Appendix 5.13: Secondary systems- SCADA ASP

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

Reference Documents

Document	Version	Date
National Electricity Rules	94	18 July 2017
National Electricity Law **– National Electricity (South Australia) Act 1996**	15.12.2016	
ACT Utilities (Technical Regulations) Act (ACT)		2014
Electricity Distribution Asset Management Policy PO1101	2.0	5/11/2015
Asset Management Strategy SM1192	1.0	14/11/2014
Asset Management Objectives	1.0	08/12/2015
Asset Management System Manual SM1193	1.0	14/11/2014
Asset Management Governance Framework SM1190	1.0	14/11/2014
Disruptive Technology – EN Strategic Direction Plan	V2.16	3 July 2017
ActewAGL Grid Vision 2016-2046		December 2016
Secondary Systems Strategy	1.0	August 2017
ActewAGL ICT Security Standard SM4321	1.0	30/01/2017
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	Definition
AC	Alternating Current
ACT	Australian Capital Territory
ADMS	Advanced Distribution Management System
AEMC	Australia Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
ArcFM	Asset management system, incorporating GIS (Geographic Information System)
ASP	Asset Specific Plan
BSD	Business Systems Division
CAPEX	Capital Expenditure
CB	Circuit Breaker
CPU	Central Processing Unit
CT	Current Transformer
DC	Direct Current
DMS	Distribution Management System
DNP3	Distributed Network Protocol version 3
DRF	Disaster Recovery Facility
FCI	Fault Current Indicator
FLISR	Fault Location, Isolation, and Service Restoration
FMEA	Failure Mode and Effects Analysis
GIS	Geographic Information System
GPS	Global Positioning System
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMI	Human Machine Interface – local touch screen interface to RTUs and IEDs
HV	High Voltage
I/O	Input/Output
ICCP	Inter Control Centre Protocol
IED	Intelligent Electronic Device – microprocessor controlled multi-function protection device
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator

kV	Kilovolt
LBS	Load Break Switch
LED	Light Emitting Diode
LV	Low Voltage
MTBF	Mean Time Between Failures
NER	National Electricity Rules
NSP	Network Service Provider
OPEX	Operational Expenditure
OPGW	Optical Ground Wire
OT	Operational Technology
PoF	Probability of Failure
PoW	Program of Work
PV	Photo-Voltaic panels (solar panel generators)
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
STPIS	Service Target Performance Incentive Scheme
VAR	Volt-Amp Reactive – a measure of reactive power in AC power systems
VT	Voltage Transformer

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 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.

Evoenergy operates a SCADA system and ADMS that provides a variety of services to facilitate the continual operation and monitoring of the electrical distribution system throughout the ACT. The SCADA/ADMS system incorporates the real-time monitoring and control of Evoenergy's distribution network extending from field data collection points (i.e. remote terminal units, reclosers, etc.) to the operator interfaces driven by the master station. The Evoenergy Control Room is the main user of the SCADA/ADMS for network operations. Other uses of the ADMS include performing network technical studies and planning functions.

SCADA assets providing electricity network 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 strategic direction to determine the optimal strategy to maintain and replace SCADA assets over their lifetime. 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 SCADA 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 SCADA assets in the changing distribution network environment.

Accordingly, the condition and technical capabilities of SCADA 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 SCADA asset type and selects the optimal strategy for maintenance. Where existing assets are not capable of providing functionality, or where technology advances render existing assets obsolete, strategic replacement prior to asset end of life is recommended. A greater penetration of SCADA 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, communications and other asset 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 CAPEX and OPEX is presented in Table 1.

Total Budget	2019/20	2020/21	2021/22	2022/23	2023/24
CAPEX (Replacement Program)	**575,000**	**225,000**	**375,000**	**300,000**	**225,000**
OPEX	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**
Planned Maintenance (OPEX)	75,000	75,000	75,000	75,000	75,000
Unplanned Maintenance (OPEX)	25,000	25,000	25,000	25,000	25,000
Condition Monitoring (OPEX)	0	0	0	0	0

Table 1: OPEX and CAPEX Optimised Program of Work Budget

This ASP presents a broad-based program of works in terms of CAPEX replacements, a greater penetration into the distribution network for SCADA assets, and an optimised program of work approach for maintenance. CAPEX replacement projects are justified based on various option considerations in a Project Justification Report.

2 Asset Class Overview

This ASP covers the SCADA asset class within the secondary systems asset portfolio. The SCADA assets within this class are responsible for providing real-time and historical information for the critical function of electrical network monitoring and control. For details of the asset groups contained within the SCADA 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

Table 2 provides a broad-based classification of asset groups within the asset class.

Asset Class	Secondary Systems SCADA
Asset Groups	HMI Computer GPS Distribution RTU Zone Sub RTU Distribution Network Monitor (future) Fault Current Indicator

Table 2: Asset Classification – SCADA Assets

2.3 Asset Functions

SCADA assets provide real-time and historical information for the effective operation and monitoring of the electrical network. SCADA is a key component of the overall electricity network management system. The functions of network management systems include:

- Manage the network state: Real-time monitoring, control and analysis of the network to optimise network performance;
- Administer planned work: Determine outage needs in order to perform requested work, notify interested parties and arrange access and/or switching as required;
- Administer unplanned faults: Using information reported by customers and SCADA, diagnose and isolate faults and notify interested parties;
- Network control analysis and forecasting: Ongoing assessment of network performance to determine future action required to ensure supply reliability and reliability reporting as required by interested parties;
- Regulatory compliance: Comply with the NER requirements for Inter Control Centre Protocol (ICCP) reporting of system status and performance to AEMO and TransGrid;
- Manage emergencies: Preparation and execution of emergency management plan to respond to major outages and ongoing emergency management exercise; and
- Provide ancillary asset data: Provide asset condition information and other data related to primary and secondary systems.

2.3.1 Asset Function Definitions

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

2.3.1.1 HMI Computer

The mimic panels installed in the zone substations and HV switching stations are in varying states of repair and functionality due to age, end of life componentry and technological obsolescence. Some of the mimic panels have non-operational segments meaning that the panel is not presenting an accurate indication of the operational configuration of the substation. The missing indications present an issue when operators are on site, as they have to verify the status and alarm state of the substation by other means. In addition the mimic panels' design and build is not compatible with the latest generation of IEDs. In their current form, the mimic panels cannot be modified or upgraded to support IEDs.

The mimic panels in the zone substations and HV switching stations are being replaced by SCADA HMI displays. The HMI displays are a single-screen 21” display powered by a dedicated Windows PC located in the cabinet. The SCADA HMI fully integrates with the SCADA interfaces and provides a touch screen graphical interface to view the status of the system, event logs and alarm lists, and is able to control SCADA connected equipment within the substation.

The home screen display is a single line diagram of the substation showing the status of all assets in the substation. By switching screens the HMI can also show event history, alarms view, communications overview, analogue values, and relay health overview screens.

The HMI can be used to carry out local fault analysis, local testing of substation equipment and can be used to control the assets located in the substation. The introduction of the HMI into the zone substations allows for complete local control of the zone substation in conditions where communications have been lost between the substation and the control centre or the control centre is otherwise unavailable.

In the event of a loss of remote control from the control centre, the HMI can be used to control the substation locally under direction from the control centre. This facility ensures that the substations can be controlled and co-ordinated in a major event, such as a bushfire or a cyber security incident, where some communications links may be impacted.

All of the zone substations and HV switching stations will be gradually upgraded to incorporate SCADA HMI interfaces over the Regulatory Periods. Bruce switching station and Tennent zone substation have been upgraded with HMI. City East, Belconnen & Woden zone substations are programmed to be upgraded over the current Regulatory Period.

2.3.1.2 GPS

The function of the GPS clocks is to provide accurate synchronised time sources for the critical geographically separate parts of the SCADA network (data centres, zone substations and HV switching stations). This ensures that SCADA servers are synchronised, events and alarms gathered by RTUs and other devices in zone substations are accurately time-stamped, and Sequence of Events can be determined for fault conditions.

2.3.1.3 Distribution RTU

The function of the distribution RTUs is to provide monitoring and control of electrical network assets at the distribution substation level. The distribution RTUs are installed in chamber substations, padmount substations and switching stations in the 11kV distribution network. They are typically a combination of hardwired I/O and OP interfacing to IEDs, monitoring up to 100 I/O points for each site.

Distribution RTUs are either self-contained, or single-chassis based with processor, power supply and a few I/O modules.

2.3.1.4 Zone Sub RTU

The function of the zone substation RTUs is to provide monitoring and control of electrical network assets at the zone substation level. The zone RTUs are installed in zone substations and HV switching stations. They are typically a combination of hardwired I/O and OP interfacing to IEDs, monitoring more than 100 I/O points for each site.

Zone substation RTUs are rack/chassis based, with separate processor modules, power supply modules and I/O modules. Each installation can have from 1 to 4 chassis. In some cases, the internal communication bus is extended for remote I/O monitoring to reduce electrical cabling costs.

2.3.1.5 Distribution Network Monitor

The function of the distribution network monitors is to provide monitoring of electrical network assets on the LV side of distribution substations, in order to monitor and manage power quality issues resulting from disruptive technologies such as grid-connected photovoltaics and battery storage.

2.3.1.6 Fault Current Indicator

The function of the Fault Current Indicators is to detect fault events on overhead distribution lines and provide digital and analogue fault data information for intelligent switching and restoration decisions. A conductor temperature sensor is also available as an important diagnostic tool to evaluate line sag and potential hotspots. Load levelling and load memory features enable FCIs to automatically set fault trip current rating in relation to peak load current. When an FCI detects fault current above its trip current rating, it sends a signal to the pole-mounted concentrator and begins to flash a bright red blinking LED. In addition to event based fault identification, the FCI also communicates fault data, load current and status data, enabling rapid fault location and service restoration as part of Evoenergy’s FLISR (Fault Location, Isolation, and Service Restoration) system approach.

2.4 Needs and Opportunities

Station monitoring and control of the distribution network is currently performed via RTUs in the field as well as a limited number of intelligent field devices such as reclosers and load break switches (LBSs). To date, Evoenergy’s telemetry philosophy is focused primarily on full coverage of all zone substations, with a growing degree of penetration into the distribution network. Many devices in the distribution network may be capable of or warrant monitoring, including distribution substations, reclosers and LBSs. In future, the need for station monitoring will be decided by using a set of defined criteria. Evoenergy intends to implement SCADA using a strategic and standard approach to extend network coverage and support the need for improved asset data for monitoring and control functions. The extent of existing SCADA coverage of the network is limited almost exclusively to zone substations, HV switching stations, approximately 10 percent of chamber distribution substations, and a small number of padmount distribution substations.

2.4.1 Needs

The most significant element of risk for SCADA assets is the reliability consequence associated with SCADA 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 SCADA 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 SCADA penetration into the distribution network. All of this has to be performed in a regulatory environment that is driving down expenditure and capping costs. The decisions on the upgrade and extension of the SCADA assets 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.

The following needs and challenges have been identified for SCADA:

- Additional zone substations
- Embedded generation and its penetration into the distribution network
- Internet of Things (and Big Data) which requires more monitoring devices to be connected to each other
- Data-driven decision making
- Increased penetration of SCADA, resulting in:
  - A need for a centralised system to manage configuration and remote debugging, leading to potential reduction in reactive maintenance OPEX costs. This drives the adoption of IP-based communication for this to be more effective.
  - A need to invest in cyber security measures, as more devices means greater vulnerability
- There are some existing installations of assets that communicate using the Conitel protocol, requiring protocol converter RTUs. This increases asset count and knowledge retention for maintenance and troubleshooting. These assets are to be replaced with current technologies and standard supported protocols such as DNP3.
- Cyber security.

These needs and challenges are explored in the following sub-sections.

2.4.1.1 Additional Zone Substations

There are 3 zone substations planned to be installed by Evoenergy in the 2019-2024 Regulatory Period, and these will all involve additional RTUs, HMIs and GPS devices.

Additionally, the TransGrid Stockdill substation will require the installation of OPGW links and the implementation of transmission line unit protection devices. Refer to the *Communications ASP* and *Zone Substation Protection ASP* for details of how these assets are managed.

2.4.1.2 Embedded Generation

Embedded generation poses a number of challenges for the electrical distribution network. The distribution network was designed to deliver reliably generated electricity to predictable loads. With the advent of wind farms, solar farms and rooftop photovoltaic systems feeding into the network, a great deal of complexity and variability is added. Increasingly, the distribution network is being asked to do things that it was never designed to do.

Maintaining the quality of electricity within regulatory parameters will become ever more difficult as embedded generation increases its penetration into the distribution network. Voltage levels, power levels, and frequencies must be managed across the network as generators drop in and out due to prevailing conditions of wind and sunlight. Harmonic distortions introduced by feed-in inverters of differing manufacturing standards could also become an issue in the near to intermediate future. Power factor correction measures may also need to be taken in order to ensure system losses are kept to a minimum.

Management of energy usage versus generation is another factor that needs to be considered. The generation of large amounts of power during the middle of the day (when often this is one of the lower domestic usage periods) will require storage facilities such as batteries to even out the changing nature of energy peaks and troughs.

The rate of changes affecting the electricity transmission and distribution industry is increasing rapidly. Government policies such as increased renewable energy targets, emerging technologies such as embedded generation, energy storage and electric vehicles, consumer engagement such as management of their energy generation and utilisation, and changes to tariff structures are all contributing to significant changes in Evoenergy's operating environment. In response, SCADA will need to play an increasing role in asset monitoring and control at the distribution substation level.

2.4.1.3 The Internet of Things and Increased Monitoring Requirements

Numerous technologies have converged in recent years to make the concept of the Internet of Things (IoT) an imminent reality. Increasingly, the inter-networking of smart devices from consumer goods to electric cars to home automation systems to building management systems and beyond will become the new reality.

The challenge for the electricity network, and for SCADA in particular, is to keep up with the increasing monitoring of data that will result from the Internet of Things. As part of the brave new world of interconnected appliances and devices, monitoring of energy consumption and consumer energy management will become achievable with much greater granularity of control than previously possible.

With the ability to load manage or load shed individual devices (for example control of air conditioner units), and the ability to more effectively balance distributed power generation with energy usage, there exists a great opportunity to revolutionise the electricity network.

The challenge faced by SCADA systems and communications systems is to be able to keep pace with the sheer volume and complexity of data that will flow as a result of the Internet of Things, and to interface securely across the interconnected data networks that private residences and business premises are becoming. The scale of data storage, processing and analysis needed by the Internet of Things will require investment in infrastructure as we enter the age of Big Data systems.

2.4.1.4 Data-Driven Decision Making

As the quantity and quality of data received from the field continues to increase, the challenge faced by the SCADA system will be to use the data to inform decision making. The SCADA system will allow Evoenergy to take advantage of and respond to the changing face of electricity distribution networks and disruptive technologies such as PV, micro-generation and batteries, through enablement of real-time data acquisition on the change in supply requirements related to time, events and customer requirements. This data can be provided to ADMS for real-time tactical demand response, stored on a central repository, and analysed to enhance network planning and asset management. This will lead to informed decision making on network augmentation or upgrades, asset renewal and optimised asset maintenance.

2.4.1.5 Cyber Security

Historically, SCADA system cyber security was maintained through physical separation from other networks, and the esoteric nature of the proprietary protocols and software utilised. Increasingly with interconnected SCADA and corporate network systems that are connected to the internet, the attack vectors and threats of cyber-attack becomes significantly higher. Additionally off-the-shelf products and standards-based protocols such as DNP3, allow knowledgeable attackers to target SCADA systems. The tools and techniques employed by threat agents are becoming more complex and targeted, hence the risk of disruption when they are successful is increasing in magnitude. The threat of cyber security incursion into the SCADA system must be addressed as an operational priority.

The risk of adverse impacts on SCADA systems from cyber security incursions, either in the form of targeted attacks or unintentional collateral damage, has been increasing in recent years. SCADA 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.

The risk and consequences of a cyber security breach within an OT/SCADA system are different to those within a corporate IT environment. Safety, system integrity, system availability, and real-time operation are key requirements for OT/SCADA system monitoring and control of critical infrastructure. As a result, response to OT/SCADA system breaches must be rapid and decisive in order to minimise the downtime of monitoring and control functionality, and to lessen the risk of damage to assets and the threat to public safety.

At the device level, RTUs and HMIs 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.

At the accessibility level, access to devices (RTUs and HMIs) must be restricted with appropriate levels of password protection and system restriction as per Evoenergy's IT and OT management standards. User and administrator privileges (for example read-only access or full read-write-execute access) must also be managed accordingly, ensuring a balance between system usability and system security across a number of organisational roles.

Appropriate levels of device and application logging should be in place, in order to allow for intrusion detection procedures to be effective, and to ensure that enough data is available for forensic analysis in the event of a successful or partially successful cyber security event.

Backup strategies should be in place to allow for restoration of individual devices or the full system. This would include such components as RTU configuration files, device drivers, HMI operating systems, and local HMI monitoring and control software.

Finally, communications staff, SCADA support staff and engineering staff should have the appropriate level of cyber security awareness and training in order to conduct their duties in a safe and secure manner, and to ensure timely and appropriate response to a cyber security intrusion.

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

The following opportunities have been identified for SCADA:

- Provision of more monitoring and control SCADA devices for greater visibility of power quality within the electrical distribution network
- Implementation of IEC 61850 protocol with its maturity and increasing adoption amongst other electrical utilities in Australia. In keeping with Evoenergy's strategic direction, all future green field zone substation sites will be implemented using the IEC 61850 protocol.
- Retro-fitting existing chamber distribution substations with SCADA monitoring and control capability where possible
- Enabling of SCADA communications with 3G/4G technologies where restrictions exist in installation of antenna structures
- Intelligent network monitoring and control
- HMI software management.

These opportunities are explored in the following sub-sections.

2.4.2.1 Increased SCADA Penetration

Access to information provides the opportunity to make the distribution network more robust, reliable, flexible, responsive and affordable. Regulatory requirements see an ever-increasing need for additional information about the network. As more IEDs and RTUs are installed, there is an increased SCADA penetration into the distribution network. This results in more devices providing Evoenergy with more pertinent information about the state of the network, so that the most appropriate control actions can be taken in response to such things as changes in load, clearing of faults, re-routing of supply, or bushfire mitigation.

Additionally, in response to the growing penetration of PV, the increase in SCADA monitoring of power quality will allow voltage profiling to be gathered for volt/VAR control and optimisation, for improved electrical network efficiency and management of power quality issues resulting from photovoltaics.

2.4.2.2 Intelligent Network Monitoring and Control

The SCADA system is transitioning to an integrated network which combines protection, control and monitoring of the electricity network into one central system. Over the course of the Regulatory Periods 2014-2019 and 2019–2024 the devices installed, upgraded and replaced on the transmission and distribution networks will be numerical protection relays. The capabilities of these devices, combined with the ADMS and the new communications network, provides Evoenergy with an integrated secondary systems environment that will yield significant benefits for the management of assets and control of the electricity network.

Application of heuristic methods in a complex monitoring and control network will enable a degree of intelligence to be incorporated into the control system. The presence of intelligent monitoring (e.g. fault current indicators) will enable far more rapid identification of issues and fault conditions, allowing operators to be more proactive in managing the network. This will result in minimisation of outage impacts and durations resulting in more effective utilisation of the network and lower operating costs, improving SAIFI, SAIDI, and related indices. Impacts on the clients will be minimised and safety of personnel will be protected.

Another aspect of the next generation of SCADA network will be the ability to apply embedded intelligence to the management of the electricity network. Potential faults and issues on the electricity network will be detected much more quickly based on improved monitoring and comparison with historical data. The ADMS/SCADA system will “learn” based on historical events, advanced programming and input from the monitoring capability of the SCADA network. Options will be able to be presented to the operators well before a condition reaches a trigger or alert level. Mitigation will be able to be initiated prior to an issue or fault occurring.

Fault Location, Isolation, and Service Restoration (FLISR) provides manual, semi-automated and fully automated Smart Grid management of power distribution networks in order to assure the quality of power supply. In situations of contingency, due to occurrences that result in interruptions of the power supply, it is indispensable to quickly minimize the number of affected customers until reestablishment of supply. By reconfiguring the distribution network, it is possible to isolate faults and transfer loads to other healthy feeders.

2.4.2.3 HMI Software Management

Currently, HMIs installed at zone substations and HV switching stations provide local monitoring and control of electrical assets. The HMIs rely on local Windows-based servers with ClearSCADA control systems installed on them.

Ongoing security management (antivirus, firewall, etc.), patch management (Windows updates) and software management (ClearSCADA updates) is required to ensure the HMIs remain reliable and secure. Windows updates, security updates and other patches should be reviewed on a testbed system before rolling out to substation HMIs, to ensure HMI functionality is not compromised by any operating system or complementary software updates. Once verified as safe on the testbed system, the updates can be installed on the substation HMIs.

In order to streamline and simplify asset management of HMIs, it is proposed to replace existing thick client ClearSCADA HMIs with thin client HMIs, leveraging the in-built web server-based SCADA HMI functionality of ABB RTUs, providing static and dynamic components, event and alarm lists, system events, and trend charts.

It is proposed that HMI hardware be replaced on a 7-year cycle, in order to address cyber security issues, avoid obsolescence and allow for easier maintenance. HMI operating systems will be updated on an as-need basis in accordance with vendor recommendations and Evoenergy's internal IT and OT management practices.

2.5 Associated Asset Classes

The operation of SCADA assets is associated with other asset classes. Specifically, this involves the communication system and electrical network assets connected to the SCADA system for monitoring and control.

Current asset class associations:

- Hardware:
  - Transformers
  - CB Isolators
  - Reclosers
  - Gas Switches
  - RTUs
  - Protection Relays
  - System Monitoring Devices
  - Battery Chargers
  - Wireless Routers
  - Surveillance Cameras
  - Infrared Monitors
  - Physical Access Control
  - Corporate PCs
  - IP Telephones.
- 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

SCADA asset data are recorded in the ArcFM GIS.

Table 3 gives details of Evoenergy's in-service SCADA assets as at August 2017.

Asset Type	Quantity	Design Life (yrs)	Average Age (yrs)	Oldest Age (yrs)
HMI Computer	11	7	7	24
GPS	10	15	5	9
Distribution RTU	105	15	5	28
Zone Sub RTU	40	15	10	29
Distribution Network Monitor (future)	20 (proposed)	15	1	1
Fault Current Indicator	12	15	1	1

Table 3: In-service Assets

NOTE

The quantity of 40 zone substation RTUs given in Table 3 is the total number of RTU chassis. The actual quantity of logical zone substation RTUs is 16, with each logical RTU containing one to four chassis.

3.2 Asset Service Life Expectancy

The design life of SCADA 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 SCADA assets.

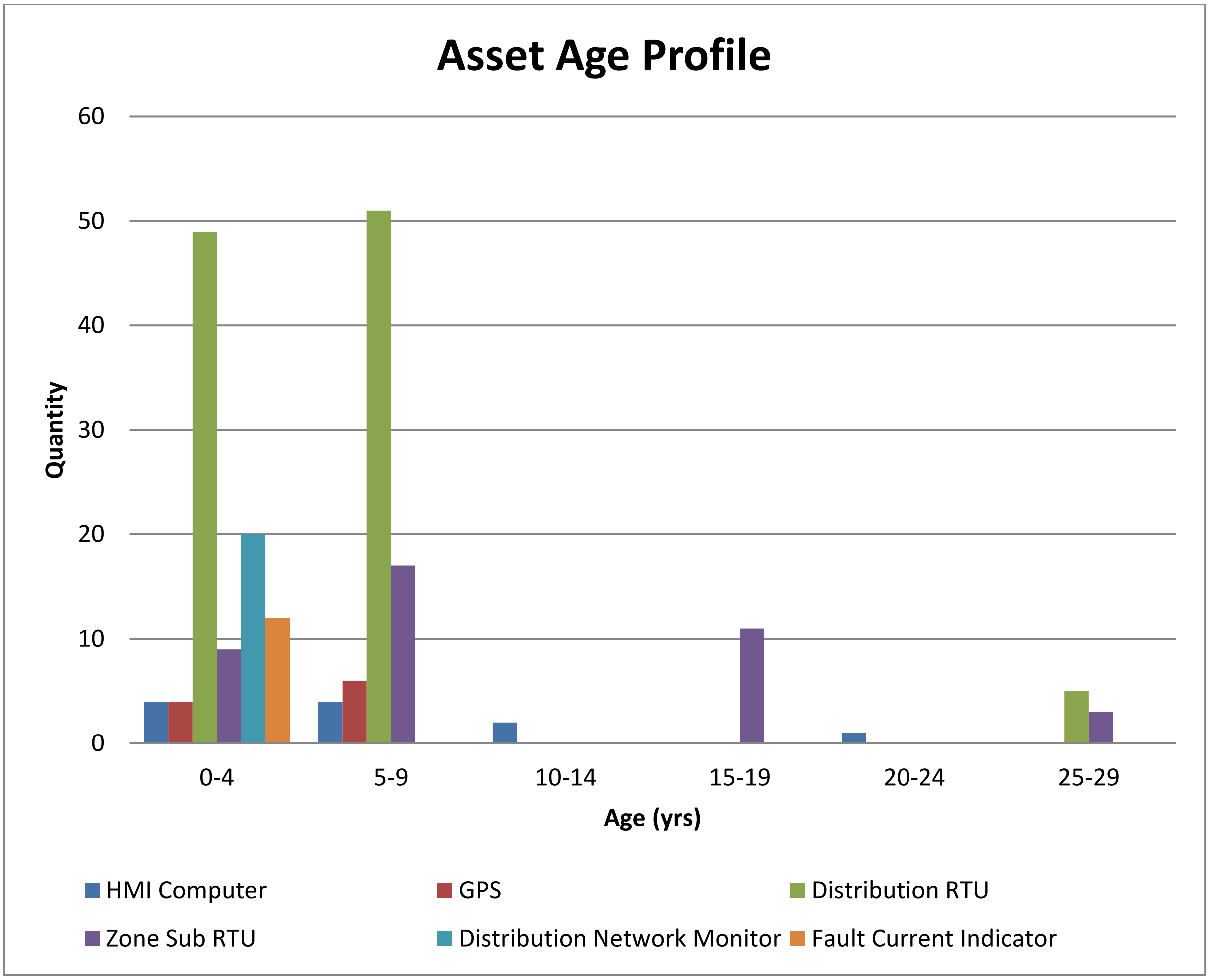

Figure 1: Age Profile of SCADA Assets

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 capacity to meet requirements, the asset reliability and its level of obsolescence. 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.

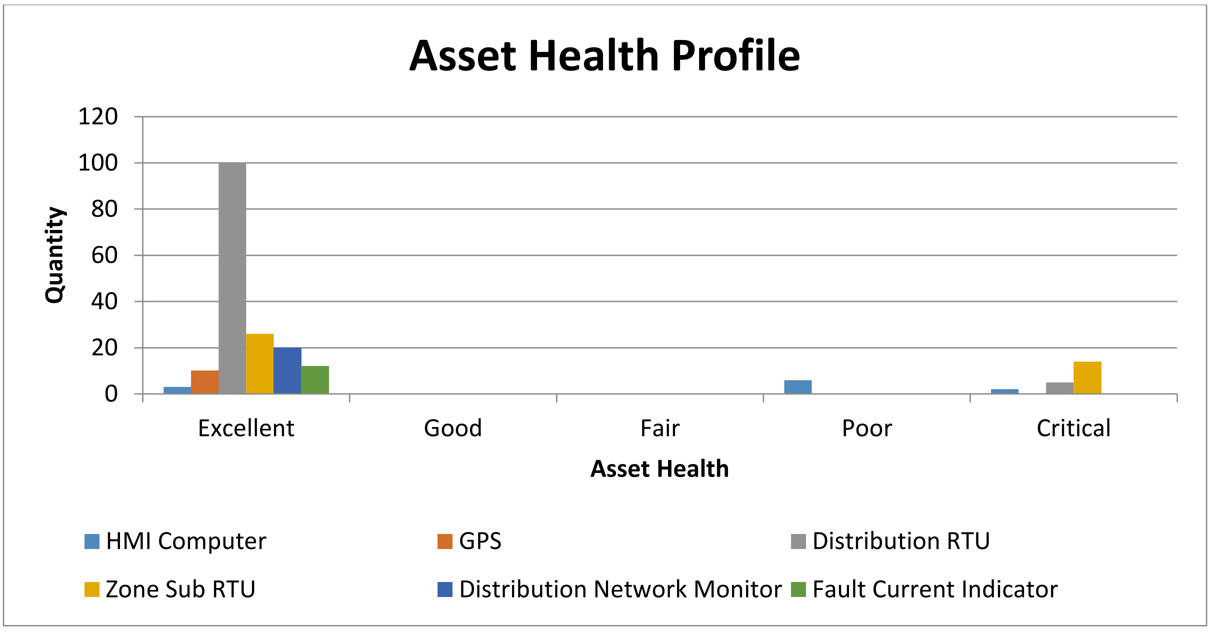

Figure 2: Asset Health Profile of SCADA Assets

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 the SCADA assets.

Asset Type	Manufacturer	Model	Quantity	Average Health
HMI Computer			**11**	**Poor**
	Advantech		**3**	**Excellent**
		(blank)	3	Excellent
	IBM		**7**	**Poor**
		(blank)	7	Poor
	LEEDSNORTHRUP		**1**	**Critical**
		(blank)	1	Critical
GPS			**10**	**Excellent**
	TEKRON		**10**	**Excellent**
		TCG-01E	8	Excellent
		TCG-01G	2	Excellent
Distribution RTU			**105**	**Excellent**
	ABB		**20**	**Excellent**
		560CID11	20	Excellent
	INVENSYS		**79**	**Excellent**
		SCD5200	77	Excellent
		C50	2	Excellent
	LEEDSNORTHRUP		**2**	**Critical**
		C25	1	Critical
		C225	1	Critical
	LOGICA		**3**	**Critical**
		MD3311	3	Critical
	Schneider		**1**	**Excellent**
		OTHER	1	Excellent
Zone Sub RTU			**40**	**Fair**
	ABB		**3**	**Excellent**

		OTHER	3	Excellent
	GEHARRIS		**6**	**Critical**
		D25	6	Critical
	INVENSYS		**25**	**Excellent**
		SCD5200	25	Excellent
	LEEDSNORTHRUP		**3**	**Critical**
		C225	1	Critical
		C2025	2	Critical
	MITS		**3**	**Critical**
		MD1000	3	Critical
Distribution Network Monitor			**20**	**Excellent**
	(blank)		**20**	**Excellent**
		(blank)	20	Excellent
Fault Current Indicator			**12**	**Excellent**
	(blank)		**12**	**Excellent**
		(blank)	12	Excellent

Table 4: Current SCADA Asset Condition

Based on the information in Table 4, the following assets are either at or approaching end of life conditions which should be managed by the preferred asset class strategy:

- Leeds and Northrup HMI computer
- Leeds and Northrup distribution RTUs
- Logica distribution RTUs
- GE Harris zone substation RTUs
- Leeds and Northrup zone substation RTUs
- MITS zone substation RTUs.

3.5 Projected Asset Count

The projected asset count is an estimate of the number of SCADA 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.

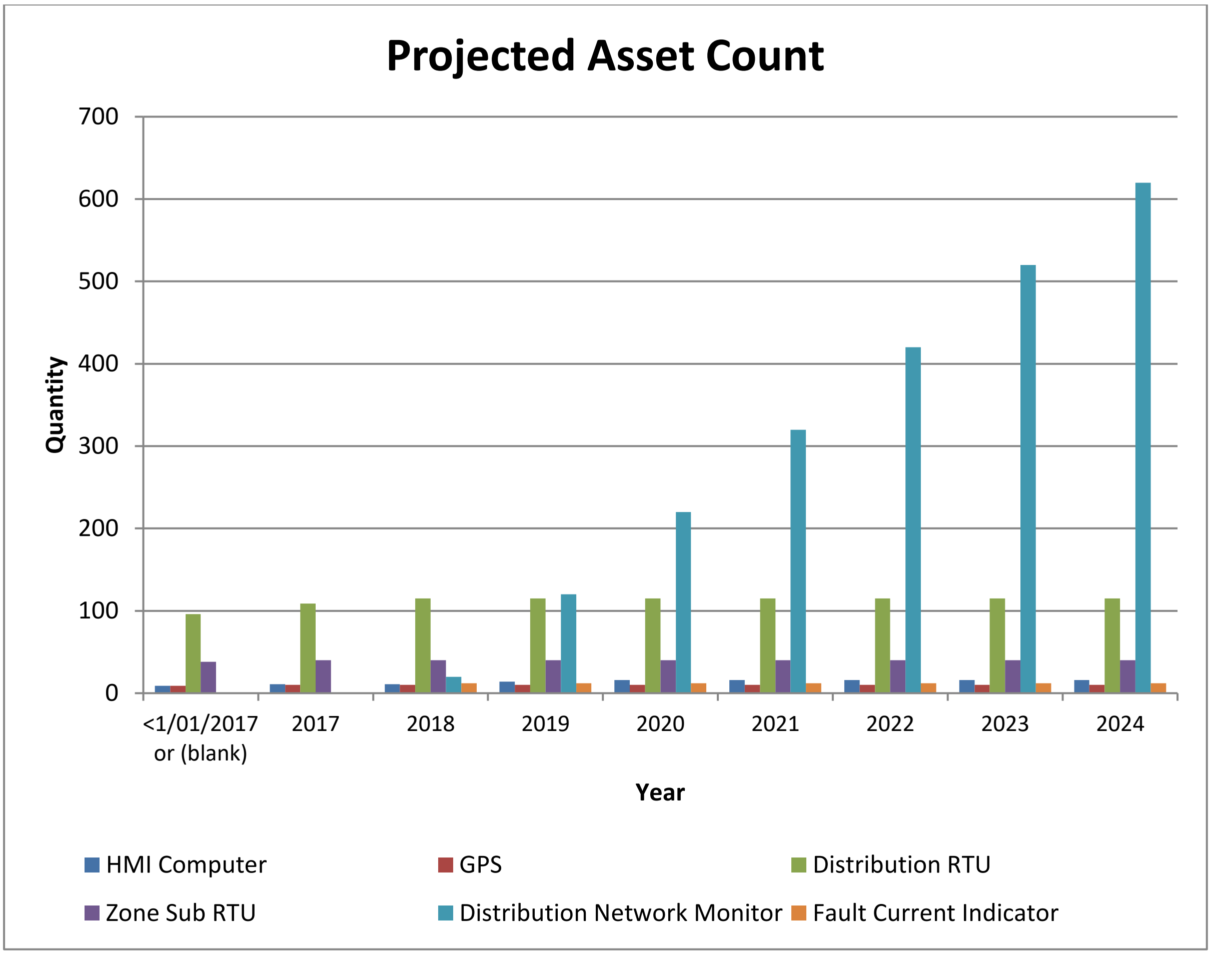

Figure 3: Projected Asset Count of SCADA Assets

3.5.1 Network Augmentation and Infrastructure Development

The following network augmentation projects affect the asset class population.

3.5.1.1 Molonglo Zone Substation

The new zone substation at Molonglo will require the installation of zone substation RTU(s), a GPS and a HMI in the substation.

3.5.1.2 Mitchell Zone Substation

The new zone substation at Mitchell will require the installation of zone substation RTU(s), a GPS and a HMI in the substation.

3.5.1.3 Strathnairn Zone Substation

The new zone substation at Strathnairn will require the installation of zone substation RTU(s), a GPS and a HMI in the substation.

3.5.1.4 Stockdill Zone Substation

The new TransGrid substation at Stockdill will require the installation of line protection on the Canberra-Stockdill-Woden transmission line. Unit protection will be the responsibility of Evoenergy, so OPGW will have to be installed from the Canberra-Woden transmission line to Stockdill substation.

3.5.1.5 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 have 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, and to protect Evoenergy network assets from damage.

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 SCADA 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.

4.1.1 HMI Computer

Table 5 summarises the common modes of failure for HMI Computer assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	HMI is rendered inoperable due to asset deterioration. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	3	3	45
RTU HMI CPU Card Failure	Failure of RTU's CPU card that connects the RTU to the HMI. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	2	3	30
HMI Monitor Failure	Failure of HMI monitor or touch screen. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	2	3	30
HMI Peripheral Device Failure	Failure of HMI mouse or keyboard. Effect: Local users are unable to interact with the HMI.	4	2	3	24
HMI PC Failure	Hardware failure of HMI PC. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	3	3	45
HMI PC HDD Failure	Failure of HMI hard drive. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	2	3	30
Obsolescence	HMI is no longer able to perform its function due to advances in technology, and no upgrade path is available to restore function. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	3	3	45
HMI Operating System Failure	Failure of HMI operating system. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	3	3	45

HMI Software Interface Failure	Errors in the programming or configuration of the HMI software not detected during acceptance testing, or errors introduced due to updates or patches. Effect: The HMI displays incorrect asset data from the RTU(s) or issues incorrect asset controls to the RTU(s).	4	2	4	32
Cyber Security Intrusion	HMI is rendered inoperable due to cyber security intrusion. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	2	5	50
Accident	HMI is rendered inoperable due to accidents such as fire. Effect: Local users are unable to monitor or control substation SCADA-enabled assets from the HMI.	5	2	1	10

Table 5: Common Modes of Failure for HMI Computer Assets

4.1.1.1 Deterioration Drivers

HMIs are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Wear and tear of moving parts such as fans.

4.1.2 GPS

Table 6 summarises the common modes of failure for GPS assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	GPS is rendered inoperable due to asset deterioration. Effect: Time synchronisation of RTUs, IEDs and HMIs will start to drift.	5	2	5	50
GPS Antenna Failure	GPS antenna fails and GPS satellite connections are lost. Effect: Time synchronisation of RTUs, IEDs and HMIs will start to drift.	5	2	3	30
GPS Antenna Cable Failure	GPS antenna cable fails due to corrosion or breakage, and GPS satellite connections are lost. Effect: Time synchronisation of RTUs, IEDs and HMIs will start to drift.	5	2	5	50
GPS Data Cable Failure	GPS data cable fails due to corrosion or breakage. Effect: Time synchronisation to one or more of RTUs, IEDs and HMIs will start to drift.	5	2	5	50
Accident	GPS is rendered inoperable due to	5	2	1	10

	accidents such as fire. Effect: Time synchronisation of RTUs, IEDs and HMIs will start to drift.				

Table 6: Common Modes of Failure for GPS Assets

4.1.2.1 Deterioration Drivers

GPSs are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Wear and tear of moving parts such as fans.

4.1.3 Distribution RTU

Table 7 summarises the common modes of failure for Distribution RTU assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	RTU is rendered inoperable due to asset deterioration. Effect: Loss of monitoring and control of assets connected to the RTU.	6	3	2	36
CPU Module/Card Failure	RTU CPU module/card fails. Effect: Loss of monitoring and control of assets connected to the RTU.	6	2	2	24
I/O Module/Card Failure	RTU I/O module/card fails. Effect: Loss of monitoring and control of assets connected to the RTU through the failed I/O module/card.	5	2	3	30
I/O Wiring Failure	Wiring between RTU and I/O fails due to corrosion or breakage. Effect: Loss of monitoring and control of assets connected to the RTU through the failed I/O wiring.	5	2	3	30
Communications Port Failure	RTU communications port fails. Effect: Loss of monitoring and control of assets connected to the RTU.	5	2	2	20
Power Supply Failure	RTU power supply fails. Effect: Loss of monitoring and control of assets connected to the RTU.	6	2	2	24
RTU Software Failure	Errors in the programming or configuration of the RTU 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; incorrect monitoring of inputs, maloperation of outputs, loss of communications function.	5	2	3	30
Cyber Security Intrusion	RTU is rendered inoperable due to cyber security intrusion or malicious maloperation	7	1	3	21

	is initiated. 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 RTU.				
Accident	RTU is rendered inoperable due to accidents such as fire. Effect: Loss of monitoring and control of assets connected to the RTU.	7	2	1	14

Table 7: Common Modes of Failure for Distribution RTU Assets

4.1.3.1 Deterioration Drivers

There is a small fleet of MD3311 distribution substation RTUs in service. These were the first DNP3 RTUs to be deployed in the Evoenergy electricity network. The devices are beginning to become more unreliable with more frequent hardware issues. As the devices are now end-of-life there are plans in place to replace them in the distribution substations.

Distribution substation RTUs are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Primary systems faults causing voltage excursions above ratings on RTU I/O modules.

4.1.4 Zone Sub RTU

Table 8 summarises the common modes of failure for Zone Sub RTU assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	RTU is rendered inoperable due to asset deterioration. Effect: Loss of monitoring and control of assets connected to the RTU.	8	3	2	48
CPU Module/Card Failure	RTU CPU module/card fails. Effect: Loss of monitoring and control of assets connected to the RTU.	8	2	2	32
I/O Module/Card Failure	RTU I/O module/card fails. Effect: Loss of monitoring and control of assets connected to the RTU through the failed I/O module/card.	6	2	3	36
I/O Wiring Failure	Wiring between RTU and I/O fails due to corrosion or breakage. Effect: Loss of monitoring and control of assets connected to the RTU through the failed I/O wiring.	6	2	3	36
Communications Port Failure	RTU communications port fails. Effect: Loss of monitoring and control of assets connected to the RTU.	6	2	2	24

Power Supply Failure	RTU power supply fails. Effect: Loss of monitoring and control of assets connected to the RTU.	8	2	2	32
RTU Software Failure	Errors in the programming or configuration of the RTU 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; incorrect monitoring of inputs, maloperation of outputs, loss of communications function.	6	2	3	36
Cyber Security Intrusion	RTU is rendered inoperable due to cyber security intrusion or malicious maloperation is initiated. 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 RTU.	8	2	3	48
Accident	RTU is rendered inoperable due to accidents such as fire. Effect: Loss of monitoring and control of assets connected to the RTU.	8	2	1	16

Table 8: Common Modes of Failure for Zone Sub RTU Assets

4.1.4.1 Deterioration Drivers

A number of SCADA RTUs deployed in zone substations (Belconnen and Latham) are nearing or have passed their serviceable life. These devices are beginning to become more unreliable with more frequent hardware issues. These ageing devices are now classified as obsolete by the supplier and spare parts are becoming increasingly difficult to source. Replacement of this equipment is becoming extremely critical as the original suppliers of some equipment no longer provide any support, and with no alternative supplier available these units are becoming unmaintainable and unrepairable. RTU replacement projects are in place for the affected zone substations. Belconnen RTU will be replaced prior to the 2019-2024 Regulatory Period, and Latham substation RTUs will be replaced during the 2019-2024 Regulatory Period with Causeway RTU proposed to be decommissioned.

Zone substation RTUs are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Primary systems faults causing voltage excursions above ratings on RTU I/O modules.

4.1.5 Distribution Network Monitor

Table 9 summarises the common modes of failure for distribution network monitor assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	Distribution network monitor is rendered inoperable due to asset deterioration. Effect: Loss of monitoring of assets	5	2	4	40

	connected to the distribution network monitor.				
CPU Module Failure	Distribution network monitor CPU module fails. Effect: Loss of monitoring of assets connected to the distribution network monitor.	5	2	3	30
I/O Module Failure	Distribution network monitor I/O module fails. Effect: Loss of monitoring of assets connected to the distribution network monitor.	4	2	4	32
I/O Wiring Failure	Wiring between distribution network monitor and I/O fails due to corrosion or breakage. Effect: Loss of monitoring of assets connected to the distribution network monitor through the failed I/O wiring.	4	2	4	32
Communications Port Failure	Distribution network monitor communications port fails. Effect: Loss of monitoring of assets connected to the distribution network monitor.	4	2	4	32
Power Supply Failure	Distribution network monitor power supply fails. Effect: Loss of monitoring of assets connected to the distribution network monitor.	5	2	3	30
Software Failure	Errors in the programming or configuration of the distribution network monitor 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; incorrect monitoring of inputs, loss of communications function.	4	2	4	32
Cyber Security Intrusion	Distribution network monitor 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, loss of communications function.	5	1	5	25
Accident	Distribution network monitor is rendered inoperable due to accidents such as fire. Effect: Loss of monitoring of assets connected to the distribution network monitor.	5	2	1	10

Table 9: Common Modes of Failure for Distribution Network Monitor Assets

4.1.5.1 Deterioration Drivers

Distribution network monitors are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Primary systems faults causing voltage excursions above ratings on distribution network monitor input modules.

4.1.6 Fault Current Indicator

Table 10 summarises the common modes of failure for Fault Current Indicator assets.

Failure Mode	Description	Severity	Occurrence	Detection	RPN
Physical Mortality	Fault Current Indicator is rendered inoperable due to asset deterioration. Effect: Loss of monitoring of a distribution network power line.	5	3	5	75
Concentrator Module Failure	Fault Current Indicator concentrator module fails. Effect: Loss of monitoring of up to twelve distribution network power lines.	5	3	5	75
Communications Port Failure	Fault Current Indicator communications port fails. Effect: Loss of monitoring of a distribution network power line.	4	3	5	60
Power Supply Failure	Fault Current Indicator power supply fails. Effect: Loss of monitoring of a distribution network power line.	5	3	5	75
Cyber Security Intrusion	Fault Current Indicator 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, loss of communications function.	5	2	5	50
Accident	Fault Current Indicator is rendered inoperable due to accidents such as fire. Effect: Loss of monitoring of a distribution network power line.	8	2	5	80

Table 10: Common Modes of Failure for Fault Current Indicator Assets

4.1.6.1 Deterioration Drivers

Fault Current Indicators are subject to damage from external influences, including:

- Direct or indirect effects of lightning/storms,
- Ingress of dust, dirt, water or corrosive materials, and
- Primary systems faults causing excursions above ratings on Fault Current Indicator inputs.

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 Capacity and Capability

The upgrade of existing SCADA technology at zone substations and distribution substations currently being undertaken as SCADA RTU upgrade CAPEX projects will standardise, modify and significantly increase SCADA real-time data, providing the capacity to more accurately capture, record and report real-time asset performance, network events and supply data.

4.2.2 Utilisation

An effective SCADA system enables more rapid fault analysis and supply restoration, thereby minimising lost energy consumption and revenue. In terms of functional requirements and processing usage, SCADA assets are utilised to 100% of their capacity, and there is little or no inbuilt redundancy.

4.3 Risk and Criticality

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

4.3.1 Asset Criticality

The SCADA assets are considered critical for the reliable and safe operation of the network for the following reasons:

- The availability of a modern and reliable SCADA system enables more rapid and accurate identification of system faults, and more rapid restoration of supply
- A modern SCADA system will also enable real time monitoring of system status and network element loads, which will in turn enable dynamic ratings to be applied
- Without monitoring and control, system operations and automated distribution functions will not be possible
- The loss of continuous, real-time monitoring and control puts people at risk
- 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
- Without SCADA, Evoenergy would not be able to continuously monitor parameters and collect data for compliance reporting
- The SCADA system is a key component of the ADMS, gathering critical real-time data which enables power flow analyses for smarter operational decisions.

4.3.2 Geographical Criticality

Geographical criticality is not applicable for this asset class.

4.3.3 Asset Reliability

SCADA monitoring at zone substations and HV switching stations is critical to the effective operation and control of the distribution network. Very high levels of service reliability are demanded from SCADA.

In general, all SCADA issues are directed to the Secondary Systems section in the first instance. The SCADA team will then identify the systems at fault and perform/coordinate system restoration. SCADA/ADMS issues will generally require assistance from Schneider Electric while communications issues will require investigation and assistance from BSD (Business Systems Division). A significant failure or loss of the Fyshwick facility will require activation of the DRF (Disaster Recovery Facility).

The SCADA network has little redundancy and limited spares for legacy equipment and as such there is little that can be pre-planned for restoration when a non-redundant system fails. Generally if a non-redundant system fails, the net effects of that failure will remain until the network and/or equipment can be repaired or replaced. Spares are readily available for monitoring sites that have been upgraded in recent years, and equipment that is proven to be faulty can be readily replaced within a relatively short time frame.

In terms of statistics, the reliability of SCADA in the Evoenergy distribution network is approximately 99%, with current RTU upgrade projects underway to achieve the minimum acceptable availability of 99.5%.

Where installed the SCADA system is used to monitor substations 24 hours a day for 365 days per year. The availability of the SCADA system is:

- SCADA/ADMS system availability of between 99.95% and 99.99% over 12 months
- Individual equipment item availability of between 99.5% and 99.8% over 12 months.

Zone substation SCADA issues are to be identified immediately, reported and investigated within 4 hours. Distribution substation SCADA issues are to be identified immediately, reported and investigated within 24 hours.

4.3.4 Risk Assessment

The consequence of losing availability of SCADA would result in loss of data and control for operating the power system. This would have a significant impact on power system reliability and the ability to effectively manage network outages.

As a direct consequence, Evoenergy would investigate and assess the levels of damage and risk, and take the appropriate actions in response. Depending on the severity of the SCADA system disruptions, actions may include reactive repair of SCADA assets and/or postponement of maintenance and reactive works.

If the situation is more deleterious and/or disastrous such as a successful cyber security attack, Evoenergy may require activation of the Electricity Networks, Emergency Management Plan.

5 Asset Management Strategy Options

This section discusses asset class strategies to manage SCADA 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 SCADA 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 11.

		Inherent Risk				
Likelihood	Almost Certain					
	Likely	Low 5	Medium 2	High 4		
	Possible	Low 1	Medium 7	Medium 8	High 5	
	Unlikely	Low 9	Low 6	Medium 9	Medium 4	
	Rare					
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 11: Qualitative Risk Assessment – Option 0

5.1.1.3 Option Assessment

Whilst the run to fail option provides economic benefits in terms of avoided OPEX and CAPEX expenditures, the 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 three-yearly maintenance and a like for like replacement of SCADA assets at their end of life.

5.1.2.1 Description

For Evoenergy SCADA assets, the current program of three-yearly inspections would be retained. This process will ensure high availability of the SCADA assets. Assets are upgraded based on their age.

5.1.2.2 Risk

Retaining the current expenditure level for replacing SCADA 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 large 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 12.

		Option 1 Risk				
Likelihood	Almost Certain					
	Likely					
	Possible	Low 1				
	Unlikely	Low 26	Low 8	Medium 22	Medium 3	
	Rare					
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 12: 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 SCADA 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 SCADA 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 SCADA asset type and selects the most optimal strategy for maintenance. Where existing assets are not capable of providing functionality, or where technology advances render existing assets obsolete, strategic replacement prior to asset end of life is recommended. A greater penetration of SCADA assets into the distribution network is also pursued as a strategic response to the changing nature of the electrical distribution landscape.

5.1.3.1 Description

This strategy option reduces the OPEX costs compared to the existing asset class strategy by optimising maintenance intervals. It also pursues a balanced CAPEX investment in distribution network SCADA assets to allow monitoring and management of power quality on the LV side of the distribution network, where the greatest effects of disruptive technologies such as grid-connected photovoltaic generation and battery storage will be felt.

This strategy includes the following tasks:

- Strategic execution of RTU upgrade by combining with 11kV feeder protection upgrades. This approach results in combining design engineering for control and protection at the same time.
- Combined testing and commissioning of protection and SCADA functions, resulting in time and cost savings
- Perform 6 monthly maintenance for zone substation HMIs and RTUs
- Retain current maintenance intervals of 3 years for all other SCADA devices, and align SCADA maintenance at critical sites such as zone substations with communications equipment inspection every 12 months

5.1.3.2 Risk

Setting the expenditure at this level for critical SCADA infrastructure will ensure that SCADA/ADMS 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 SCADA 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 13.

		Option 2 Risk				
Likelihood	Almost Certain					
	Likely					
	Possible					
	Unlikely	Low 19	Low 11	Medium 18	Medium 3	
	Rare	Low 8				
		Negligible	Minor	Moderate	Major	Severe
		Consequence				

Table 13: Qualitative Risk Assessment – Option 2

5.1.3.3 Option Assessment

This option is recommended, as the level of risk exposure is alleviated through additional CAPEX investment to augment LV distribution network SCADA assets. The rapid encroachment of disruptive technologies has changed the focus of strategic investment in the monitoring and control of the electricity network. Option 2, with its emphasis on preventative maintenance and strategic upgrades to capability minimises the risks and enhances monitoring and control of the network. By strategically upgrading the SCADA capabilities, cost is spread over a longer period and the reliability and life of the devices is enhanced, resulting in lower operational costs over the life of the devices.

The following advantages are realised by Option 2:

- Combined execution of SCADA and protection testing and commissioning, leading to efficient SCADA testing
- RTU assets are renewed earlier, thus extending their life
- Newer features and capabilities of products can be utilised
- Updated RTU software versions reduces vulnerability to cyber threats
- Alignment with vendor product roadmaps for future and extended product support
- Bringing forward RTU upgrades results in smoother project execution, in contrast to upgrading all RTUs at once, resulting in inability to deliver due to competing priorities.

5.2 Option Evaluation

In order to assess the most optimal SCADA asset management strategy, a condition and Risk-Cost based modelling approach has been conducted using the RIVA Asset Management modelling tool 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 14.

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 14: 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 15: Scoring Matrix

5.3 Recommended Option

A risk condition based approach has been adopted to determine the most 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 risk mitigation, strategic alignment and compliance with regulatory requirements in section 5.2, and based on the risk management approach adopted to deliver a viable SCADA 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.

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

- Allowance 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 SCADA assets for the recommended asset maintenance strategy.

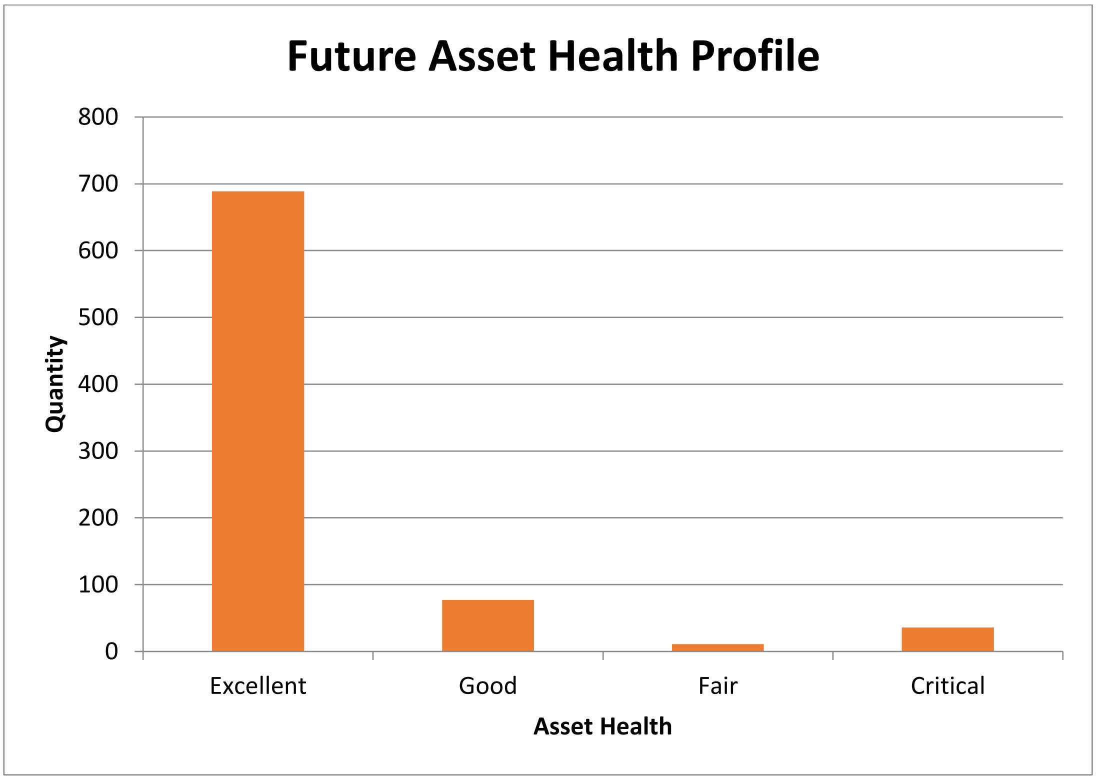

Figure 4: Asset Future Health Profile – SCADA Assets

6 Implementation

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

6.1 Network Augmentation and Infrastructure Development

The following initiatives have been adopted and supported by the Secondary Systems section via CAPEX projects to realise SCADA rationalisation opportunities:

- Improve SCADA availability, reliability and data accuracy by implementing control equipment replacement programs:
  - Zone substation SCADA RTU upgrade projects
  - Legacy distribution substation SCADA RTU upgrade projects
  - Customer indoor chamber substation SCADA RTU installations (customer initiated projects)
- Support compliance with regulatory requirements by reducing network outage duration and response times of the electricity network as well as providing appropriate operational reporting data.

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 SCADA 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 Asset Maintenance Plan

The objective of this maintenance plan is to economically achieve the longest possible reliable working life of SCADA assets. This is done through 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)
- Historic performance
- Equipment manuals
- Continuous review of asset performance and fine-tuning of maintenance triggers.

Asset Type	Maintenance Task	Maintenance Trigger
Zone substation HMI	Condition Assessment	6 months
Zone substation RTU	Condition Assessment	6 months
Zone substation GPS	Condition Assessment	3 years
Distribution substation RTU	Condition Assessment	3 years
Distribution network monitor	Condition Assessment	3 years
Fault Current Indicator	Condition Assessment	3 years

Table 16: SCADA Asset Maintenance Interval Summary

6.3.2 Condition Monitoring

Condition monitoring is not applicable for this asset class.

6.3.3 Preventative Maintenance

Critical SCADA equipment in the zone substations will be inspected on a six-monthly basis. The items to be inspected are the HMIs and the RTUs in each location. The six monthly inspections will include checking of the logs for each device to verify performance over the previous period.

The six monthly maintenance activities at these critical sites will include testing of batteries and DC systems, inspection of equipment, cleaning of hardware (fans, filters and heatsinks), configuration backups and firmware upgrades.

6.3.4 Corrective Maintenance

Defects detected during inspection or maintenance activities are recorded by the asset defects process and prioritised for repair by their severity.

Reactive repairs are carried out when faults occur and are prioritised for repair in line with network operational requirements.

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)
- Safety risk (inherent fault in a type of equipment)
- Suitability of ratings
- Strategic replacement – when a significant work program is occurring on an asset, it may be opportune to align a planned SCADA 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 SCADA work may be brought forward or held back to align with the planned outages.

The decision to replace or refurbish SCADA 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. The following options are being considered with the planned asset maintenance (renewal) projects:

- Implementation of new distribution substation SCADA architecture and RTU technology with low cost and low maintenance RTUs, with augmentation projects and distribution substation RTU renewals.

6.4.1.1 Refurbishment

For the SCADA 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 SCADA 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 SCADA technology becoming obsolete, or no longer usable. The proposed nominal lifespan of SCADA assets varies between 7 and 15 years, depending on the asset type. This is determined by the duration the assets continue to achieve reliability requirements or the duration the assets remain supported by the vendor. Given these nominal life spans however, assets can evolve or transition to the next generation because of changing requirements (e.g. regulatory) or improvements to technology. As such, asset plans should continually evolve with the assets 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 an asset occurs when:

- The current asset 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 asset; 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.

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

SCADA 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* document.

6.6 Associated Asset Management Plans

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

- Secondary Systems Zone Substation Protection ASP
- Secondary Systems Distribution Substation Protection ASP
- Secondary Systems Communications 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 planned and unplanned maintenance.

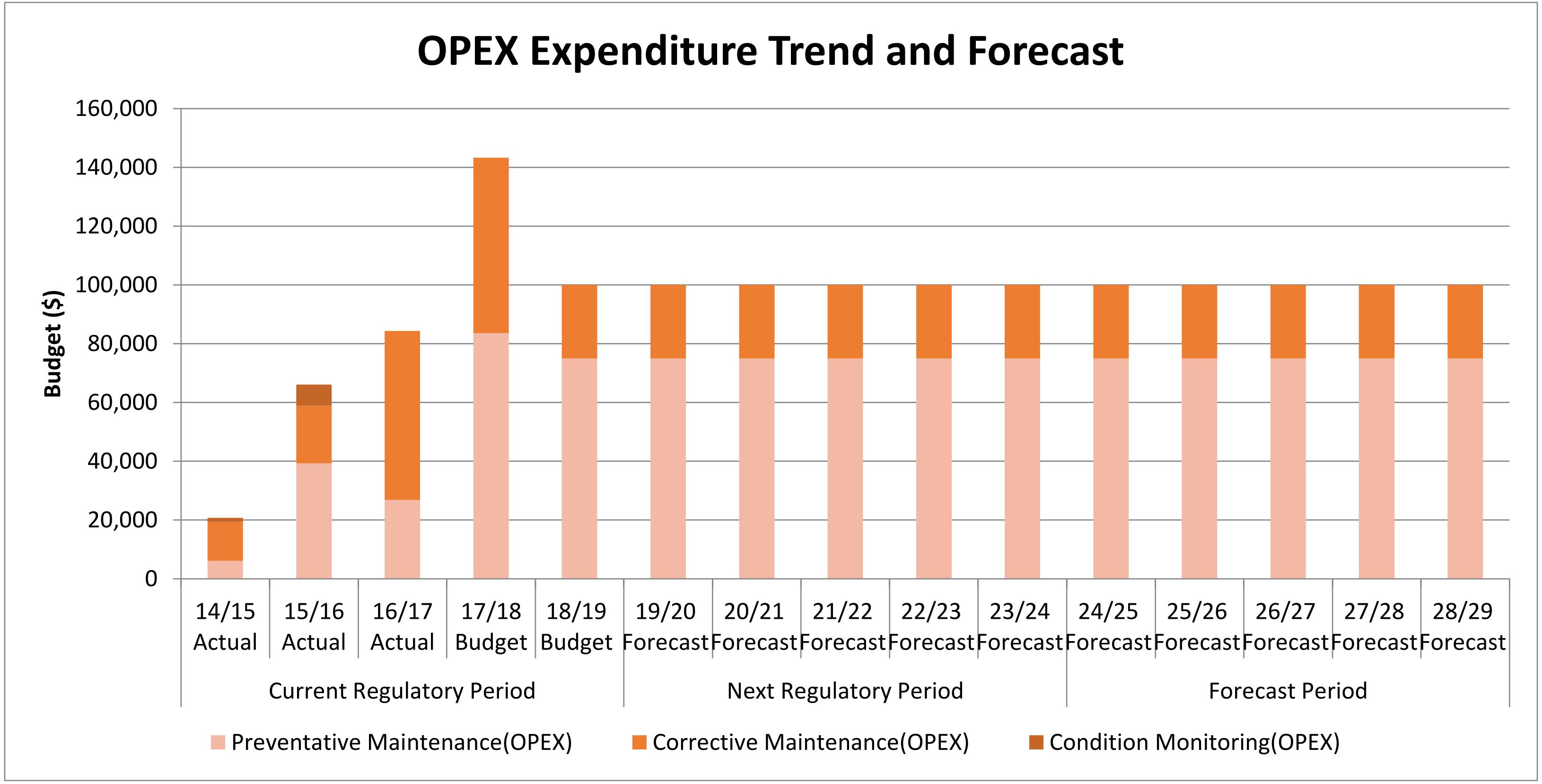

Figure 5: OPEX for Maintenance Program of SCADA Assets

Program	Secondary Systems SCADA Maintenance
2019-24 Budget	Annual budget for SCADA asset maintenance: **$100,000**
Scope	This program includes: Planned and unplanned maintenance
Project(s) Details	**SCADA Maintenance** The following maintenance activities are to be undertaken for zone substation SCADA assets on a six-monthly basis: Zone substation HMI condition assessment Zone substation RTU condition assessment The following maintenance activities are to be undertaken for SCADA assets on a three-yearly basis: Zone substation GPS condition assessment Distribution substation RTU condition assessment Distribution network monitor condition assessment Fault Current Indicator condition assessment
Risks and Opportunities	SCADA condition assessment and maintenance allows the identification and rectification of issues in SCADA assets before failure occurs and saves the business any potential loss of revenue and reputational risks due to failure to clear the faults.
	The strategy for optimised maintenance is based on the revised maintenance strategy of alignment with primary systems assets.

Table 17: Secondary OPEX SCADA Maintenance Program

7.2 Capital Program

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

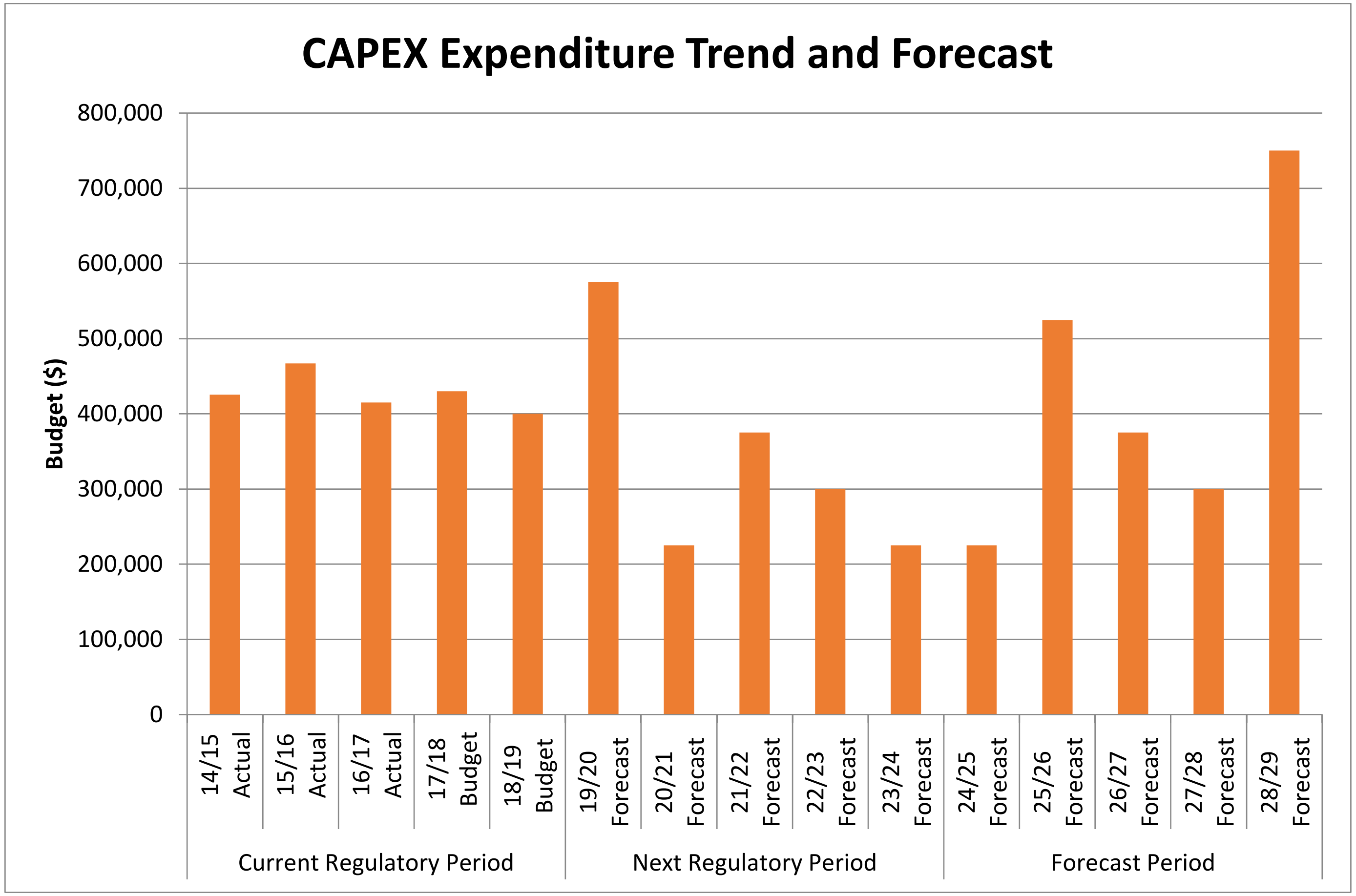

Figure 6: CAPEX Program for SCADA Assets

S. No	Project Title	Proposed Budget	Nominated Year
1	Chamber distribution substation SCADA installation	$150,000	2019-2020
2	Latham Zone substation HMI replacement	$75,000	2019-2020
3	Wanniassa Zone substation HMI replacement	$75,000	2019-2020
4	Zone Substation RTU Replacement (Latham, Wanniassa, City East and includes 3 GPS Replacement)	$275,000	2019-2020
5	Chamber distribution substation SCADA installation	$150,000	2020-2021
6	Gilmore Zone substation HMI replacement	$75,000	2020-2021
7	Chamber distribution substation SCADA installation	$150,000	2021-2022
8	Woden Zone substation RTU replacement (including GPS)	$150,000	2021-2022
9	Telopea Zone substation HMI replacement	$75,000	2021-2022
10	Chamber distribution substation SCADA installation	$150,000	2022-2023
11	Moss Zone substation RTU replacement (including GPS)	$75,000	2020-2023
12	Moss Zone substation HMI replacement	$75,000	2022-2023
13	Chamber distribution substation SCADA installation	$150,000	2023-2024
14	Theodore Zone substation HMI replacement	$75,000	2023-2024
15	Chamber distribution substation SCADA installation	$150,000	2024-2025
16	Chamber distribution substation SCADA installation	$150,000	2025-2026
17	Zone Substation RTU Replacement (Theodore, Gilmore, Civic, Eastlake and includes 4 GPS Replacement)	$300,000	2025-2026
18	Gold Creek Zone substation HMI replacement	$75,000	2025-2026
19	Chamber distribution substation SCADA installation	$150,000	2026-2027
20	Zone Substation RTU Replacement (includes 2 GPS)	$150,000	2026-2027
21	Chamber distribution substation SCADA installation	$150,000	2028-2029
22	Zone Substation RTU Replacement (includes GPS)	$75,000	2028-2029

23	Zone substation HMI replacement	$75,000	2028-2029
24	Chamber distribution substation SCADA installation	$150,000	2027-2028
25	Zone Substation RTU Replacement (includes GPS)	$150,000	2027-2028
26	Zone substation HMI replacement	$150,000	2027-2028
27			

Table 18: Secondary Systems CAPEX SCADA 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 (Replacement Program)	**575,000**	**225,000**	**375,000**	**300,000**	**225,000**	**225,000**	**525,000**	**375,000**	**300,000**	**450,000**
OPEX	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**	**100,000**
Planned Maintenance (OPEX)	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000	75,000
Unplanned Maintenance (OPEX)	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000	25,000

Table 19: CAPEX & OPEX 10 Year Budget Forecast

The replacement projects have been confirmed through a Project Justification Report where applicable.

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 have been estimated in Riva using recent actual cost data.

A.1.1 Planned Maintenance Tasks

Unit Costs			
Asset Type	**Task**	**Cost Basis**	**Unit Cost**
SCADA	SCADA power supply and UPS functional validation. System visual inspection of all related hardware, devices, cables, cabinet	Planned Maintenance for ZS SCADA installations	$50,000

Table 20: Planned Maintenance Task Unit Costs

A.1.2 Condition Monitoring Tasks

None for this asset class.

A.1.3 Reactive Maintenance Tasks

Unit Costs			
Asset Type	**Task**	**Cost Basis**	**Unit Cost**
SCADA	SCADA legacy upgrade	SCADA upgrade	$250,000
SCADA	SCADA reactive fault repairing and bug fixing in order to achieve designed overall system availability & reliability	SCADA Site Reactive Unplanned Maintenance (Faults & Repairs)	$50,000
SCADA Component	Replacement cost	SCADA replacement	$20,000

Table 21: Reactive Maintenance Task 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