	**Excellent**
	ELTEK		**28**	**Excellent**
		FLATPACK S 48/1000 HE	28	Excellent
Tele-Protection Devices			**37**	**Fair**
	ACTEWAGL		**3**	**Critical**
		Intertrip Communicator MK1	3	Critical
	DEWAR		**18**	**Poor**
		695	12	Critical
		DM1200	6	Excellent
	SEL		**14**	**Excellent**
		2506	5	Excellent
		RTAC	2	Excellent
		2505	7	Excellent
	TC COMMUNICATIONS		**2**	**Excellent**
		JumboSwitch TC3846-2	2	Excellent
TMR Base Stations			**16**	**Fair**
	TAIT		**16**	**Fair**
		TB8100	16	Fair
TMR Gateways			**2**	**Fair**
	SUN		**2**	**Fair**
		Sun Nextra 240 T1541 Node	2	Fair
UHF Base Stations			**7**	**Critical**
	TRIO		**7**	**Critical**

Asset Type	Manufacturer	Model	Quantity	Average Health
		DB10	4	Critical
		EB1	3	Critical
UHF Remotes			**116**	**Fair**
	TRIO		**116**	**Fair**
		ER3	41	Excellent
		DR	13	Poor
		ER1	28	Critical
		ER2	24	Poor
		DRx	6	Critical
		QR	3	Excellent
		ER	1	Excellent
Underground Optical Fibre			**29**	**Excellent**
	(blank)		**29**	**Excellent**
		48c UG SMOF	22	Excellent
		72c UG SMOF	3	Excellent
		144c UG SMOF	3	Excellent
		UG SMOF	1	Excellent
WAN Devices			**22**	**Excellent**
	CISCO		**22**	**Excellent**
		ASR903	14	Excellent
		CGR2010	8	Good
Zone Sub Ethernet Switches			**79**	**Excellent**
	CISCO		**15**	**Excellent**
		C2960	2	Excellent
		IE5000	13	Excellent
	RUGGEDCOM		**64**	**Excellent**
		RS910NC	11	Excellent
		RS2100	41	Excellent
		RX1500	12	Excellent

Table 4: Current Communication Asset Condition

From the information in Table 4, the following assets are approaching or have exceeded end of life conditions, which should be managed by the preferred asset class strategy:

- Pilot cables
- ActewAGL Intertrip Communicator MK1 Tele-Protection devices and Dewar 695 Tele-Protection devices – these will be replaced as part of the Protection Replacement projects
- Trio D-series and E-series UHF remote radios and base stations
- TMR base stations and remotes (being replaced with DMR)
- Microwave Radios; although not all have reached their design life, all are past the manufacturer's end of life.

During the regulatory period 2019-2024, it is forecast that the next generation 5G network mobile network will be operational. Upgrading existing 4G devices to 5G before the 4G network is decommissioned has been forecast towards the end of the period.

Some Zone Substation routers and switches will reach their design life within the regulatory period, and increased bandwidth requirements are expected. Replacements for these will be required during the 2021-2024.

3.5 Projected Asset Count

The projected asset count is an estimate of the number of communication assets by year. The estimate includes asset additions and retirements through estimated network augmentation and asset retirements over the period. Refer to Figure 3 for details.

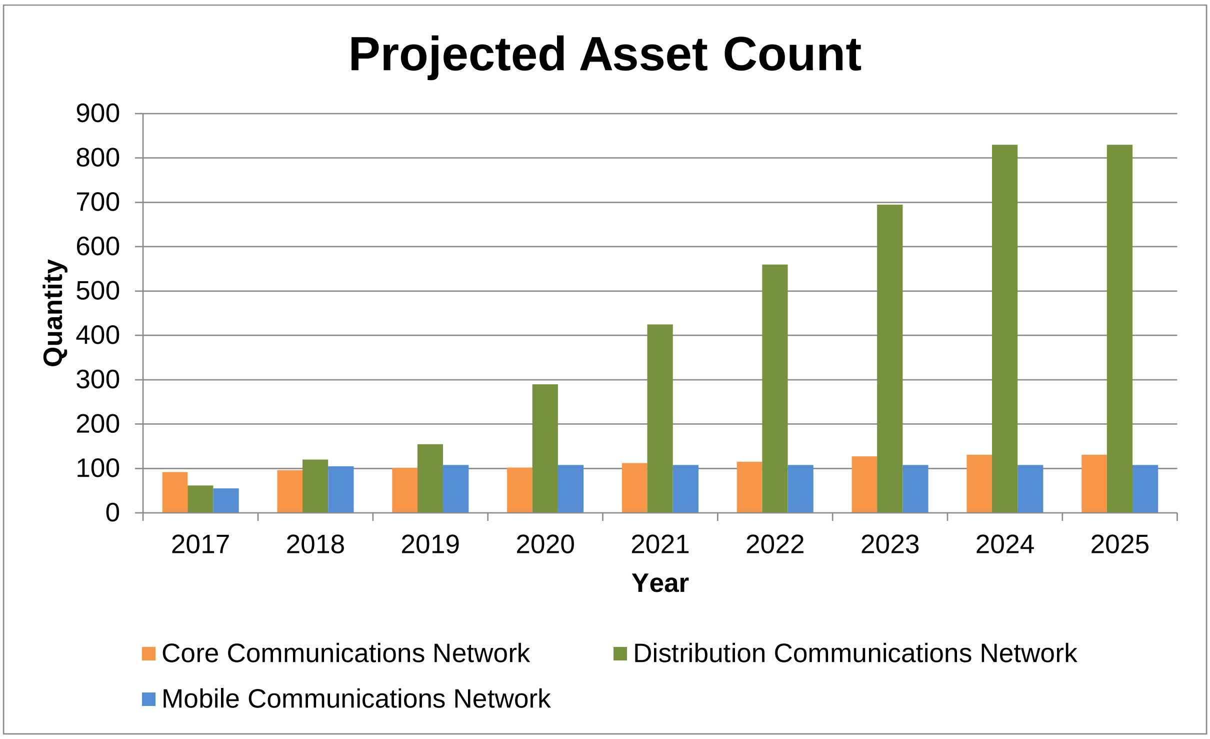

Figure 3: Projected Asset Count of Communication Assets

3.5.1 Network Augmentation and Infrastructure Development

The following network augmentation projects affect the asset class population.

3.5.1.1 Stockdill Zone Substation

The new TransGrid substation at Stockdill will have Evoenergy MPLS infrastructure installed in the substation, and OPGW links will be provisioned along the transmission feeders.

The optical fibre links will be between Stockdill-Woden and Stockdill-Canberra substations.

3.5.1.2 Distribution Substation Monitoring

With the increasing penetration of distributed generation such as PVs, and the introduction of fixed batteries and electric vehicle batteries to the supply grid, there will be an increasing need to extend network monitoring to lower levels of the distribution network. This will result in IEDs and monitoring devices being installed in an increasing number of distribution substations. The presence of PVs has already been shown to have direct impacts such as excessive voltage rise, thermal overload of low voltage feeders, harmonic saturation, and load balancing issues on distribution feeders. The monitoring and control of such PV initiated excursions will have to occur at lower levels within the electrical network than has previously been the practice within Evoenergy's network. The monitoring will have to take place at least at distribution substation level to be able to localise where the disturbance is originating. Rapid detection, isolation and control of these incidents will be necessary to prevent localised damage to customer appliances or premises, to protect Evoenergy network assets from damage, and to ensure public and staff safety.

Evoenergy has 480 chamber substations within its distribution network. They are generally located on sites of high local consumption such as data centres, hospitals, large departmental complexes and apartment complexes. It is Evoenergy policy that all chamber substations are to be connected to the SCADA network, at least initially with monitoring capability. All new and upgraded chamber substations are to be provisioned as SCADA capable.

The chamber substation protective device upgrade program has been started, with all new chamber substations being outfitted with IEDs since 2014. There is a program in place to upgrade the LV boards at a rate of 5 per year for the next 10 years. In addition, chamber substation HV boards will be upgraded at the rate of 2 per year for the same period. As existing monitoring devices fail in service they will be replaced with IEDs. In parallel with this project, SCADA connectivity will be extended to each of the chamber substations as they are upgraded.

Currently there are 43 SCADA connected protection devices in chamber substations.

Padmount substations are utilised for the distribution network where the power requirement of a building is greater than 500kVA. The standard padmount transformer ratings within Evoenergy are 315, 500, 750 and 1500kVA. Padmounts contain only one transformer.

The use of numerical control relays connected to the SCADA network in padmount installations is only required for transformers rated at greater than 1000kVA. Padmounts with transformers of lower capacity installed, such as 500 and 750kVA units, are currently protected by fuses and electro-mechanical devices. As the electro-mechanical and first generation electronic protection devices are replaced due to age, device fault profile or end of manufacturer support, they will be replaced with multi-function numerical protection devices (IEDs). Except for specifically identified instances, these lower capacity transformers will not be connected to the SCADA network.

Distribution substation monitoring will be extended to 20% of the substations over the 2019-2024 Regulatory Period. It is planned that 100 distribution substations per year (mostly padmounts) will be connected to SCADA, with IEDs or monitoring devices installed at each one. This will allow for advanced monitoring of the distribution network to be performed.

4 Asset Performance Requirements

This section details the reliability and performance requirements of the communication asset class.

4.1 Failure Modes

This section outlines the Failure Mode and Effects Analysis (FMEA) and deterioration drivers for each asset type. Failure modes and Risk Priority Number (RPN) have been nominated by subject matter experts. This analysis is used to evaluate strategy options for this asset class.

For full details of individual asset failure modes, refer to Appendix C.

4.1.1 Deterioration Drivers

The optical fibre infrastructure has differing deterioration drivers, depending on whether it is installed overhead, as with OPGW and ADSS, or underground. Typically, overhead optical fibre infrastructure will suffer from deterioration of performance and eventual fibre failure if mechanical pressures or vibrations exceeding manufacturer’s specifications are applied to the fibres. High winds or excessive sagging can introduce tiny cracks and imperfections in the optical fibres, especially at sites where bend radii or unsupported lengths approach recommended values. By its nature, OPGW is protected physically to a greater degree than ADSS. Underground optical fibre is protected from the effects of wind and vibration, but is still subject to recommended minimum bend radius values.

Owing to the careful design and installation procedures as well as the young age of the optical fibre infrastructure and the design life of 40 years, little to no deterioration is expected at this stage. Regular testing of signal attenuation on fibres will continue to measure any deterioration over time.

For the majority of electronic devices such as Ethernet switches, media converters, modems and radios, standard deterioration is to be expected, in line with manufacturers’ data and practical field experience. Moving parts such as cooling fans are subject to wear and tear. Any dust and dirt build-up that compromises device heat extraction would increase rates of deterioration and failure.

Pilot cables have been used as a communication medium in some cases for 40 years, for example in providing longitudinal feeder (line) differential protection unit schemes. Regular testing of in-service pilot cables has indicated a decline in their electrical characteristics, providing a risk of protection mal-operation of protection schemes.

Replacement of existing pilot cable based Translay feeder protection with optical fibre based differential protection is proposed in the Protection ASPs and the pilot cable replacement with optical fibre is part of this Communications ASP.

4.2 Asset Utilisation

This section details the utilisation level of the assets. Depending on the asset type, the level of utilisation will have a direct impact on asset condition and performance deterioration rates.

4.2.1 Availability

Zone substation communication issues are required to be identified immediately, and reported and investigated within 4 hours. Due to the critical nature of zone substation assets, redundant communications paths are required to be maintained to meet availability requirements.

Distribution substation communication issues are required to be identified immediately, and reported and investigated within 24 hours. Due to the less critical nature of distribution substation assets, a single communications medium is sufficient and a small outage to the communications links can be tolerated.

The optical fibre communications network provides a high speed redundant communications network that exceeds the 99% availability required under the NER. This, combined with the existing microwave and UHF links, ensures that Evoenergy meets the performance requirements for communications issues and monitoring and control of the electricity network.

4.2.2 Capacity and Capability

The maximum capacity of the existing UHF radio network is 9600bps. With the expected evolution of network monitoring and control capabilities through the introduction of numerical relays, and the intended utilisation of the zone substation communication systems for other corporate functions, the UHF radio network is unable to provide the required communications capacity for communications to zones. The required capacity for identified operational needs is 28Mbps under normal, 76Mbps under P90 calculated using Monte-Carlo statistical analysis, and 90Mbps under worst case scenario.

The optical fibre network exceeds the capacity requirements stated above. The connection speeds between zone substations and the control centres is set at 1GBps, and communications between the control centres and the data centres is at higher speeds, up to 10GBps. In addition, the communications network configuration has QoS configured so that tele-protection and the SCADA communications have guaranteed capacity and performance on the network, and other functions may have performance curtailed in high demand situations. QoS is needed to ensure guaranteed bandwidth is available for expected levels of SCADA data in the communications network.

Evoenergy will monitor the bandwidth demands for network traffic between the zone substations and the control centres. If the demand is high, the capacity of the optical fibre links between the zone substations, the control centres and the data centres will be upgraded to 10GBps. This will be driven by the requirements to enable FLISR, video monitoring and possible thermal image monitoring. Enabling the additional network capabilities such as the engineering network and the extension of the corporate network to zone substations will also contribute to the bandwidth requirements, with the most likely outcome being upgraded link capacity to 10GBps during the 2019-2024 upgrades to the zone MPLS router and switch equipment.

These business requirements and the proposed augmentation program are contained in the Evoenergy *Secondary Systems Strategy* document.

4.2.3 Utilisation

In terms of providing information transfer and visibility of assets back to the SCADA master station, communication assets are utilised 100% of the time. With the increased amount of information provided by numerical relays, the monitoring of assets and the increased ability to directly control assets, the network utilisation will remain extremely high from a SCADA perspective. Adding in the additional corporate networks and functions will also increase the load on the communications network. The capacity of the optical fibre network will be sufficient to handle all that is currently known of the potential load on it. Additionally, QoS rules will ensure that SCADA traffic will have priority on the communications network. Hence, the communications network will be utilised 100% of the time, but not at 100% capacity.

4.3 Risk and Criticality

This section details the criticality of the communication assets and their exposure to risk.

4.3.1 Asset Criticality

The communication assets are considered critical for the reliable and safe operation of the electrical network. The failure of communication equipment affects the system in the following ways:

- Remote monitoring and control, operations and distribution functions are not possible
- The loss of continuous, real-time monitoring and control would make the network unsafe
- Protection inter-trip functions would not operate and this would put assets, environments and the public at risk if the fault is not isolated
- Increased risk to the safety of the public and Evoenergy staff. The risk of damage to electrical network assets would also increase significantly.
- Impact on the outage duration on the primary network would affect the SAIFI/SAIDI indices
- In the event of a black start Evoenergy will not be able to automatically re-energise the electricity network, and will not be able to meet the regulated requirements under the NER
- The loss of real-time monitoring of TNSP meters providing metering functions and inter control centre data reporting to AEMO and TransGrid.
- Loss of real-time monitoring of voltage measurements, other power quality information and device operation to the ADMS, and therefore loss of history for network parameters during the outage.

4.3.2 Geographical Criticality

Geographical criticality refers to environmental interference. For example, UHF radio transmission is sensitive to routing, and is affected by obstacles such as hills and buildings that can significantly weaken its signal strength. Microwave links need to be 'line of sight' and can be impacted by adverse weather conditions. The growth of vegetation (typically trees) in the path between transmitter and receiver can interfere with the reception of radio signals by attenuating the signal to levels that cause performance issues with the radio link.

The new optical fibre network is not impacted by geographic features, the built environment or weather conditions, making it a more reliable network in all conditions. The major potential impact on the optical fibre network is where sections of it follow underground sub-transmission paths, resulting in vulnerability to damage from digging or trenching operations.

In 2017, a tree planting exercise outside Canberra Hospital damaged the installed optical fibre cable, causing loss of SCADA connection to a zone substation. As there was not yet a redundant connection to the site, this required reinstatement of the UHF link while the replacement of the cable in the damaged section was carried out. The *Secondary Systems Strategy* outlines requirements and plans for the for redundant communications paths into critical sites such as zone substations.

4.3.3 Asset Reliability

The redundant optical fibre communications network aims to remove single points of failure that exist in the communications network, enhancing the inherent reliability of the communications network. In particular this is required in order to meet NER protection communications requirements, AEMO ICCP communications requirements and Evoenergy ADMS SCADA operational requirements. Diversity of communications also maintains performance independent of weather conditions and is not susceptible to other forms of interference which impact on the radio networks. With the optical fibre network in combination with the existing microwave and UHF links, the reliability of the communications network exceeds the reliability standards set under the NER in all conditions due to the high level of redundancy built into the communications network.

Because of the criticality of Evoenergy protection and SCADA functions, a loss of capability can have significant adverse impacts. The operations and maintenance of the Energy Networks communications network is the responsibility of the BSD communications group. BSD is also responsible for the corporate IT communications network. The two networks service different sets of users, each with differing requirements as to geographical spread, accessibility, performance, security and reliability, requiring different design philosophies, service levels and skill-sets. The implementation of the IP-MPLS communications network simplifies the requirements on BSD as the network topologies move closer together. The communications network is an IP-MPLS network based on the same infrastructure as the corporate network, which will result in higher network reliability and better support from BSD as the infrastructure is common across both networks.

Effective coordination with BSD in planning system works and outages will further improve the reliability of the communications systems.

4.3.4 Risk Assessment

A partial or complete loss of communications can severely impact Evoenergy's ability to provide a safe operating environment for staff and the public and could risk damage to assets. This has been factored into the implementation of the core communications network, and the optical fibre network has diverse paths between most zone substations in the Evoenergy electricity network.

Sufficient communications network redundancy is an NER requirement for 132kV protection systems and is important for the availability of SCADA monitoring and control in ADMS. This ensures appropriate network resilience, and loss of a core communications link will not impact on the ability to monitor and control the electrical network. This ensures the availability of communications in credible scenarios that can affect the network.

The risk assessment of communications asset failure is difficult to quantify in terms of financial impact. For risks to materialise, a fault must manifest in the primary system, associated SCADA system, protection system and the communication system. The consequence of failure can be extreme with 132kV protection mal-operation, and could dramatically effect operations if a failure affects visibility of the network in the SCADA ADMS system. For these reasons a qualitative risk assessment approach has been used in the following section of the ASP.

The major identified risk in today’s environment is a successful cyberattack. Evoenergy has implemented the MPLS network in accordance with industry best practices to ensure security of the Secondary Systems communications network, including network segmentation. Additionally, the proposed upgrade of the UHF radio network will incorporate current generation equipment that allows encryption and protects against threat vectors related to the existing equipment which is beyond the manufacturer’s end of life.

5 Asset Management Strategy Options

This section discusses asset class strategies to manage communication assets throughout their lifecycle and recommends the preferred option. The preferred asset class strategy supports the business asset management policy, strategy and objectives.

5.1 Option Overview

Asset class strategies are evaluated against their cost, risk, benefits and consideration of trade-offs between capital and operational expenditure to achieve the asset management objectives. The options that have been considered include:

- Option 0 – Do Nothing Strategy
- Option 1 – Periodic Maintenance with Age-Based Replacement
- Option 2 – Optimised Maintenance with Strategic Replacement.

5.1.1 Option 0 – Do Nothing Strategy

This option assesses the inherent risk rating for the communication asset class if no controls or mitigating strategies are in place.

5.1.1.1 Description

This option is the do nothing strategy whereby assets are 'run-to-failure' without planned maintenance or planned replacement. Upon failure, assets are assessed and reactively repaired or replaced as necessary. Typical asset management tasks for this strategy include:

- Operation of critical assets until partial or catastrophic failure
- Corrective maintenance to repair faults
- Reactive replacement to restore unrepairable assets.

5.1.1.2 Risk

As asset condition deteriorates and assets approach the end of their expected life, their reliability will decrease and the risk exposure of this option will rapidly increase.

A qualitative risk assessment of this option highlights the inherent risks (no controls) of this asset class and the risk exposure. This is shown in Table 5.

		Inherent Risk				
Likelihood	Almost Certain					
	Likely	Low 3	Medium 2	High 5	High 1	
	Possible	Low 2	Medium 9	Medium 13	High 3	
	Unlikely	Low 4	Low 7	Medium 8	Medium 2	
	Rare			Low 1		
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 5: Qualitative Risk Assessment – Option 0

5.1.1.3 Option Assessment

The run to fail strategy does not provide any benefits from a reliability perspective. There would be an unavoidable increase in unplanned outages leading to long intervals of power disconnection, safety issues, and inconvenience to customers. Evoenergy would be impacted negatively through:

- Reputational loss
- Loss of reliability and revenue
- Non-compliance with NER, ACT Regulations and reporting requirements to AEMO
- Worsening SAIFI/SAIDI numbers and loss of STPIS revenue incentives.

This option is rejected given the risk it poses in terms of reliability and safety, the two core objectives of Energy Network's strategic vision.

5.1.2 Option 1 – Periodic Maintenance with Age-Based Replacement

This option entails periodic annual maintenance and a like for like replacement of communication assets at their end of life.

5.1.2.1 Description

For Evoenergy communications assets, a program of annual inspections would be instigated. This process will ensure high availability of the communications assets throughout the communications network. Assets are upgraded based on their age.

5.1.2.2 Risk

Retaining the current expenditure level for replacing communications assets will expose Evoenergy to an increasing level of risk due to a large number of assets showing poor future health. Current expenditure levels will not meet the need to replace assets, and a number of assets will reach a critical health level at the end of the regulatory period in 2024.

Risk summary:

- Substantial deterioration of condition of assets failing regularly and replaced like for like.

The exposed asset class risk ratings for this option at the end of the regulatory period (2024) are shown in Table 6.

		Option 1 Risk				
Likelihood	Almost Certain					
	Likely					
	Possible		Medium 4	Medium 9		
	Unlikely	Low 11	Low 17	Medium 18	Medium 1	
	Rare					
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 6: Qualitative Risk Assessment – Option 1

5.1.2.3 Option Assessment

Whilst this option limits the increase of risk compared to the Do Nothing option, it does not address the need for greater communications penetration into the distribution network in response to photovoltaics and other disruptive technologies.

This option is rejected given the risk it poses. To alleviate the level of risk exposure, additional CAPEX investment would be needed to augment distribution communication assets in order to monitor and manage power quality on the LV side of the distribution network.

5.1.3 Option 2 – Optimised Maintenance with Strategic Replacement

This option takes into consideration each communications asset type and selects the optimal strategy for maintenance. Where existing assets are not capable of providing functionality, or where technology advances in media or protocols render existing assets obsolete, strategic replacement prior to asset end of life is recommended.

5.1.3.1 Description

For communications assets located in Evoenergy critical sites, a program of annual inspections combined with online condition monitoring would be instigated. This process will ensure high availability of the communications assets at these sites. The assets may be upgraded based on several factors, one of which may be the age of the asset. Other factors which may be considered in deciding on asset replacement are changes in technology, manufacturer support, or repeated faults occurring.

Additionally, alignment of communications asset maintenance with SCADA asset maintenance is proposed at zone substations, in order to reduce the number of planned maintenance outages.

The critical Evoenergy sites with Secondary Systems communications assets installed are listed in section 6.3.3.

The periodic maintenance regime should ensure continued high performance of the communications assets until they are considered to be end of life. As the asset's life cycle approaches its end of design life, a decision will be made on replacement of the asset based partly on its condition and performance at that time in addition to the factors previously described in this section.

For communications assets which are located in sites identified as non-critical, their condition will be monitored utilising tools such as Solarwinds and Trio T-View. Regular reports on the performance of the assets will be produced from the applications, to be considered by Secondary Systems asset managers. Decisions regarding maintenance, upgrade or replacement of assets will be based on the information presented in the reports or if the unit fails in service.

The Evoenergy sites with Secondary Systems communications equipment installed that are to be subject to condition monitoring only are listed in section 6.3.4.

Secondary Systems requirements for the reporting on communications assets are detailed in section 6.3.5.

Replacement of assets located at Evoenergy high value sites may be accelerated due to strategic considerations. Factors which will inform a strategic replacement project may include:

- Changes in regulatory requirements
- Significant changes in technology
- Opportunity to change/upgrade due to related primary asset and secondary asset projects.

This strategy option reduces the OPEX costs compared to the existing asset class strategy by optimising maintenance. It includes the following tasks:

- Condition monitoring of communications assets by utilising embedded applications such as Solarwinds and Trio T-View. No preventative maintenance of these assets.
- Generation of regular reporting on asset performance
- Alignment of communications asset maintenance with SCADA asset maintenance at critical sites.

5.1.3.2 Risk

Setting the expenditure at this level for critical communications infrastructure will ensure that ADMS/SCADA is always available for control of the Evoenergy electricity grid. This is important at all times but is particularly critical during network faults and incidents. The level of expenditure has been identified as the minimum needed to guarantee the required high availability of the communications network. This will enable Evoenergy to meet its obligations to provide a stable, safe electricity network, ensure the safety of its employees and the public and meet its obligations under the NER for control and fault resolution on the electricity network, whilst at the same time managing costs.

The exposed asset class risk ratings for this option at the end of the regulatory period (2024) are shown in Table 7.

		Option 2 Risk				
Likelihood	Almost Certain					
	Likely					
	Possible					
	Unlikely	Low 18	Low 20	Medium 10		
	Rare	Low 10		Low 1		
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 7: Qualitative Risk Assessment – Option 2

5.1.3.3 Option Assessment

The risks presented by this option are significantly lower than the Do Nothing option and are lower than for Option 1. At the same time, the CAPEX investment allows greater penetration into the LV distribution network, which is in alignment with the strategic direction of Evoenergy and meets the requirements of the NER for the Regulatory Period 2019-2024. The introduction of the detailed maintenance regimes will enhance the stability of the network and increase the security of the environment.

5.2 Option Evaluation

In order to assess the optimal communication asset management strategy, a condition and risk-based modelling approach has been conducted for the various scenarios.

5.2.1 Options Assessment

A scoring matrix approach is used to assess the advantages, disadvantages, risks and benefits of each of the asset class management options. Each option is given an overall score, based on the scoring criteria detailed in Table 8.

Criteria	Description and Weighting
Cost	This ranks the relative CAPEX and OPEX costs associated with the options. The weighting reflects the relative importance of this criterion.
Risk – Safety, Environmental, Reliability, Other	The extent to which the option provides mitigation/controls to risks identified. The weighting reflects the relative importance of this criterion.
Strategic Objectives	The extent to which the option meets the requirements of the asset management strategic objectives. The weighting reflects the relative importance of this criterion.
Innovation/Benefits	The extent to which the option provides business benefits including but not limited to information or intelligence to support innovative asset management and network operation. The weighting reflects the relative importance of this criterion.

Table 8: Option Evaluation Scoring Criteria

	Criteria				Option Score
	Cost	Risk	Strategic Objectives	Innovation/ Benefits	
Criteria Weighting	**30%**	**30%**	**30%**	**10%**	**100%**
Option 0 – Do Nothing	*3*	*1*	*1*	*1*	*53%*
Option 1 – Periodic Maintenance with Age-Based Replacement	*2*	*2*	*2*	*2*	*67%*
Option 2 – Optimised Maintenance with Strategic Replacement	*2*	*3*	*3*	*3*	*90%*

Scoring Key			
0	Fatal flaw	1	Unattractive
2	Acceptable	3	Attractive

Table 9: Scoring Matrix

5.3 Recommended Option

A risk condition based approach has been adopted to determine the optimal recommendation for capital replacement projects and maintenance strategy that will provide the best technical and commercial benefit to Evoenergy in alignment with the AER's strategic objective of reduction in condition monitoring expenses.

This approach is expected to improve the SAIFI/SAIDI figures and improve the STPIS benefits. Based on the evaluation of different scenarios for management of communications network risks and meeting of strategic and regulatory requirements in section 5.2, and based on the risk management approach adopted to deliver a viable communication asset management plan, Option 2 – Optimised Maintenance with Strategic Replacement has been chosen as the most viable strategic approach. This would provide the following benefits:

- Regulatory compliance
- Strategic alignment
- Risk mitigation
- Cost optimisation of OPEX and CAPEX
- Management of asset profile risk and improved future health condition
- Condition monitoring of communications assets.

5.3.1 Forecast Asset Condition

Health profile is determined by asset condition and performance history. Condition is determined by asset age and expected life. Obsolescence is determined by maintenance requirements and availability of support from manufacturers.

The future health profile is the asset health profile at the end of the Regulatory Period, 2024. This forecast is based on:

- Initial health profile
- Deterioration due to ageing
- Allowances made for replacement and refurbishments.

A strategic decision is made at the start of the period on the adequacy of the asset class health, and whether the asset class health should be maintained, improved, or allowed to decline during the period. The maintenance program is adjusted to achieve the required asset class health at the end of the period.

Figure 4 shows the future asset health profile of the core, distribution and mobile communications network assets for the recommended asset maintenance strategy.

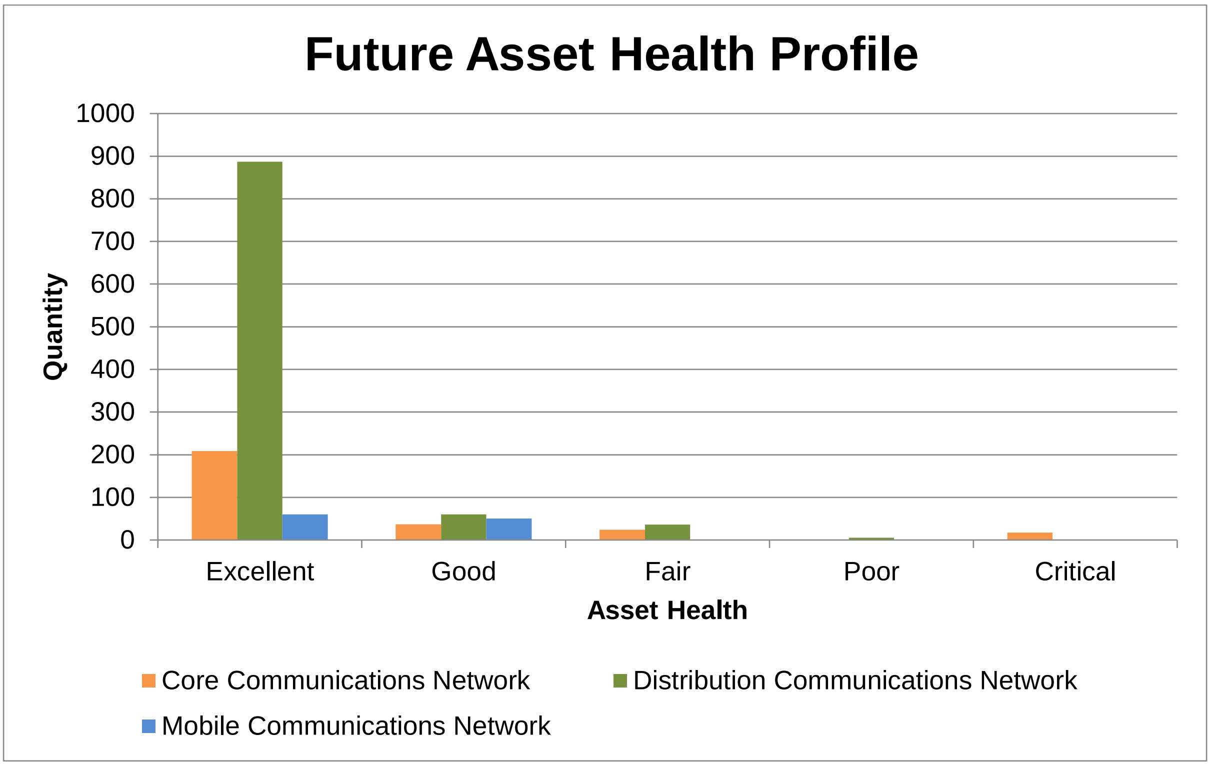

Figure 4: Future Asset Health Profile – Communication Assets

6 Implementation

This section provides implementation details for the recommended asset management strategy option.

6.1 Network Augmentation and Infrastructure Development

The Secondary Systems communications network supports critical infrastructure and must be secured from unwanted intrusions, and as such, needs to meet the highest security standards. In recent years, there has been an increasing trend towards using IP protocols over electricity utilities' communications networks. To accommodate an open standard protocol such as DNP3 or IEC 61850, the communications system must make allowance for the increased bandwidth requirements with the additional overheads of the new protocol.

The Evoenergy *Secondary Systems Strategy* document outlines a program to improve the communications network performance to meet the needs of the SCADA system. This includes:

- Implementation of interconnected SCADA, protection and communications systems that permit real time network management of dynamic energy flows resulting from the expanding use of distributed energy sources
- Implementation of systems that provide enhanced condition monitoring of electricity network assets to optimise asset management and maximise economic benefits
- Implementation of systems that provide fault location and anticipation of faults in the electricity network
- Provision of a unified communications network capable of servicing the following functions:
  - Substation condition monitoring
  - Zone substation physical security systems
  - Zone substation VoIP phones
  - Corporate network presence in zone substations
  - Remote engineering access to protection and other IEDs.

6.2 Asset Creation Plan

Assets are added to the network from asset replacement and network expansion plans. This asset specific plan considers all known network augmentation projects which change the asset class population, detailing the known major projects which will increase the number of communications assets deployed. These projects are the planned zone substation builds and the expansion of SCADA into the distribution substations. Refer to section 3.5.1 for details.

6.3 Communications Asset Maintenance Plan

The objective of this maintenance plan is to economically achieve the longest possible reliable working life of communications assets. This is done through condition monitoring, preventative and corrective maintenance and has been adapted to Evoenergy's assets, operating environment and conditions.

6.3.1 Development

The maintenance plan is designed to achieve the objectives of the asset specific strategy. The following engineering techniques were used to develop the maintenance plan:

- Failure Mode and Effects Analysis (FMEA)

- Condition monitoring
- Historic performance
- Equipment manuals
- Continuous review of asset performance and fine-tuning of maintenance triggers.

Table 10 gives a summary of communications asset maintenance tasks and triggers.

Asset Type	Maintenance Task	Maintenance Trigger
Base Station Ethernet Switches	Condition Assessment	Annual
Distribution Ethernet Switches	Condition Assessment	Annual
Zone Sub Ethernet Switches	Condition Assessment	Annual
Media Converters	Condition Assessment	Condition monitoring
ADSS Optical Fibre	Condition Assessment	Condition monitoring
OPGW	Condition Assessment	Condition monitoring
Underground Optical Fibre	Condition Assessment	Condition monitoring
Pilot Cables	Condition Assessment	Condition monitoring
Power Supplies	Condition Assessment	Annual
3G/4G Modems	Condition Assessment	Condition monitoring
DMR Base Stations	Condition Assessment	Annual
DMR Gateways	Condition Assessment	Annual
Mobile Radios	Condition Assessment	Condition monitoring
Microwave Radios	Condition Assessment	Annual
UHF Base Stations	Condition Assessment	Annual
UHF Remotes	Condition Assessment	Condition monitoring
Tele-Protection Devices	Condition Assessment	Condition monitoring
WAN Devices	Condition Assessment	Annual

Table 10: Communication Asset Maintenance Interval Summary

6.3.2 Communications Asset Monitoring

Communications asset operation and performance is monitored via data points and collected by the SCADA system. There are performance monitoring tools available at BSD (Solarwinds and Trio T-View), and these can be utilised to provide information to Secondary Systems in the form of regular reporting on communication assets by BSD. Details on the Secondary Systems reporting requirements are given in section 6.3.5 of this ASP. The provision of direct access to the monitoring tools will benefit Secondary Systems by allowing the asset managers to directly interrogate performance of assets under their control.

6.3.3 Preventative Maintenance

Annual maintenance of the defined critical sites in the Evoenergy communications network is to be undertaken on behalf of Energy Networks. The critical sites are:

- ADMS and voice radio communications equipment at Greenway data centre, Civic DRF and Fyshwick control centre
- MPLS terminal equipment at zone substations
- UHF equipment in zone substations
- Communications equipment at radio repeater sites.

The annual maintenance activities at these critical sites will include testing batteries and DC systems, inspection of equipment and antenna systems, cleaning of hardware (fans, filters and heatsinks), configuration backups and firmware upgrades. This applies to all Energy Networks equipment installed at critical locations and included in the asset list in section 6.3.1.

Access to the monitoring systems by Energy Networks Secondary Systems staff is important, as it would allow for proactive monitoring of the assets and investigation of the root causes of reported Communications issues. This would also allow Secondary Systems to actively monitor the performance of assets that are showing signs of deterioration in performance, to assist with planning of maintenance and replacement activities, and would permit identification of generic issues across a type of asset requiring attention.

6.3.4 Condition Based Maintenance

All radios and network equipment at sites not listed in section 6.3.3 or in this section 6.3.4 will rely on condition monitoring head-end systems, and will only be visited resulting from alarm indications or deterioration of performance monitoring indicating an issue with the equipment.

The sites using the condition monitoring approach are:

- Chamber substations (UHF radio, 4G and IP)
- Customer generation sites (UHF radio and 4G)
- Reclosers and automated switches (UHF radio and 4G)
- Fault Passage Indicators (4G).

This approach relies on central monitoring systems within the BSD operations centre such as the Solarwinds and Trio T-View systems. The monitoring would utilise the applications and human operators to provide information on the performance of the assets. Based on accurate commissioning records, any change in operation of the assets could be identified early and action taken to prevent in-service failure of the devices. Critical to this approach to maintenance is on-call technicians, available to carry out repair or workarounds before there is an impact on the business.

6.3.5 Asset Reporting Requirements

A monthly report will be required on each asset type, detailing the following:

- Uptime for the month. Total and by asset type.
- Incidents for the month – number of incidents opened, closed and remaining open. Total and by asset type.
- Failures for the month. Total and by asset type.
- Replacements for the month, with reasons, such as performance degradation, failure, age, technology.

The report shall also include the following:

- Number of devices tested per month, by asset type.
- For assets that are showing performance degradation, a graph of the degradation over time.

6.4 Asset Renewal Plan

This asset renewal strategy minimises risk through planned replacement or refurbishment of assets at end of life before catastrophic failure. The condition based replacement strategy uses asset condition to trigger asset replacement or refurbishment and considers the following factors:

- Poor condition from condition assessments and consequently high risk
- Economic obsolescence (economical to replace with alternative product)
- Technological obsolescence (non-availability of spare parts and support, no longer able to meet requirements)
- Strategic replacement – when a significant work program is occurring on an asset, it may be opportune to align a planned communications upgrade or replacement with the planned outage. This would remove the need for two or more outages on a primary asset such as a zone substation. The planned communications work may be brought forward or held back to align with the planned outages.

The decision to replace or refurbish communication assets is assessed on a case by case basis to the whole of life costs, technical feasibility, safety improvements from modern technology and network planning.

6.4.1.1 Refurbishment

For the communications assets, refurbishment is not conducted as an in-house activity. When an asset fails in service it is replaced and the failed unit is returned to the manufacturer to assess if it is repairable. Where the refurbishment of a unit would involve expenditure, the cost is assessed against potential remaining life and the purchase price of a new unit.

6.4.1.2 Replacement

A communications asset will be replaced when a unit shows signs of significant performance degradation, is subject to repeated faults, or fails in service. Replacement will be a planned process where possible, based on the criteria listed above. Sudden failure in service will result in immediate replacement, and an investigation into the failure to determine if a pattern may be emerging. Generally for IT equipment there are supply agreements in place where the asset type is subject to performance standards for supply of replacements in the event of failure. Evoenergy has agreements in place for the supply and support of network equipment with preferred suppliers.

6.5 Asset Disposal Plan

The disposal phase is characterised by any of the communication technology becoming obsolete, or no longer usable. The proposed nominal lifespan of the communication technology systems varies between 7 and 40 years, depending on the asset type. This is determined by the duration the systems continue to achieve reliability requirements or the duration the systems remain supported by the vendor. Given these nominal life spans however, systems can evolve or transition to the next generation because of changing requirements (e.g. regulatory) or improvements to technology. As such, system plans should continually evolve with the systems while much of the environmental, management, and operational information should still be relevant and useful in developing the plan for eventual replacement. The decision to dispose of a system occurs when:

- The current system can no longer meet the businesses requirements at acceptable risk levels;
- A new requirement is best achieved by replacing all or part of the current system; or
- The current components (software and/or hardware) can no longer be maintained, repaired or supported by the vendor.

Disposal activities shall ensure a planned phased termination of the system, preserving any reusable hardware (spares) and required business information so that some or all of the information may be used in the future, if required (e.g. historical network data). Particular emphasis is given to minimal disruption to normal operations and proper preservation of the data within the retired system so that the data is effectively migrated to the new system or archived in accordance with applicable records management regulations and policies for potential future access.

Communications assets that have been leased are either retained under a renewed lease or terminated and replaced by new assets.

Assets that are faulty are repaired where possible and retained as spares inventory, ready to be deployed as and when required.

Communications assets may contain sensitive information pertaining to system configuration, and will need to be disposed of in a secure manner. The procedure for the correct sanitisation of assets potentially containing data, issued by BSD, is the *Media Sanitisation, Destruction and Disposal Standard* document.

This document is referenced in section 15 of the *ActewAGL ICT Security Standard – SM4321* document, and in sections 3.40 and 3.41 of the *ActewAGL ICT Security Framework – SM4326* document.

6.6 Associated Asset Management Plans

The following associated ASPs have an impact on the management of communication assets:

- Secondary Systems Zone Substation Protection ASP
- Secondary Systems Distribution Substation Protection ASP
- Secondary Systems SCADA ASP.

7 Program of Work

This section provides the Program of Work and the resulting operational and capital expenditure forecasts.

7.1 Maintenance Program

This section outlines the operational expenditure for preventative maintenance, corrective maintenance and condition monitoring.

For modern communications equipment, asset life is not extended by maintenance. Evoenergy is implementing increased condition monitoring to provide early detection of faults, especially where the redundant architecture may otherwise hide a failure when it does not result in a loss of visibility within the network.

NOTE

Planned and unplanned maintenance OPEX labour expenditure for Radio systems and WAN equipment is currently captured in overall BSD service charges. From 2019/20 planned maintenance (preventative) tasks and unplanned (corrective) maintenance have been defined in this ASP and these tasks will be costed against annual planned and unplanned maintenance programs.

Hence the evident expenditure uplift from 2019/20 in Figure 5 on *the following page.*

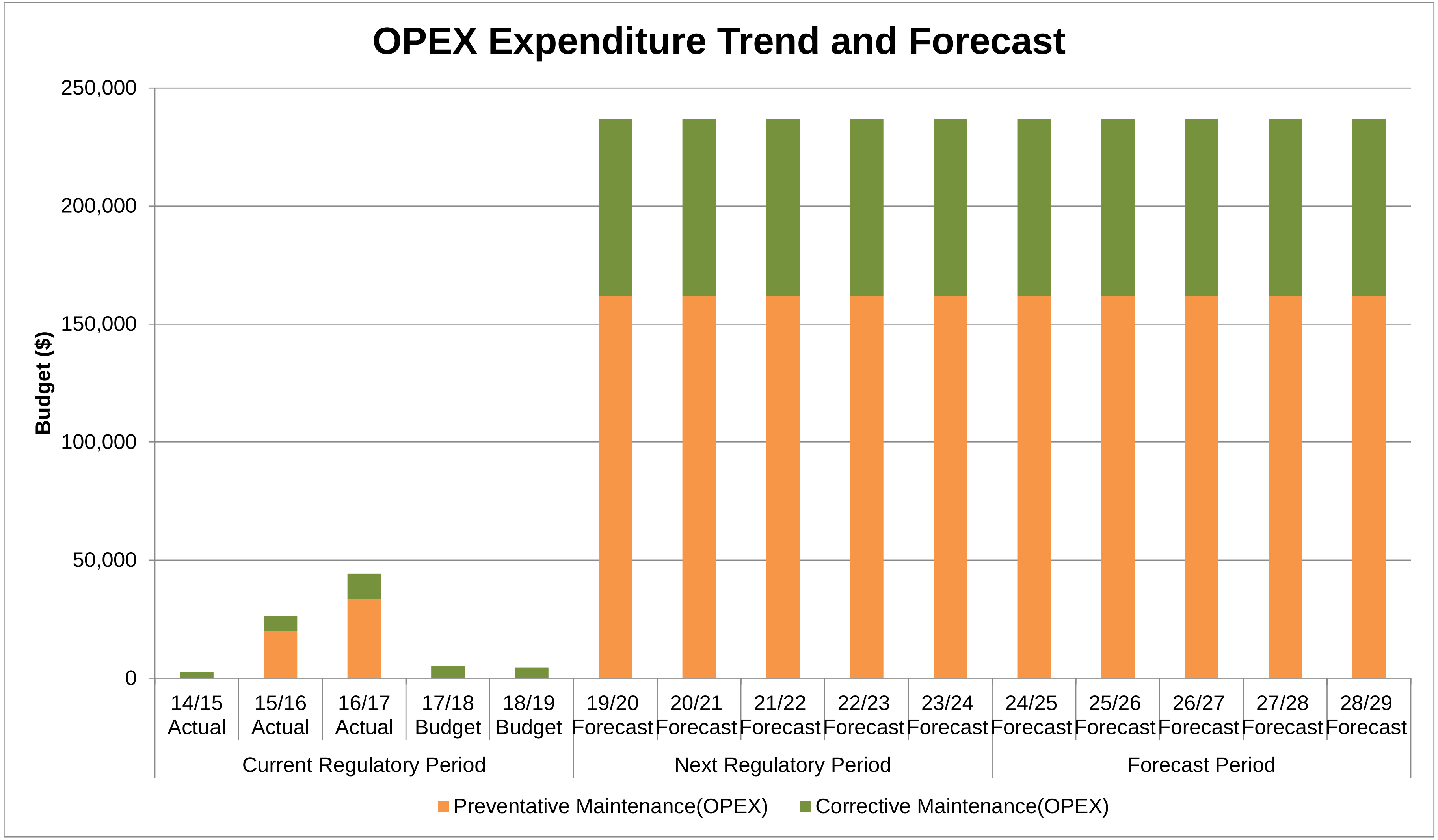

Figure 5: OPEX for Maintenance Program of Communication Assets

Program	Secondary Systems Communications Maintenance and Condition Monitoring
2019-24 Budget	Annual budget for communications asset maintenance: **$237,000**
Scope	This program includes: Planned and unplanned maintenance Condition monitoring
Project(s) Details	**Communications Maintenance and Condition Monitoring** The following maintenance activities are to be undertaken for communications assets on an annual basis: Base Station Ethernet Switch maintenance Distribution Ethernet Switch maintenance Zone Sub Ethernet Switch maintenance Power Supply maintenance DMR Base Station maintenance DMR Gateway maintenance Microwave Radio maintenance UHF Base Station maintenance WAN Device maintenance The following condition monitoring activities are to be undertaken: Media Converter condition monitoring ADSS Optical Fibre condition monitoring OPGW condition monitoring Underground Optical Fibre condition monitoring Pilot Cable condition monitoring 3G/4G Modem condition monitoring Mobile Radio condition monitoring UHF Remote condition monitoring Tele-Protection Device condition monitoring
Risks and Opportunities	Communications asset condition monitoring and maintenance allows the identification and rectification of issues in assets before failure occurs. Condition monitoring is also used to assess the condition and suitability of communications assets and to optimise the on-going replacement program.
	Rollout of increased monitoring to the distribution network will mitigate the risks of disruptive technologies and allow control close to the source of any issues.

Table 11: Secondary OPEX Communication Maintenance Program

7.2 Capital Program

This section outlines the capital expenditure for asset replacement and refurbishment.

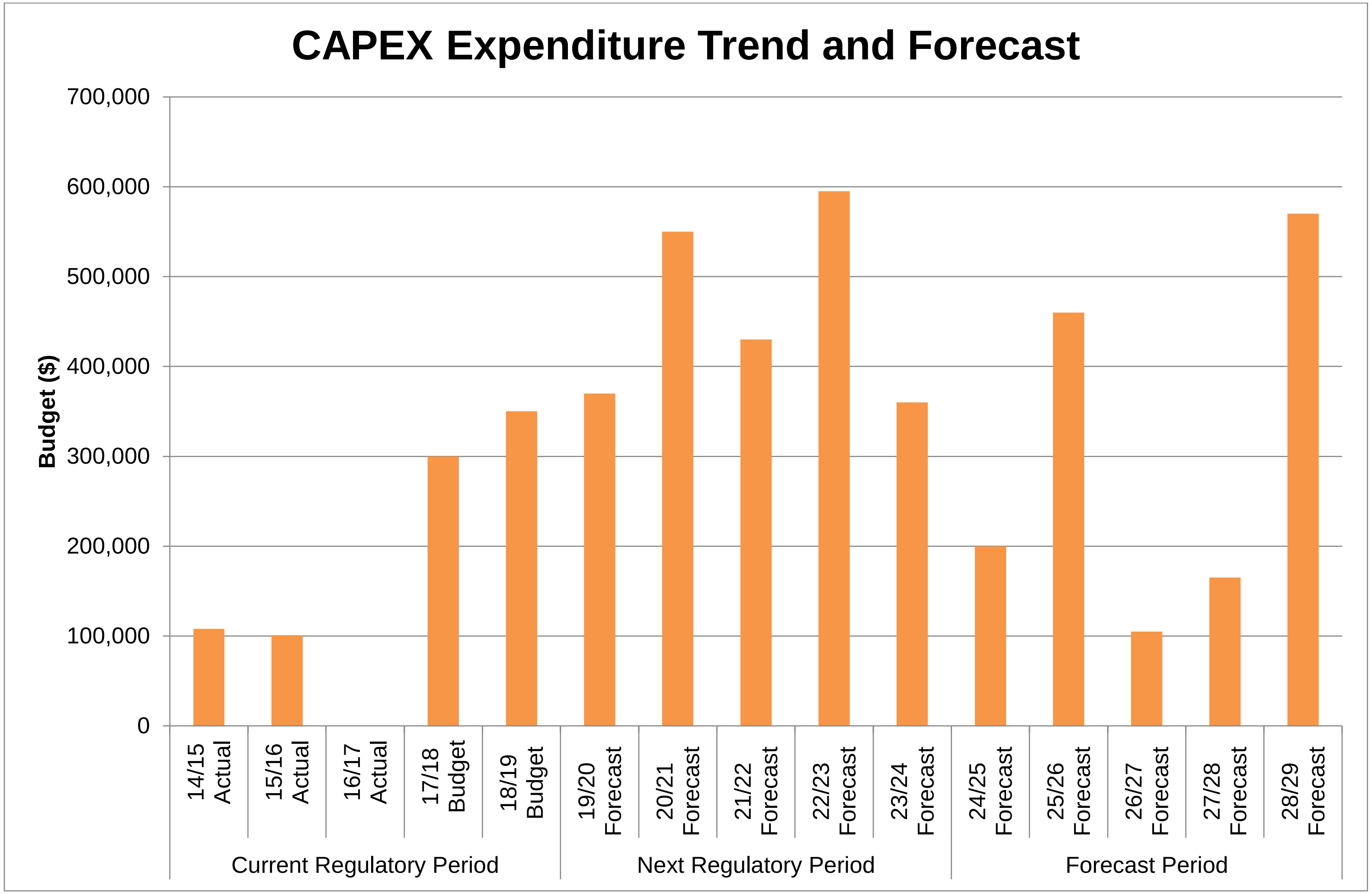

Figure 6: CAPEX Program for Communication Assets

S. No	Project Title	Proposed Budget	Nominated year
1	ZSS Router Replacement	$400,000	2021/24
2	UHF Remote Radio Replacement	$600,000	2019/23
3	Microwave Radio Replacement	$720,000	2020/24
4	TMR Final Replacement with DMR	$240,000	2019/21
5	Pilot Cable Replacement	$200,000	2019/21
6	ZSS Switch Replacements	$105,000	2022/23
7	4G to 5G Modem Replacements	$140,000	2022/24

Table 12: Secondary CAPEX Communication Replacement Program

7.3 Budget Forecast

This section provides a 10 year forecast for the CAPEX & OPEX budgets.

Total Budget	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25	2025/26	2026/27	2027/28	2028/29
CAPEX	**370,000**	**550,000**	**430,000**	**595,000**	**360,000**	**200,000**	**460,000**	**105,000**	**165,000**	**570,000**
OPEX	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**	**237,000**
Planned Maintenance (OPEX)	126,000	126,000	126,000	126,000	126,000	126,000	126,000	126,000	126,000	126,000
Unplanned Maintenance (OPEX)	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000
Condition Monitoring (OPEX)	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000	36,000

Table 13: CAPEX & OPEX 10 Year Budget Forecast

Appendix A Maintenance Plan Details

Appendix A provides additional details of the data used in evaluation of the asset management strategy options, including the costing and budget forecasting.

A.1 Maintenance Task Costing

Unit costs for work on this asset class are held in RIVA and are regularly reviewed against actual project costings. Industry standard estimation techniques are applied as a further review against the project costs and the results updated in RIVA.

A.1.1 Planned Maintenance Tasks

Unit Costs			
Asset Type	**Task**	**Cost Basis**	**Unit Cost**
Communication	Communication maintenance	Comms Upgrade	$250,000
Communication	UHF Radio & Power Supply Test	Cost for testing UHF & Battery Systems (Every 2 years)	$1,800
Communication	Replace switches and routers	Replace critical IT hardware	$20,000

Table 14: Planned Maintenance Task Unit Costs

A.1.2 Condition Monitoring Tasks

Unit Costs			
Asset Type	**Task**	**Cost Basis**	**Unit Cost**
Communication	Monitoring performance of optical fibre links	Cost for testing optical fibre connectivity and performance (Every 2 years)	$3,600

Table 15: Condition Monitoring Task Unit Costs

A.1.3 Reactive Maintenance Tasks

Unit Costs			
Asset Type	**Task**	**Cost Basis**	**Unit Cost**
Communication	UHF Radio Failure & Replacement	Replace UHF radio due to hardware failure	$3,500

Table 16: Reactive Maintenance Task Unit Costs

A.1.4 Asset Unit Costs

Unit Costs		
Asset Type	**Task**	**Unit Cost**
3G/4G Modems	Replacement Cost	$2,000
ADSS Optical Fibre	Replacement Cost	$100,000
Base Station Ethernet Switches	Replacement Cost	$30,000
Distribution Ethernet Switches	Replacement Cost	$15,000
DMR Base Stations	Replacement Cost	$25,000
DMR Gateways	Replacement Cost	$65,000
DWDM Optical Multiplexers	Replacement Cost	$20,000
Media Converters	Replacement Cost	$3,000
Microwave Radios	Replacement Cost	$40,000
Mobile Radios	Replacement Cost	$500
OPGW	Replacement Cost	$100,000
Power Supplies	Replacement Cost	$3,000
Tele-Protection Devices	Replacement Cost (e.g. Jumbo Switches, SEL 2505/2506, and Dewar devices)	$10,000
UHF Base Stations	Replacement Cost	$6,000
UHF Remotes	Replacement Cost	$2,000
Underground Optical Fibre	Replacement Cost	$100,000
WAN Devices	Replacement Cost	$60,000
Zone Sub Ethernet Switches	Replacement Cost	$20,000

Table 17: Asset Unit Costs

Appendix B Risk Definitions

Appendix B provides reference information detailing how the severity of an effect, the probability of failure and the likelihood of detection are defined and ranked for the analysis of risk.

B.1 Severity

Effect	SEVERITY of Effect	Ranking
Catastrophic	Hazardous-without warning. Very high severity ranking, potential failure mode affects safety, noncompliance with policy and without warning.	10
Extreme	Hazardous-with warning. Very high severity ranking, potential failure mode affects safety, noncompliance with policy with warning.	9
Very High	Item inoperable, with loss of primary function	8
High	Item operable, but primary function at reduced level of performance	7
Moderate	Equipment operable, but with some functions inhibited	6
Low	Operable at reduced level of performance	5
Very Low	Does not conform. Defect obvious.	4
Minor	Defect noticed by routine inspection	3
Very Minor	Defect noticed by close inspection	2
None	No effect	1

B.2 Occurrence

PROBABILITY of Failure	Failure Probability	Failure rate Lamda "λ"	Ranking
Very High: Failure is almost inevitable	Very High: Failure is almost inevitable. Possible Failure Rate >= 1 every week.	0.1429	10
	Very High: Failure is almost inevitable. Possible Failure Rate >= 1 every month.	0.0333	9
High: Repeated failures	High: Repeated failures. Possible Failure Rate >= 1 every 3 months.	0.0111	8
	High: Repeated failures. Possible Failure Rate >= 1 every 6 months.	0.0056	7
Moderate: Occasional failures	Moderate: Occasional failures. Possible Failure Rate >= 1 every year.	0.0027	6
	Moderate: Occasional failures. Possible Failure Rate >= 1 every 3 years.	0.0009	5
	Moderate: Occasional failures. Possible Failure Rate >= 1 every 5 years.	0.0005	4
Low: Relatively few failures	Low: Relatively few failures. Possible Failure Rate >= 1 every 8 years.	0.0003	3
	Low: Relatively few failures. Possible Failure Rate >= 1 every 15 years.	0.0002	2
Remote: Failure is unlikely	Remote: Failure is unlikely. Possible Failure Rate >= 1 every 20 years.	0.0001	1

B.3 Detection

Detection	Likelihood of DETECTION	Ranking
Absolute Uncertainty	Control cannot prevent / detect potential cause/mechanism and subsequent failure mode	10
Very Remote	Very remote chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	9
Remote	Remote chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	8
Very Low	Very low chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	7
Low	Low chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	6
Moderate	Moderate chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	5
Moderately High	Moderately High chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	4
High	High chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	3
Very High	Very high chance the control will prevent / detect potential cause/mechanism and subsequent failure mode	2
Almost Certain	Control will prevent / detect potential cause/mechanism and subsequent failure mode	1

Appendix C Asset Failure Modes

C.1 LAN Devices

Table 18 summarises the common modes of failure for LAN assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Devices at the end of the cable will not be able to communicate with network.	5	3	4	60
Copper Port Failure	Failure of the copper communications port. Effect: Devices connected through the port cannot communicate with network.	4	2	4	32
Cyber Security Intrusion	Communications Network is rendered inoperable due to cyber security intrusion. Effect: Various, depending on the nature and scope of the cyber security intrusion; incorrect monitoring of inputs, maloperation of outputs, loss of communications function, loss of monitoring and control of assets connected to the LAN device.	7	1	6	42
Device Lockup	Device locking up, needing reset. Effect: Device will be out of service until a site visit to reset the device.	5	2	4	40
EMI / EMC Interference	Electrical interference from nearby devices or electrical network disturbances. Effect: Device may operate in an unexpected manner, which may be hard to pin point, especially when the problem is intermittent.	5	1	6	30
Flood / Water Damage	Ingress of water from the site becoming flooded or water entering from the roof. Effect: Shorting of components will cause failure of the device.	5	1	4	20
Obsolescence	Device becomes inoperable due to the age of the technology. Effect: No changes can be made to the configuration, maintenance/support not available.	3	2	3	18
Optical SFP Failure	Failure of the optical communications port. Effect: Devices connected through the port cannot communicate with network.	4	3	4	48
Physical Mortality	LAN device is rendered inoperable due to asset deterioration. Effect: Performance will deteriorate until the device stops operating and will need replacement.	5	1	4	20
Power supply failure	Failure of the power supply. Effect: Device will be offline until the power supply is restored/replaced.	5	3	4	60
Site Fire	Damage by fire.	5	1	1	5

	Effect: Device will fail in service; the damage may be limited to the device only.				
Software Corruption	Errors in the programming or configuration of the LAN device software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: Various, depending on the nature and scope of the software fault; loss of communications function.	5	2	4	40

Table 18: Common Modes of Failure for LAN Assets

C.2 Media Converters

Table 19 summarises the common modes of failure for media converter assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Devices at the end of the cable will not be able to communicate with network.	5	3	6	90
Copper Port Failure	Failure of the copper communications port. Effect: Devices connected through the port cannot communicate with network.	5	1	6	30
Flood/Water Damage	Ingress of water from the site becoming flooded or water entering from the roof. Effect: Shorting of components will cause failure of the device.	5	1	6	30
Optical SFP Failure	Failure of the optical communications port. Effect: Devices connected through the port cannot communicate with network.	5	1	6	30
Physical Mortality	Media converter is rendered inoperable due to asset deterioration. Effect: Protection device attached to media converter cannot be monitored or controlled remotely.	5	2	6	60
Site Fire	Damage by fire. Effect: Device will fail in service; the damage may be limited to the device only.	5	1	1	5

Table 19: Common Modes of Failure for Media Converter Assets

C.3 Optical Fibre Network

Table 20 summarises the common modes of failure for ADSS optical fibre network assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Bush Fire	Optical fibre is rendered inoperable due to the high heat from a bushfire damaging the outer or melting the fibres themselves. Effect: Communications network link is out of service until replaced.	5	2	3	30
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Communications network link is out of service until replaced.	5	3	4	60
High Winds	Over time, mechanical failure. Also structures or trees falling over in the wind and severing the cable. Effect: Communications network link is out of service until replaced.	5	2	3	30
Incorrect installation	Failure to meet installation requirements such as minimum bending radius, or appropriate cable supports. Effect: Primary communications network link is out of service until replaced.	5	4	4	80
Lightning strike	High powered lightning strike to the cable or nearby, allowing a surge of electrical power that could damage the outer and melt the fibre cores. Effect: Primary communications network link is out of service until replaced.	5	1	3	15
Physical Mortality	Optical fibre is rendered inoperable due to asset deterioration. Effect: Communications network link is out of service until replaced.	5	1	3	15
Site Fire	Damage by fire. Optical fibre cable damaged where it enters the structure or within the structure. Effect: Fibres or terminations/splices could be melted. Communications network link is out of service until replaced.	5	1	3	15
Vandalism / Firearms	Cable used as a target for shooting practice (or shooting at a bird), or vandals swinging on the cable. Effect: Fibre is severed and communications network link is out of service until replaced.	5	1	3	15

Table 20: Common Modes of Failure for ADSS Optical Fibre Network Assets

Table 21 summarises the common modes of failure for OPGW optical fibre network assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Communications network link is out of service until replaced.	5	3	4	60
High Winds	Extreme winds causing transmission towers/poles to fall or placing extreme pressure on attachment points. Effect: Primary communications link is out of service until replaced.	5	1	3	15
Incorrect installation	Failure to meet installation requirements such as minimum bending radius, or appropriate cable supports. Effect: Primary communications network link is out of service until replaced.	5	4	4	80
Lightning strike	High powered lightning strike to the cable or nearby, allowing a surge of electrical power that could damage the outer and melt the fibre cores. Effect: Primary communications network link is out of service until replaced.	5	1	3	15
Physical Mortality	Optical fibre is rendered inoperable due to asset deterioration. Effect: Communications network link is out of service until replaced.	5	1	3	15
Site Fire	Damage by fire. Optical fibre cable damaged where it enters the structure or within the structure. Effect: Fibres or terminations/splices could be melted. Communications network link is out of service until replaced.	5	1	3	15

Table 21: Common Modes of Failure for OPGW Optical Fibre Network Assets

Table 22 summarises the common modes of failure for underground optical fibre network assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Bush Fire	Optical fibre is rendered inoperable due to the high heat from a bushfire, especially where there are large logs burning above the buried fibre, damaging the outer or melting the fibres themselves. Effect: Communications network link is out of service until replaced.	5	1	3	15
Excavation Damage	Underground optical fibre is rendered inoperable due to excavation in the vicinity of the cable which severs the fibre cores. Effect: Primary communications link is out of service until replaced.	5	3	2	30
Flood / Water Damage	Flooding causing washouts and breakage of the fibre where it is exposed. Effect: Primary communications link is out of service until replaced.	5	2	3	30
Incorrect installation	Failure to meet installation requirements such as minimum bending radius, or appropriate cable supports. Effect: Primary communications network link is out of service until replaced.	5	4	4	80
Physical Mortality	Optical fibre is rendered inoperable due to asset deterioration. Effect: Communications network link is out of service until replaced.	5	1	3	15

Table 22: Common Modes of Failure for Underground Optical Fibre Network Assets

C.4 Pilot Cables

Table 23 summarises the common modes of failure for pilot cable assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Bush Fire	Bush Fire along the route of the buried cable, resulting in the cable melting and becoming unusable. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	1	3	21
Cabling damaged by Vermin / Animals	Vermin or animals such as rats or wombats chewing through the cable or insulation. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	1	3	21
Excavation Damage	Cable dug up and broken during excavation works. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	5	3	105
Flood / Water Damage	Flooding along the cable route causing a washout and breaking of the cable where it loses support. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	2	3	42
Insulation failure	Failure of the insulation of the cable due to age. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	2	3	42
Lightning strike	Lightning strike to the ground in the vicinity of the cable causing it to be damaged. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	1	3	21
Physical Mortality	Pilot cable is rendered inoperable due to asset deterioration. Effect: Protection devices are no longer connected together, so unit protections cannot operate and CBs trip to protect the line.	7	1	3	21

Table 23: Common Modes of Failure for Pilot Cable Assets

C.5 Power Supplies

Table 24 summarises the common modes of failure for power supply assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	Power supply is rendered inoperable due to asset deterioration. Effect: Device will be offline until the power supply is restored/replaced.	7	2	3	42
Rectifier failure	Failure of a redundant rectifier module. Effect: loss of redundancy, which may not be detected.	5	2	6	60

Table 24: Common Modes of Failure for Power Supply Assets

C.6 3G/4G Modems

Table 25 summarises the common modes of failure for 3G/4G modem assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cyber Security Intrusion	Device is rendered inoperable due to cyber security intrusion. Effect: Various, depending on the nature and scope of the cyber security intrusion; incorrect monitoring of inputs, maloperation of outputs, loss of communications function, loss of monitoring and control of assets connected.	6	1	3	18
Device Lockup	Device locking up, needing reset. Effect: Device will be out of service until a site visit to reset the device.	6	7	3	126
Physical Mortality	Device is rendered inoperable due to asset deterioration. Effect: Device will be offline until it is restored/replaced.	6	1	3	18
Software Corruption	Errors in the programming or configuration of the device software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: Various, depending on the nature and scope of the software fault; loss of communications function.	6	2	3	36
Vandalism / Firearms	Damage to the antenna mounted on the top of a substation. Effect: Loss of communications function.	6	3	3	54

Table 25: Common Modes of Failure for 3G/4G Modem Assets

C.7 DMR Base Stations and Gateways

Table 26 summarises the common modes of failure for DMR base station and gateway assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Device Lockup	Device locking up, needing reset. Effect: Device will be out of service until a site visit to reset the device.	6	2	5	60
Lightning strike	Transient overvoltage, Heat. Effect: Communications for the affected channel will be cut off.	6	2	5	60
Physical Mortality	Device is rendered inoperable due to asset deterioration. Effect: Communications for the affected channel will be cut off.	6	2	5	60
Software Corruption	Errors in the programming or configuration of the device software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: Various, depending on the nature and scope of the software fault; loss of communications function.	6	2	5	60
Vandalism / Firearms	Device antenna is rendered inoperable due to vandalism. Effect: Communications for the affected channel will be cut off.	6	2	5	60

Table 26: Common Modes of Failure for DMR Base Station and Gateway Assets

C.8 Mobile Radios

Table 27 summarises the common modes of failure for mobile radio assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Accident	Handset Damage - Handset is rendered inoperable due to damage. Effect: Handset will have to be replaced. Another method of communications will be required.	2	3	1	6
Loss	The portable handset is lost. Effect: Radio will have to be replaced. Another method of communications will be required.	2	3	1	6
Physical Mortality	Mobile radio is rendered inoperable due to asset deterioration. Effect: Radio will have to be replaced. Another method of communications will be required.	2	3	1	6
Theft	Theft of radio from vehicle or theft of vehicle. Effect: Radio will have to be replaced. Another method of communications will be required.	2	2	1	4

Table 27: Common Modes of Failure for Mobile Radio Assets

C.9 Microwave Radios

Table 28 summarises the common modes of failure for microwave radio assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Lightning strike	Transient overvoltage, Heat. Effect: Communications for the affected link will be cut off.	6	2	2	24
Physical Mortality	Microwave radio is rendered inoperable due to asset deterioration. Effect: Communications link is not available until replacement is procured and installed.	6	1	2	12
Vandalism / Firearms	Device antenna is rendered inoperable due to vandalism. Effect: Communications for the affected link will be cut off.	6	2	2	24

Table 28: Common Modes of Failure for Microwave Radio Assets

C.10 UHF Base Stations

Table 29 summarises the common modes of failure for UHF base station assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	UHF base station is rendered inoperable due to asset deterioration. Effect: Communications link is not available until replacement is procured and installed.	5	2	3	30
Lightning strike	Transient overvoltage, Heat. Effect: Communications for the affected channel will be cut off.	5	2	3	30
Vandalism / Firearms	Device antenna is rendered inoperable due to vandalism. Effect: Communications for the affected channel will be cut off.	5	3	3	45

Table 29: Common Modes of Failure for UHF Base Station Assets

C.11 UHF Remotes

Table 30 summarises the common modes of failure for UHF remote assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	UHF remote is rendered inoperable due to asset deterioration. Effect: Radio will have to be replaced.	5	2	3	30
Lightning strike	Transient overvoltage, Heat. Effect: Communications for the affected channel will be cut off.	5	2	3	30
Vandalism / Firearms	Device antenna is rendered inoperable due to vandalism. Effect: Communications for the affected channel will be cut off.	5	3	3	45

Table 30: Common Modes of Failure for UHF Remote Assets

C.12 Tele-Protection Devices

Table 31 summarises the common modes of failure for tele-protection assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Tele-protection function will not operate.	6	3	3	54
Cyber Security Intrusion	Tele-protection function is rendered inoperable due to cyber security intrusion. Effect: Various, depending on the nature and scope of the cyber security intrusion; corruption of data flow, maloperation of outputs, loss of communications function, loss of monitoring.	7	1	6	42
Device Lockup	Device locking up, needing reset. Effect: Device will be out of service until a site visit to reset the device.	6	2	4	48
EMI / EMC Interference	Electrical interference from nearby devices or electrical network disturbances. Effect: Device may operate in an unexpected manner, which may be hard to pin point, especially when the problem is intermittent.	5	1	6	30
Flood / Water Damage	Ingress of water from the site becoming flooded or water entering from the roof. Effect: Shorting of components will cause failure of the device.	5	1	3	15
Obsolescence	Device becomes inoperable due to the age of the technology. Effect: No changes can be made to the configuration, maintenance/support not available.	3	2	2	12

Optical SFP Failure	Failure of the optical communications port. Effect: Tele-protection will be inoperable.	5	3	3	45
Physical Mortality	Device is rendered inoperable due to asset deterioration. Effect: Performance will deteriorate until the device stops operating and will need replacement.	6	1	3	18
Power supply failure	Failure of the power supply. Effect: Device may continue to operate on a redundant supply, but if the supply has completely failed the tele-protection function will not be available.	6	3	6	108
Site Fire	Damage by fire. Effect: Device will fail in service; the damage may be limited to the device only.	5	1	1	5
Software Corruption	Errors in the programming or configuration of the device software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: Various, depending on the nature and scope of the software fault; loss of tele-protection function.	6	2	4	48

Table 31: Common Modes of Failure for Tele-Protection Assets

C.13 WAN Devices

Table 32 summarises the common modes of failure for WAN assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Cabling damaged by Vermin / Animals	Vermin gnawing through cabling or making a home in or on the equipment. Effect: Devices at the end of the cable will not be able to communicate with network.	6	3	3	54
Cyber Security Intrusion	Communications Network is rendered inoperable due to cyber security intrusion. Effect: Various, depending on the nature and scope of the cyber security intrusion; incorrect monitoring of inputs, maloperation of outputs, loss of communications function, loss of monitoring and control of assets connected to the WAN device.	8	1	6	48
Device Lockup	Device locking up, needing reset. Effect: Device will be out of service until a site visit to reset the device.	7	2	4	56
EMI / EMC Interference	Electrical interference from nearby devices or electrical network disturbances. Effect: Device may operate in an unexpected manner, which may be hard to pin point, especially when the problem is intermittent.	6	1	6	36
Flood / Water Damage	Ingress of water from the site becoming flooded or water entering from the roof.	6	1	3	18

	Effect: Shorting of components will cause failure of the device.				
Obsolescence	Device becomes inoperable due to the age of the technology. Effect: No changes can be made to the configuration, maintenance/support not available.	3	2	3	18
Optical SFP Failure	Failure of the optical communications port. Effect: Devices connected through the port cannot communicate with network.	6	3	3	54
Physical Mortality	WAN device is rendered inoperable due to asset deterioration. Effect: Performance will deteriorate until the device stops operating and will need replacement.	7	1	3	21
Power supply failure	Failure of the power supply. Effect: Device will be offline until the power supply is restored/replaced.	6	3	5	90
Site Fire	Damage by fire. Effect: Device will fail in service; the damage may be limited to the device only.	6	1	1	6
Software Corruption	Errors in the programming or configuration of the WAN device software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: Various, depending on the nature and scope of the software fault; loss of communications function.	6	2	4	48

Table 32: Common Modes of Failure for WAN Assets