



31 January 2023

Attachment 5.8.c: Control system core refresh program

Ausgrid's 2024-29 Regulatory Proposal

Empowering communities for a resilient, affordable and net-zero future.



Table of Contents

1. Executive summary.....	4
2. CONTEXT.....	6
2.1. Background.....	6
2.1. Problem/opportunity.....	7
2.2. Compliance obligations.....	9
2.3. Risk appetite.....	12
2.4. Management approach for OT infrastructure.....	12
2.5. Control System Core Refresh Program.....	13
2.6. Investment objectives.....	13
2.7. Customer outcomes.....	14
3. OPTIONS.....	16
3.1. OVERVIEW OF OPTIONS.....	16
3.2. OPTION 1: EXTENDED INFRASTRUCTURE LIFE.....	17
3.2.1. Description.....	17
3.2.2. Option 1 Assumptions.....	17
3.2.3. NPV analysis.....	18
3.3. OPTION 2: BALANCED RISK BASED REPLACEMENT.....	19
3.3.1. Description.....	19
3.3.2. Option 2 Assumptions.....	19
3.3.3. NPV analysis.....	20
3.4. OPTION 3: INCREASED PROACTIVE REPLACEMENT.....	21
3.4.1. Description.....	21
3.4.2. Option 3 Assumptions.....	21
3.4.3. NPV analysis.....	22
4. RECOMMENDATION.....	23
4.1. Recommended solution.....	23
Recommended Solution.....	23
4.2. Alignment to strategy.....	23
4.3. Program delivery risks.....	23
4.4. Program assumptions.....	24
4.5. Program dependencies.....	25
4.6. Business area impacts.....	25
APPENDIX A – PROPOSED CONTROL SYSTEM REFRESH PROJECTS.....	26

APPENDIX B – APPROACH TO QUANTIFICATION OF PROJECT BENEFITS	27
APPENDIX C – INDUSTRY BEST PRACTICE FOR OPERATIONAL TECHNOLOGY	28
APPENDIX D – BEST PRACTICE IN OT – REFERENCE STANDARDS	34

1. Executive summary

“Operational Technology” (OT) is the term used to describe hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events¹. At Ausgrid this makes up the majority of the hardware and software used to monitor and manage the electricity network in real-time.

The control system is the foundational element of the Ausgrid’s OT. This system resides within the core security zone of the OT system and directly manages the monitoring and control of the electricity network.

This program justification describes the investments necessary to maintain the ongoing and reliable operation of the control system. It describes the necessary investments in hardware and software to maintain an operational and highly available system. The key investments are developed to manage the end-of-life replacement of the dedicated control system components. These replacements are triggered by failure or lack of ongoing vendor support (lack of availability of replacement parts and software or firmware updates to maintain availability or security).

Consistent with other OT investments, we identify the most efficient means of delivering this capability, with the highest net present value (NPV), as our proposed approach. The table below provides a summary of the Control System Core Refresh program as discussed in this program justification. It demonstrates that the program of work, if approved, would continue to maintain Ausgrid’s network operational capability and deliver net benefits of \$13.0 million, against an option to provide only replacement of software or hardware following failure.

Executive summary	
Key Objective(s) of the program	<p>The purpose of the Control System Core Refresh program for the 2024-29 regulatory control period is to maintain Ausgrid’s Operational Technology resilience and to maintain a secure and supportable environment against equipment failures and known vulnerabilities.</p> <p>This program will also enable Ausgrid to maintain industry best practice for operational technology as required in its Electricity Distribution Licence Conditions, and will meet Ausgrid’s risk appetite with respect to network operation, cyber risks and resiliency of OT systems [REDACTED].</p> <p>To achieve this objective the majority of hardware and software will be replaced prior to failure which would impact the efficient operation of the electricity network. This includes implementation of a range of ‘best practice’ design architecture and technology controls specific to the utilities industry to maintain resilience to component failures.</p>
Customer benefits	<ul style="list-style-type: none"> Adapt Ausgrid’s Operational Technology environment, including its control system so that it is current and secure for the critical role in distributing energy to customers and is capable of safely facilitating energy flows in the future energy mix while providing customers with greater choice and control of their energy use. Reducing the risk of significant disruption to critical infrastructure due to cyber security related network outages/interference, ensuring the safe and secure operation and control of Ausgrid’s electricity network, consistent with the national electricity objective (NEO), which requires Ausgrid to maintain the security of both the supply of electricity and the distribution network. Reduced risk (reduced frequency and recovery time from equipment failure events) of supply loss to customers and economic impacts from loss of energy supply to customers

¹ <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>

	following an equipment failure where the electricity network cannot be monitored and controlled to avoid foreseeable events.						
Regulatory requirements	<ul style="list-style-type: none"> Ausgrid's Distribution Network Service Provider (DNSP) Ministerially Imposed Licence Conditions – Clause 9 & 10 – Critical Infrastructure. National Electricity Rules Section 4.3.4(c) – articulates the requirement for secure and available systems in order to support responding to an Australian Energy Market Operator (AEMO) direction. Security of Critical Infrastructure Act 2018, Security Legislation Amendments 2021 and 2022 Electricity Supply Act 1995 (NSW) Privacy Act 1988 						
NPV calculations	This program results in a net economic benefit of \$13.0 millions, largely driven by probabilistic benefits associated with reduced likelihood of unserved energy from failure of the core control system by component failure or a malicious cyber-attack on the OT environment from a fully maintained and vendor supported OT environment.						
Expenditure forecast	(\$m)	FY25	FY26	FY27	FY28	FY29	Total
Direct only	CAPEX	\$1.73	\$1.34	\$2.95	\$4.99	\$2.37	\$13.37
(FY24 Real \$)	OPEX	-	-	-	-	-	-
	Total	\$1.73	\$1.34	\$2.95	\$4.99	\$2.37	\$13.37

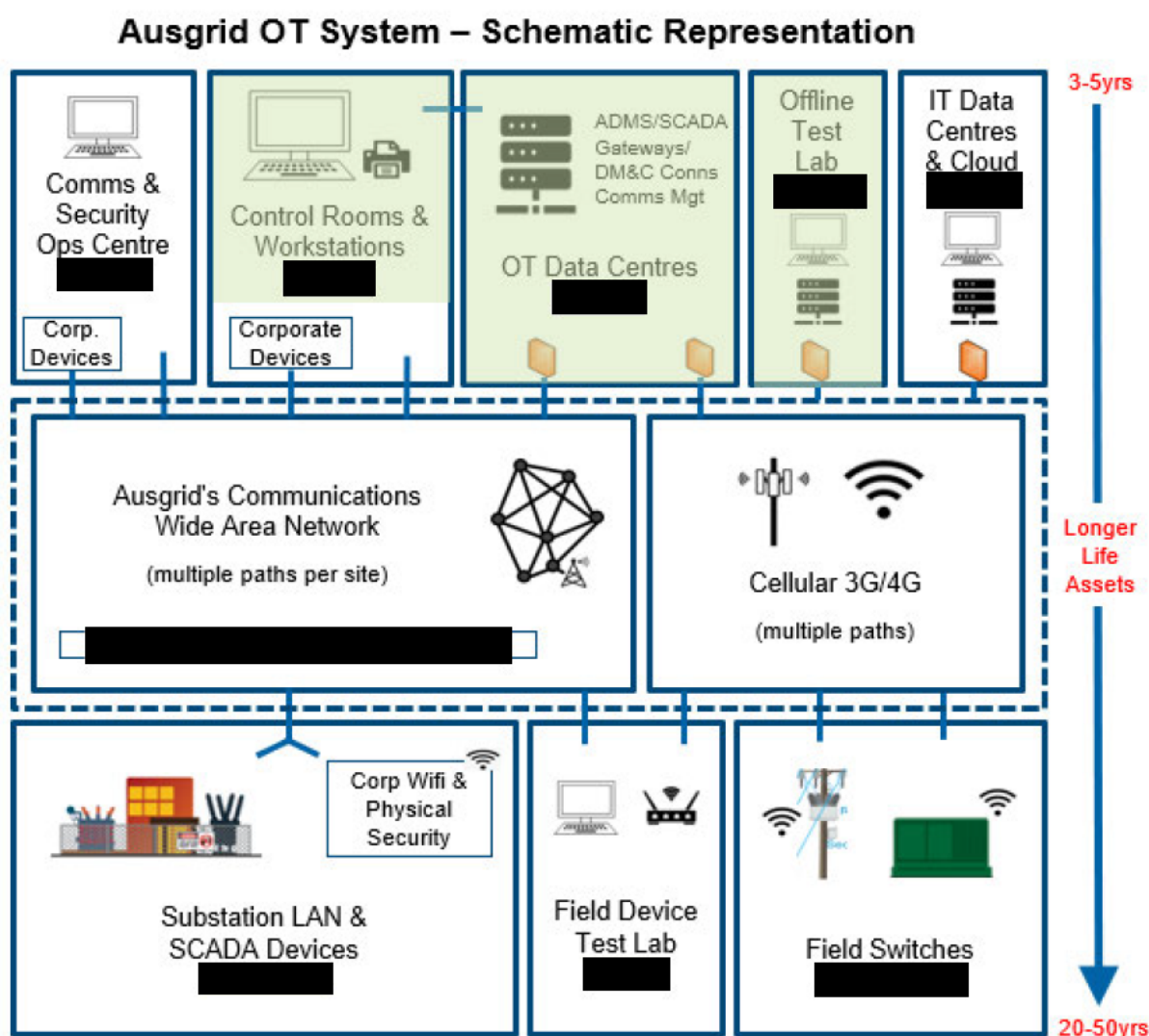
2. CONTEXT

2.1. Background

This document outlines the case for investment to maintain the reliable operation of Ausgrid's control system and Operational Technology environment using asset lifecycle management techniques. The investment in hardware and software to maintain an operational and highly available resilient control system.

Ausgrid's control system is the core of the OT system (highlighted in **Figure 1** below) and is used to monitor and control the flow of electricity by operating network switches and intelligent devices across the grid. The OT system includes large numbers of long-lived field devices, connected to our control centres via wide-area communications networks. The field devices and communications networks are complex and expensive to replace due to their distributed nature and direct impacts on supplying energy to customers during replacement.

Figure 1 Schematic Representation of Ausgrid's OT System



This Control System Core Refresh program will replace key hardware and software at end of life to continue Ausgrid's maintenance of industry best practice as required in its Electricity Distribution Licence Conditions to maintain a highly available control system for operation of the electricity network,

and regulatory obligations, and will meet Ausgrid's risk appetite with respect to resiliency of OT systems [REDACTED].

To achieve these objective, key technologies will be replaced following failure or at forecast end of life. This approach also achieves the greatest NPV for customers. The range of strategies to manage this type of infrastructure is specific to the utilities industry where the control system is required to operate 24 hours a day, 7 days a week with an availability of 99.999% of the time.

The core of the control system consists of the following key elements:

- Infrastructure for operating the Advanced Distribution Management System (**ADMS**) and related applications ([REDACTED]);
- Infrastructure for managing the communications network ([REDACTED]);
- Infrastructure for managing emergency remote access for vendor support ([REDACTED]);
- Infrastructure for operating the offline test environment for testing ([REDACTED]);
- Workstations to access the control system ([REDACTED]);
- Supporting infrastructure for Control Room Operations; and
- Software applications for the control system functions, communication management and supporting functions.

The recurrent replacement of these key components at end of life is the basis of this program.

2.1. Problem/opportunity

Electricity is an integral part of all modern economies, supporting a range of critical services including health care, transportation, communications, banking and gas and water utilities. The secure supply of electricity is therefore of paramount importance as reflected in the National Electricity Rules, Electricity Distribution Licence Conditions and Security of Critical Infrastructure Act.

Digitalisation, emerging markets and increased business intelligence is rapidly transforming the energy system, bringing many benefits for businesses and consumers. One impact of this transformation is the requirement to integrate external systems with the control system in order to provide optimised use of distributed energy resources (**DER**) and greater benefit to customers. This increased connectivity (to the electricity grid, OT and information technology (**IT**) systems) and automation increases the likelihood of cyber-attacks and consequently cyber security risks. A successful attack could trigger the loss of control over devices and processes that control the electricity network. This will have the potential to cause physical damage and put at risk the safety of the community by way of service disruption or uncontrolled discharge of electricity.

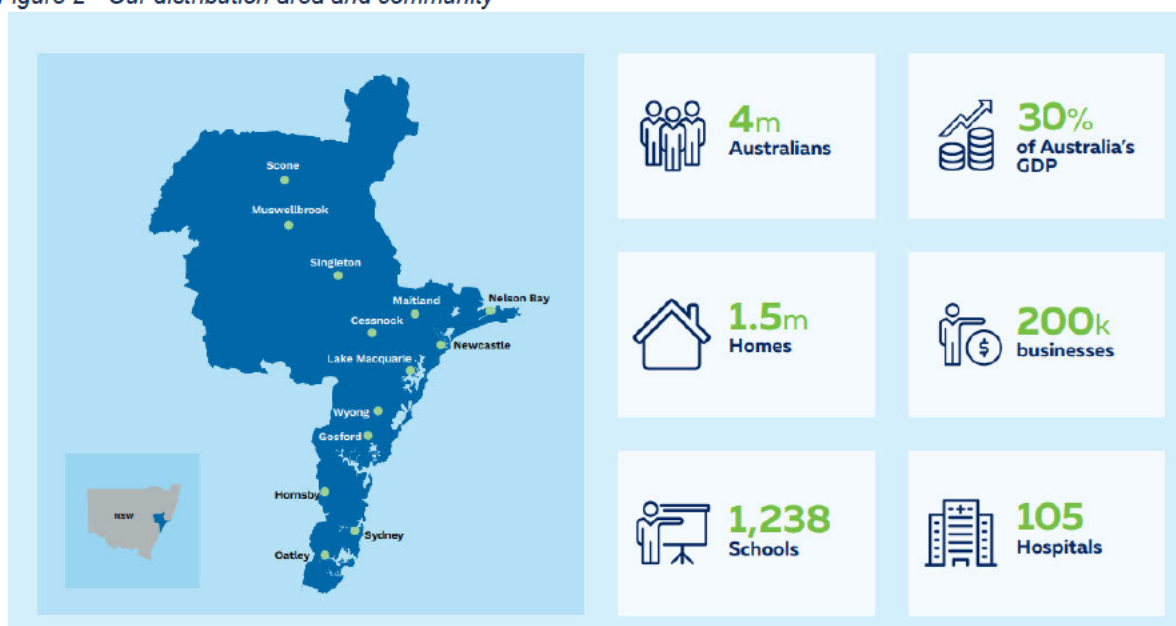
Our transformation into a Distributed Systems Operator (**DSO**) will result in further emerging challenges posed by connected devices, smart grids and Distributed Energy Resources (**DER**). Adopting innovative and secure technologies will be essential to realise the customer benefits presented by this opportunity.

Our network is critical to the national economy. If Ausgrid's ability to supply electricity safely and securely was destroyed, degraded or rendered unavailable for an extended period, it would significantly impact on the security, social or economic wellbeing of the State of New South Wales and Australia as it services the Sydney CBD and other critical infrastructure businesses which account for up to 30% of Australia's gross domestic product (**GDP**)².

Figure 2 below shows the geography serviced by Ausgrid and indicates the number of consumers, business and organisations potentially impacted by a control system failure for our distribution network.

² NSW Government, 'Sydney Facts', (online, 25 February 2022), <<https://invest.nsw.gov.au/why-nsw/sydney-facts>>.

Figure 2 - Our distribution area and community



Electricity distribution businesses rely on a number of key OT applications and systems to safely and efficiently manage the flow of electricity across the distribution network, and also perform an essential role in the day-to-day delivery of planned augmentation, maintenance and unplanned work resulting from events such as equipment faults, third party damage or natural hazards, such as storms. These applications and systems also facilitate inter-control room communication with external parties such as TransGrid and AEMO to maintain the security and stability of the national electricity grid.

These applications are integral to performing key network functions and are summarised below in terms of their functions in ensuring the distribution of electricity to Ausgrid's customers.

- Real-time monitoring of key network equipment;
- Real-time monitoring energy flows in the network;
- Real-time control (including switching and configuration change) of field devices;
- Real-time network status communication to AEMO and TransGrid;
- Controlled switching in response to faults to maintain continuity of supply;
- Managing planned and unplanned switching and network section shutdowns;
- Management of network model, SCADA points and temporary re-configuration;
- Energy flow and fault level analysis and advisory services;
- Geographic display of network and current state of operation;
- Event simulation, replay analysis and operator training;
- Operator control of field devices; and
- Provision of event and monitoring history and analysis.

Ausgrid's control system environment consists of field devices, communications and control systems. These control systems are driven and managed by software that resides on hardware provided by a system of centralised compute and storage servers, operator workstations and network equipment such as routers, switches and firewalls and other associated supporting equipment that comprise the core control system.

Ausgrid's core control system software application was recently replaced with a modern ADMS. The ADMS provides a core control system application that is also used by a number of Australian and a large number of electricity utilities internationally. The implementation of this application, commencing

in 2019 required the replacement of key components of the control system infrastructure. This infrastructure requires replacement to maintain currency like all modern computing systems upon failure or at end of life. End of life is largely driven by supportability constraints (e.g. sourcing replacement components) including cyber vulnerability management and system performance.

This program covers recurring expenditure for replacement at end of life for system components, such as servers, operator workstations and network equipment which comprise the core control system. End of life is forecast based on risk assessments that consider end of life failure or supportability/maintainability factors (including vendor support), or additional functionality requirements to meet core regulated business needs.

This program forecasts recurrent expenditure considering the age of the infrastructure and vendor support availability. During the 2019-24 period the replacement of key infrastructure and related expenditure was largely included in the ADMS implementation program. This key infrastructure purchased, installed and made operational as a component of the ADMS program will reach end of life during the 2024-29 period and require replacement creating a peak of investment in FY28.

Ausgrid must use best industry practice for management of electricity network control systems, as required by critical infrastructure licence conditions, and ensure that operation and control of its distribution system, including all associated infrastructure, can only be accessed, operated and controlled from within Australia.

As part of applying industry best practice for a control system to meet this requirement, it is critical that supporting equipment that comprises the core control system is refreshed based on a risk-based assessment. This includes the management of equipment at end of life and technology obsolescence in conjunction with available vendor support arrangements to minimise unforeseen consequences. This includes maintaining servers and workstations on currently supported operating system and firmware version releases to support functionality and latest security patches for known cyber vulnerabilities.

2.2. Compliance obligations

We are required to meet the regulatory obligations as set out in **Table 1** below.

Table 1 – OT Compliance Obligations

Obligation	Description of Requirement
Ausgrid Electricity Distribution License Conditions	<p>License conditions³ are imposed under the <i>Electricity Supply Act 1995 (NSW)</i>. The key license conditions relevant to the management of our OT are:</p> <ul style="list-style-type: none"> Clause 9 requires us to use best industry practice for electricity network control systems to ensure that the distribution system, including all associated ICT infrastructure, can be accessed, operated, and controlled only from within Australia, and that it cannot be connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside of Australia; and Clause 10 requires us to ensure that information as to the operational technology (such as the SCADA system) and associated ICT infrastructure of the operational network and personal information is held solely within Australia and accessible only by us (as the license holder) or someone authorised by Ausgrid.

³ The Minister for Resources and Energy issues the DNSP licences. IPART administers compliance with the licence conditions on behalf of the Minister. Licence conditions for Ausgrid are available from IPART's website: <https://www.ipart.nsw.gov.au/Home/Industries/Energy/Energy-Networks-Safety-Reliability-and-Compliance/Electricity-networks/Licence-conditions-and-regulatory-instruments#:~:text=Operating%20licences%20apply%20to%20Ausgrid%2C%20Endeavour%20Energy%2C%20Essential,to%20be%20read%20in%20conjunction%20with%20...%20>

Obligation	Description of Requirement
	Keeping our systems and network current and secured against cyber threats is a key enabler to meet these licence conditions. How this obligation relates to OT is detailed in Appendix C & D.
Security of Critical Infrastructure Act 2018 (SOCI Act) Includes amendments in 2021 and 2022	<p>The SOCI Act outlines specific requirements for owners and operators of critical infrastructure assets. This legislation directs the Commonwealth to establish and maintain a critical infrastructure asset register. It is this register that provides the foundation with which to identify, understand and manage the national security risks of espionage, sabotage and coercion. It also seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.</p> <p>The Act applies to 22 asset classes across 11 sectors including the energy sector and requires us to comply with the following obligations:</p> <ul style="list-style-type: none"> • Critical Infrastructure Asset Register - As a critical infrastructure operator, we are to ensure the accuracy of asset information reported in the critical infrastructure register and provide annual reports to ensure the currency of the register. • Mandatory Reporting of Cyber Security Incidents - Subsequent amendments in December 2021 established requirements for mandatory reporting of cyber security incidents where there has been exploitation of our OT or IT systems.

Obligation	Description of Requirement
Australian Energy Sector Cyber Security Framework (AESCSF)	<p>Protecting Australia's energy sector from cyber threats is of national importance. These protections outlined in the AESCSF aim to maintain secure and reliable energy supplies thereby supporting our economic stability and national security. In order to ensure an ongoing uplift in cyber maturity and the assurance to our organisations function in the electricity industry, we are required to assess our performance against the AESCSF framework annually.</p> <p>In adopting the AESCSF framework across a range of industries within the energy sector, the Australian Government forecasts a consistent and measurable increase in cyber security and organisations capability aligned with an operator's criticality in the sector.</p>
National Electricity Law and National Electricity Rules	<p>The National Electricity Law (NEL)⁴ requires us to promote efficient investment in, and efficient operation and use of electricity services for the long-term interests of consumers of electricity with respect to price, quality, safety, reliability, and security of supply of electricity as per the National Electricity Objective (NEO).</p> <p>The operating and capital expenditure objectives⁵ set out in the National Electricity Rules (NER) require us to maintain both the quality, reliability, and security of supply of standard control services and the reliability and security of the distribution network.</p>
Privacy Act 1988 & Information Privacy Act 2014	<p>As specified in the <i>Privacy Act 1988</i> and the <i>Information Privacy Act 2014</i>, we are required to maintain strong controls and security on the accessibility of customer data as well as appropriate availability of that data. Having appropriate controls and cyber security systems in place is a key enabler to appropriately securing personal identifying information and reducing the risk of a data breach.</p>

The ongoing security and resilience of critical infrastructure is a shared responsibility of the Australian Government and the owners and operators of the critical assets. We are required to comply with Commonwealth and State legislation for the protection of assets recognised as critical infrastructure.



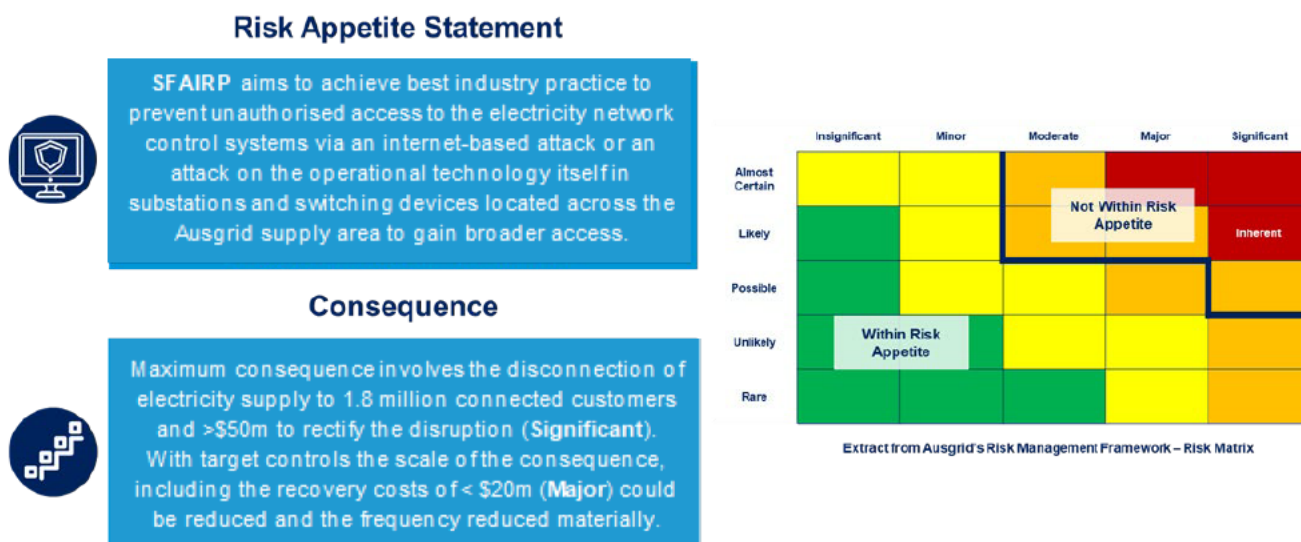
⁴ The NEL is set out in a schedule to the *National Electricity (South Australia) Act 1996*.

⁵ See clauses 6.5.6(a) and 6.5.7(a) of the NER.

2.3. Risk appetite

We are risk averse in the way that we aim to achieve best industry practice to prevent a significant interruption or loss of Operational Technology services to the operation and control of the electricity grid so far as is reasonably practical. Refer to **Figure 3** below.

Figure 3 - Ausgrid Risk statement, Risk Appetite and Risk Matrix



The proposed Control System Core Refresh program seeks to reduce the risk profile of our key OT reliability risks so that the likelihood of each of those risks falls to within our risk appetite. The key risks relate to the loss of supply of electricity to a small region of Ausgrid's supply area or to the total loss of supply of electricity to the whole supply area. These risks have consequences that are a major or significant classification respectively and the Control System Core Refresh program in combination with the OT Security program seek to maintain the likelihood to within appetite So Far As Is Reasonably Practical (**SFAIRP**).

The application of the SFAIRP approach to Control System investments is demonstrated through detailed cost benefit analysis supporting the options and recommended investments in this document.

2.4. Management approach for OT infrastructure

OT infrastructure management takes a risk-based approach to focus resources in a sustainable way on the most critical, unreliable and unsupported assets. Compensating controls are designed and introduced to mitigate where this cannot be reasonably achieved.

This program funds periodic critical infrastructure upgrades and refresh of Ausgrid's existing core control system compute and storage servers, operator workstations and network equipment such as routers, switches, firewalls.

Key risk mitigation strategies include:

- Replacement of failed equipment to maintain the control system in its designed state,
- Maintain software and firmware currency for key components of the Control System ensuring appropriate vendor support is availability,

- Hardware replacement to manage end-of-life components ensuring appropriate vendor support availability, and
- Maintenance of system architecture to meet current and future Industry Best Practice standards for Industrial Control Systems.


2.5. Control System Core Refresh Program

This program has been developed to maintain the control system environment including applications and systems SFAIRP. This approach will also continue to maintain and enhance Ausgrid's control system resilience and maintain compliance with NSW Distributors Licence, specifically the Critical Infrastructure Licence Conditions, and broader Commonwealth Government legislation and guidelines.

The Control System Core refresh program is recurrent expenditure to refresh the OT infrastructure supporting the core of the control system by replacing at end of life, including triggers of equipment failure or end of vendor support where software and firmware updates are no longer available to maintain critical security functionality.

It has also been developed in the context of Ausgrid's obligations to maintain the quality, reliability and security and maintain the safety of the distribution system through the supply of standard control services as required in the NER (6.5.7 (a) 3 & 4).

Ausgrid's control system environment consists of field devices, communications and control systems. These control systems are driven and managed by software that resides on hardware provided by a system of servers, operator workstations and network equipment such as routers, switches, firewalls and other associated supporting equipment that comprise the core control system.



As required by critical infrastructure licence conditions, Ausgrid must use best industry practice for management of electricity network control systems and ensure that operation and control of its distribution system, including all associated infrastructure, can only be accessed, operated and controlled from within Australia.

These core OT applications and systems that form the control system are integral to performing key network functions and ensuring the distribution of electricity to Ausgrid's customers. The core control system infrastructure need to be continually updated to ensure they accommodate new technology developments, manage threats and vulnerabilities, hardware failures and vendor end of support.

2.6. Investment objectives

This program is designed to achieve the following specific objectives:

- Maintain existing control system reliability, availability and capability,
- Mitigate assessed, known and emerging failure modes to the OT environment,
- Maintain compliance with existing regulatory obligations and security control obligations as the SOCI Act evolves,
- Maintain control design and effectiveness of implemented OT architectural controls,
- Develop the capability to securely integrate new technology into the network to drive efficiency in energy distribution over the long term,
- Modernise the OT security functionality to keep pace with and facilitate the adoption of new capabilities and technology,

- Improve the resilience of customer energy supply in the face of a changing external threat landscape and increasing societal dependency on electricity, and
- Deploy enabling technology, devices and systems to facilitate the resilient, safe and secure transition towards a less carbon intensive energy system including customer preferences to incorporate DER such as solar generation, electric vehicles and household batteries.

To achieve these objectives, the Control System Core Refresh Program comprises a range of investments which may evolve over time as technology matures. To manage the uncertainty associated with investment of this nature, Ausgrid will continue to prioritise the projects in line with our approach in the 2019-24 regulatory reset period.

We have not included an additional operational expenditure component for these works as the maintenance and support of the existing capabilities is included in current expenditure. We will continue to seek efficiencies to reduce this ongoing operational commitment.

To ensure the greatest economic value from the investments Ausgrid utilises quantitative risk assessment to assess options by measuring the expected risk reduction and comparing to the investment required prior to investing in each component of the program.

2.7. Customer outcomes

Through a co-design process with customer advocates, we identified six key topics that will define our business into the future. Of these, the Control System Core Refresh program is particularly aligned to Resilient theme in maintaining the safety and security of the network, also with a direct impact on Customer Experience and Value for Money.

Table 3 – Themes Identified to Define the Business into the Future

Theme	Overview
Fair	<ul style="list-style-type: none"> • Intergenerational equity • No one left behind, where practical
Sustainable	<ul style="list-style-type: none"> • Lowering Ausgrid's carbon footprint • Facilitating the transition to net zero by 2050
Future network	<ul style="list-style-type: none"> • Creating shared value in the community • Encouraging DER across different geographic and customer segments
Customer experience	<ul style="list-style-type: none"> • Digitalisation of services • Quality of service and bespoke experiences and outcomes
Resilient	<ul style="list-style-type: none"> • Respond to climate change and changing community needs • Maintain safety, reliability and network security
Value for money	<ul style="list-style-type: none"> • Unlock additional value while keeping bills stable • Benefits from investments exceed the costs which will be incurred

The proposed investment in Control System Core Refresh will deliver:

- Resilient outcomes for customers, by maintaining safety, reliability and network security,
- Maintain Customer Experience by reducing the risk of failure of the Control System resulting in network outages and disruptions to electricity supply, and
- Value for Money, with the expected benefits (i.e. reduced investment in replacing legacy electricity network technologies) being lower than alternatives require to maintain our regulatory obligations.

The benefits of this program are largely focused on maintaining business operations to maintain a safe and secure electricity supply to customers and avoid disruptions to customers from a failure of the operational technology systems of Ausgrid where the failure could disrupt or compromise the safe and reliable operation of the electricity network. The potential consequences are rarely experienced on Ausgrid's network and never at the potential of a full scale impact, therefore we must utilise the experiences of other Australian businesses and international electricity utilities to fully appreciate the

significant consequences on both the supply of electricity to consumers and also the economic impact to Australians.

These impacts are listed in the table below to better understand the detailed linkages between the impacts to customers and the investments within the Control System Core Refresh program.

Table 4 – Key Customer Benefits from the Control System Core Refresh program

Benefit	Overview
Avoid Large Scale Disruptions	Reduce exposure of the control system to unplanned failures resulting in outages to Ausgrid's Control System environment and slowing response times to supply interruption events.
Quicker Response to Disruptions	Rapid event response – Improvements to failure of components of the core control system by having current and available vendor support.
Improved Customer Safety	Rapid and remote network intervention – improve availability of the control system environment to detect and respond to electricity network failures
Efficient Customer Connections	Reduced complexity and cost – establishing pre-approved secure architecture methods of communicating between customer and electricity grid assets
Long Term Affordability	Modest and targeted investment – select investments in infrastructure to support business operations and reliability of electricity supply to customers without being conservative and investing too early or too risk taking where vulnerabilities can be exploited by third parties.

3. OPTIONS

This section provides an overview of a select number of options which could credibly address the need to maintain Ausgrid's OT infrastructure. The NPV associated with each option is also noted.

3.1. OVERVIEW OF OPTIONS

Three options have been considered, which are listed in the table below. The recommended option for the 2025-29 period is option 2 based on quantitative analysis demonstrating that it will unlock the most net economic benefits while maintaining compliance and alignment with good industry practice for OT systems as required by the critical infrastructure licence conditions.

Table 5 – Overview of OT Core Control System Program Options

Option	Description	NPV
Option 1: Extended Infrastructure Life	<p>Investment in Ausgrid's Core System environment in the 2025-29 regulatory control period is driven by an extension of infrastructure lives beyond industry accepted infrastructure end of life. This option focuses on:</p> <ul style="list-style-type: none"> - Replacement after failure to restore the core control system environment to design state - Allowance for some infrastructure to fall outside of vendor support (hardware and software) for a short period, increasing risk, before replacing <p>This option is non-compliant to the critical infrastructure clauses of the existing NSW Government Electricity Distribution Licence Conditions and the Critical Infrastructure Act</p>	\$8.4m
Option 2: Balanced Risk Based Replacement (Preferred)	<p>Routine investment in Ausgrid's OT Core System environment in the 2025-29 regulatory control period.</p> <ul style="list-style-type: none"> - Focus on maintaining vendor support for core components and replacement of critical components before failure. - A proportion of ad-hoc replacement driven by equipment failures - Risk based replacement based on vendor support and standard asset lives <p>Industry standard approach to maintenance of critical system infrastructure and compliance with Ausgrid's Electricity Distribution Licence Conditions.</p>	\$13.0m
Option 3: Increased Proactive Replacement	<p>Accelerate proactive replacement of OT infrastructure reducing reactive replacements and providing a buffer to end of vendor support arrangements.</p> <ul style="list-style-type: none"> - Focus on maintaining clear vendor support for core components and replacement of critical components before failure. 	\$11.0m

	<ul style="list-style-type: none"> - Reducing the proportion of ad-hoc replacement driven by equipment failures - A small proportion of additional disruption to business functions by increased proactive infrastructure replacement 	
--	---	--

The principal difference between the three options is the level of proactive replacement of infrastructure within the Control System environment prior to equipment failure or equipment and vendor end-of-support periods.

We did not include a “do nothing” option as this was not considered a credible option. Failure to maintain an operational electricity network control system would increase operational costs significantly and result in increased harm to the community from slower response times to hazardous network situations.

3.2. OPTION 1: EXTENDED INFRASTRUCTURE LIFE

3.2.1. Description

This option involves extending the life of control system infrastructure beyond standard asset lives and allowing key components of the infrastructure to have no vendor support. This will include increased reactive failures, including increased disruption to network operations and a heightened risk of cyber vulnerabilities resulting in a disruption to electricity supply.

Reduced proactive investment in Ausgrid’s control system during the 2024-29 regulatory control period, with increased focus on replacement of system elements once failures have occurred. This would result in components of the control system falling outside of hardware, software and firmware vendor support during the 2024-29 regulatory control period.

This will be non-compliant with the critical infrastructure clauses of the existing NSW Government Electricity Distribution Licence Conditions for Ausgrid and the requirements of the Critical Infrastructure Act.

3.2.2. Option 1 Assumptions

Option 1 has been estimated based on the following assumptions:

1. Infrastructure will be replaced at a year beyond end of asset life driven by end of vendor support arrangements unless the asset fails.
2. Failure rates are forecast to increase in line with similar critical IT/OT infrastructure.
3. The reactive replacement of infrastructure will lead to an increase in reactive replacement unit costs due to the short-term response and replacement requirements when occurring outside of normal business hours. Failures have been assumed to be random across the day/night.
4. The largest consequence from an intentional and educated breach of the OT environment will result in wide-spread power outages for 12 hours.
5. A proliferation of an IT or OT breach is modelled in 30% of occasions based upon the increase in periods where key infrastructure will not have available patches for cyber vulnerabilities due to end of vendor support. These periods are calculated based on an average of residual risk and unmitigated risk periods where any key OT infrastructure is lacking in vendor support and current patches for identified vulnerabilities.
6. The costs have been estimated based on previous estimates and invoices for similar replacements with escalation to the current year of investment. Investments are largely

contracted services and materials with small internal labour components for coordination and testing.

7. Costs have been supplemented with the variable component of indirect costs for NPV modelling.

All investment is recurrent and associated with maintaining existing functions and capacity within the OT environment.

Capital Cost and Scope Assumptions (FY24 Real \$m)

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$1.3	\$2.1	\$0.8	\$3.1	\$5.1	\$12.4

Operating Cost Assumptions

The opex supporting this option has not been included as it is already included in the current support arrangements.

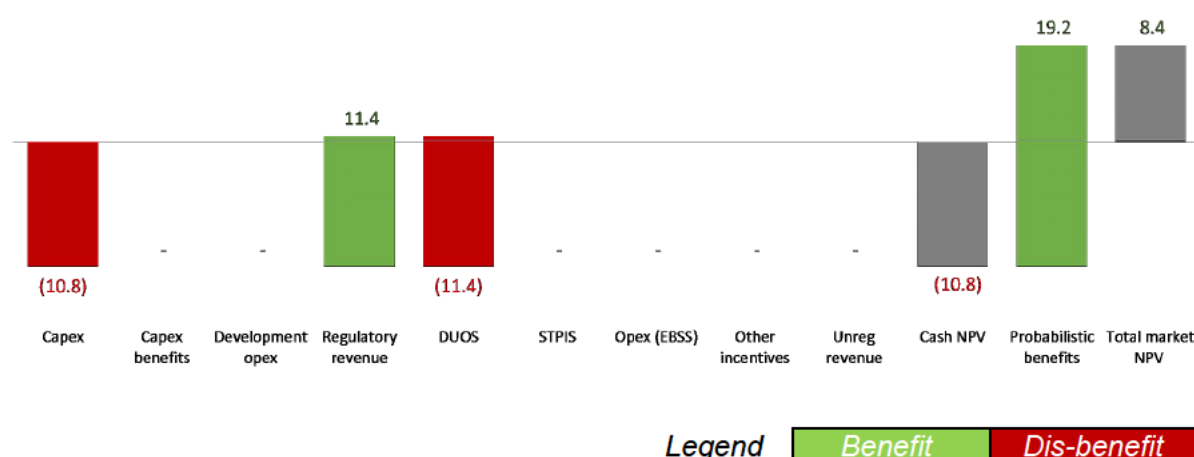
3.2.3. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Increased capex costs from performing work outside of peak periods to avoid customer and business disruption
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from proactive and reactive replacement of infrastructure within this program option.

Market NPV of option (\$' millions, real FY22)



Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber-attack on the OT environment than a fully reactive infrastructure support model. This option has positive net economic benefits compared to a fully reactive support model however is not as economically favourable as the other options.

3.3. OPTION 2: BALANCED RISK BASED REPLACEMENT

3.3.1. Description

This option involves routine investment in replacement of control system infrastructure at end of life, based on end of vendor support or asset failure, to maintain continuous vendor support for managing reliability, availability and remove known cyber vulnerabilities through system software or firmware updates.

This option takes a balanced approach to proactive and reactive replacement avoiding excessive disruption to network operations from reactive replacements or accelerated replacement of core infrastructure in a proactive way.

Ongoing and routine investment in Ausgrid's control system environment in the 2025-29 regulatory control period will focus on:

- maintaining vendor support for infrastructure,
- replacement of critical components before end of life,
- replacing equipment following failures, and
- risk based proactive replacement based on vendor support and standard asset lives.

This option takes an industry standard approach to maintenance of critical system infrastructure and maintains compliance with Ausgrid's Electricity Distribution Licence Conditions.

3.3.2. Option 2 Assumptions

Option 2 has been estimated based on the following assumptions:

1. Infrastructure will be replaced at end of asset life, driven through end of vendor support arrangements or where assets fail.
2. The reactive replacement of infrastructure will lead to an increase in reactive replacement unit costs due to the short-term response and replacement requirements when occurring outside of normal business hours. Failures have been assumed to be random across the day/night.
3. The largest consequence from an intentional and educated breach of the OT environment will result in wide-spread power outages for 12 hours.
4. A proliferation of an IT or OT breach is modelled in 10% of occasions based upon the modelled outcomes for the OT infrastructure in a fully maintained state.
5. The costs have been estimated based on previous estimates and invoices for similar replacements with escalation to the current year of investment. Investments are largely contracted services and materials with small internal labour components for coordination and testing.
6. Costs have been supplemented with the variable component of indirect costs for NPV modelling.

All investment is recurrent and associated with maintaining existing functions and capacity within the OT environment.

Capital Cost and Scope Assumptions (FY24 Real \$m)

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$1.7	\$1.3	\$2.9	\$5.0	\$2.4	\$13.4

Operating Cost Assumptions

The opex supporting this option has not been included as it is already included in the current support arrangements.

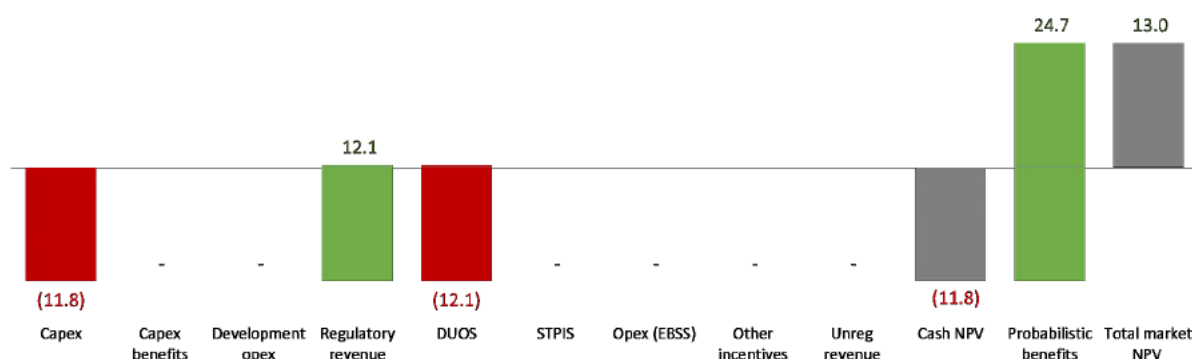
3.3.3. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Increased capex costs from performing work outside of peak periods to avoid customer and business disruption
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from proactive and reactive replacement of infrastructure within this program option.

Market NPV of option (\$' millions, real FY22)



Legend Benefit Dis-benefit

Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber-attack on the OT environment due to the nature of the maintenance of vendor support and balanced risk-based approach to replacement. The increased capex costs from the replacement of infrastructure earlier than Option 1 are offset by the larger probabilistic benefits from maintaining vendor support, resulting in the most favourable net economic benefits of all the options.

3.4. OPTION 3: INCREASED PROACTIVE REPLACEMENT

3.4.1. Description

This option involves accelerated routine investment in replacement of control system infrastructure before end of life. This approach will provide a year's buffer between replacement and end of vendor support. This will reduce reactive replacements caused by asset failure and maintain comfortable and continuous vendor support for managing reliability, availability and removing known cyber vulnerabilities through system software or firmware updates.

This option takes a conservative approach to trading off proactive and reactive replacement introducing some increased disruption to network operations from accelerated replacement of core infrastructure in a proactive way with mitigation of as much disruption as possible by scheduling work outside of normal business hours and peak periods at a marginal additional cost.

Ongoing and routine investment in Ausgrid's control system environment in the 2025-29 regulatory control period will focus on:

- maintaining vendor support for infrastructure, leveraging latest features to avoid cyber risks,
- replacement of critical components a year before end of life,
- replacing equipment following failures, and
- ensuring no assets approach or exceed their standard asset lives.

This option takes an approach exceeding industry standards for maintenance of critical system infrastructure and maintains full compliance with Ausgrid's Electricity Distribution Licence Conditions.

3.4.2. Option 3 Assumptions

Option 3 has been estimated based on the following assumptions:

1. Infrastructure will be replaced at a year prior to end of asset life driven by end of vendor support arrangements, unless the assets fails sooner.
2. The reactive replacement of infrastructure will lead to an increase in reactive replacement unit costs due to the short-term response and replacement requirements when occurring outside of normal business hours. Failures have been assumed to be random across the day/night.
3. The largest consequence from an intentional and educated breach of the OT environment will result in wide-spread power outages for 12 hours.
4. A proliferation of an IT or OT breach is modelled in 8.6% of occasions based upon the modelled outcomes for the OT infrastructure with a minor reduction in risk considering the latest features available in modern infrastructure that is in a fully maintained state.
5. The costs have been estimated based on previous estimates and invoices for similar replacements with escalation to the current year of investment. Investments are largely contracted services and materials with small internal labour components for coordination and testing.
6. Costs have been supplemented with the variable component of indirect costs for NPV modelling.

All investment is recurrent and associated with maintaining existing functions and capacity within the OT environment.

Capital Cost and Scope Assumptions (FY24 Real \$m)

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$2.1	\$3.9	\$5.7	\$2.7	\$1.4	\$15.7

Operating Cost Assumptions

The opex supporting this option has not been included as it is already included in the current support arrangements.

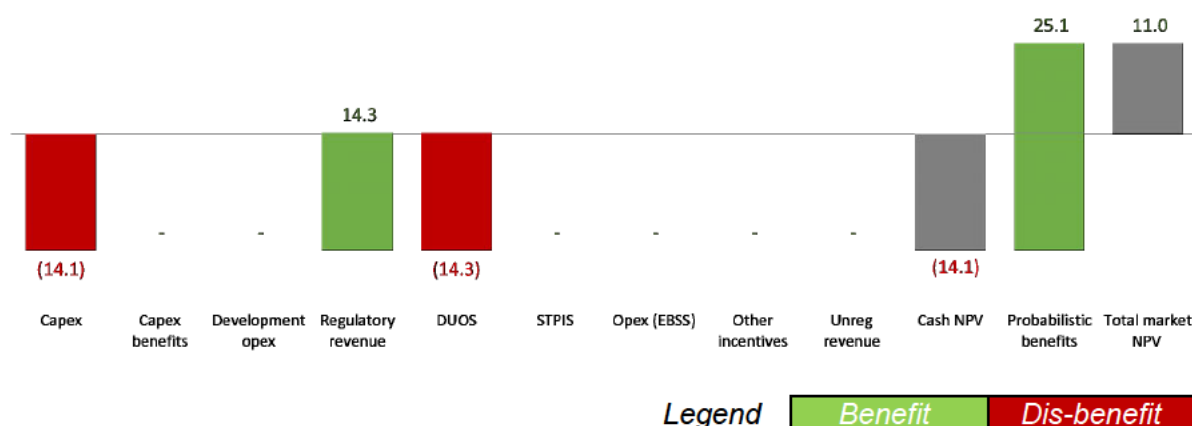
3.4.3. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Increased capex costs from performing work outside of peak periods to avoid customer and business disruption
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from proactive and reactive replacement of infrastructure within this program option.

Market NPV of option (\$' millions, real FY22)



Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber-attack on the OT environment due to the nature of the increased proactive replacement. The increased capex costs from the replacement of infrastructure earlier than the other options results in a minor reduction in the net economic benefits resulting in a less favourable outcome compared to Option 2.

4. RECOMMENDATION

4.1. Recommended solution

Recommended Solution

- Option 2 is the recommended Control System Core Refresh program as it provides the best balance of proactive and reactive replacement of infrastructure with the highest net benefits and seeks to achieve full compliance with regulatory obligations for management of Operational Technology
- This program option will proactively reduce risk within the OT domain to manage availability of the system while fully meeting licence conditions requiring the management of OT with 'best practice'

4.2. Alignment to strategy

The recommended option is included in Ausgrid's business plan and aligns to the current Corporate, Network, Asset Management and Cyber Security strategies. It also meets the NER expenditure objectives, criteria and factors relating to prudence and efficiency of expenditure.

4.3. Program delivery risks

The key risks of the program relate to delivery risk and technology selection. The program structure is designed to mitigate these risks by providing a staged approach to major infrastructure replacements so that excessive lead times for technology components can be managed without major constraints. The approach also allows for the enabling the projects to be selected and adapted to the best available information and resources within industry at the time of detailed design.

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
01	Key Resources	Key resources not available to assist in design of future state or in testing the end product.	Medium	Plan and ensure that resources are available or that resources are backfilled with knowledgeable contracted services.	Low
02	New Technology	If new technology is being introduced as part of this upgrade, the skillset might not be there to sufficiently support it after the program of work has completed.	Medium	Plan and ensure that skillset is developed to ensure that technology can be supported in the future. This includes limited involvement in the implementation projects Targeted replacement of legacy technology to align technology and skill sets.	Low
03	Scope Expansion	Expectation that the scope might include features that were not originally planned for might extend the timeline of the project.	Low	Set scope expectations early on and define boundaries clearly. If additional requirements arise, scope will be discussed through the	Low

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
				appropriate investment governance mechanism.	
04	Costs	Project Costs are estimated based upon best available market knowledge (including supplier quotations) in FY22 and costs could increase as the projects are executed in FY25-29.	Medium	Undertake Gate 3 Business Cases prior to executing each project within the program and revise costs and approach at the time of execution.	Low
05	Key Resources	Availability of SME resources within local market - After effects of the COVID19 pandemic and the economic state have caused a local skill shortage and specialist resources may not be readily available.	Medium	Define resource requirements early and leverage existing relationships with strategic partners where the required skills cannot be found internally within the organisation.	Low

4.4. Program assumptions

The key assumption is that project selection will remain dynamic prior to and throughout the FY25-29 period.

#	Type	Description
01	Resourcing	Appropriate resources will be sourced and available to deliver the selected projects. Specialist resources will also be identified to maintain the control system and broader OT functionality in a business-as-usual context.
02	Commitment	Ausgrid Distribution Licence Conditions have specific requirements for OT, including the use of 'best practice', which will persist for the foreseeable future. Subsequently business focus will remain on delivering the identified projects.
03	Priority	Moderate to high project priority within the broader portfolio of investment
04	Scope	Projects will continue to be evaluated and reprioritised based on at least an annual planning cycle to achieve the greatest risk reduction from investment in each project as part of the overall program. Each potential project is assessed against the core Industrial Control System Security Standards to determine if it aligns to industry direction and 'best practice' to support existing compliance requirements as part of Ausgrid's licence conditions A number of key technology and architecture controls referred to in the Security for Industrial Automation and Control Systems international industry standard are yet to be implemented at Ausgrid and may impact upon this concurrent program. Annual review of the program and dependencies will assist in minimising this impact.

05	Threats	<p>Ongoing reliance on the OT environment will increase as the use of DER increases and may further impact on the expected availability levels of the system.</p> <p>External threats will continue to increase as described in recent announcements from the Australian Cyber Security Centre (ACSC).</p>
-----------	----------------	--

4.5. Program dependencies

A number of currently selected projects in the program require modern integrations to core Ausgrid IT and OT systems. A key program dependency is that these systems remain available to successfully complete the projects and leverage inherent functionality in these systems to avoid additional activities to replicate functionality in isolated systems.

4.6. Business area impacts

The projects within the Control System Core Refresh program are likely to have minimal impact to business operations and customer interactions if performed successfully. The impact on resources should be localised to skilled and capable resources within business technology areas. The majority of program and related expenditure will be focused within the OT area and with appropriate planning and prioritisation impacts should be minimal.

Key partners will be required to support the majority of works and early engagement with procurement groups and partners will be key to minimising impact.

APPENDIX A – PROPOSED CONTROL SYSTEM REFRESH PROJECTS

The following table summarises the control system refresh projects Ausgrid proposes to undertake in the 2024-29 period.

Project Type	Project / Program	FY25-29 Capex (\$m)	Recurring?	Option 1	Option 2 (Preferred)	Option 3
Reactive	Reactive Failures & Minor Capital Enhancements	\$3.5m	Y	Y		
Proactive	OT Workstation Replacement	\$1.2m	Y	Y		
Proactive	OT Infrastructure Replacement – OSS/NPE	\$0.9m	Y	Y		
Proactive	OT Wallboard Replacement	\$0.5m	Y	Y		
Proactive	OT Infrastructure Replacement – ADMS	\$6.3m	Y	Y		
Reactive	Reactive Failures & Minor Capital Enhancements	\$2.6m	Y		Y	
Proactive	OT Workstation Replacement	\$1.3m	Y		Y	
Proactive	OT Infrastructure Replacement – OSS/NPE	\$0.9m	Y		Y	
Proactive	OT Wallboard Replacement	\$1.0m	Y		Y	
Proactive	OT Infrastructure Replacement – ADMS	\$7.6m	Y		Y	
Reactive	Reactive Failures & Minor Capital Enhancements	\$2.2m	Y			Y
Proactive	OT Workstation Replacement	\$1.8m	Y			Y
Proactive	OT Infrastructure Replacement – OSS/NPE	\$1.8m	Y			Y
Proactive	OT Wallboard Replacement	\$1.2m	Y			Y
Proactive	OT Infrastructure Replacement – ADMS	\$8.8m	Y			Y

APPENDIX B – APPROACH TO QUANTIFICATION OF PROJECT BENEFITS

Ausgrid has identified three potential categories of benefits and has quantified these benefits wherever feasible and practicable.

The following table details the benefits categories and our approach to quantifying the value of each type of benefit. Benefits that cannot be readily quantified are described qualitatively.

Benefit category	Description	Quantification approaches
Operational benefits to Ausgrid and/or customers (loss of OPEX productivity and loss of CAPEX productivity)	<p>Direct improvements in the operations and / or services supplied by Ausgrid as a result of an investment. These benefits are typically reflected in avoided time reacting to an event or equivalent reduced costs (efficiencies), such as direct cost savings for Ausgrid.</p> <p>These costs will be passed on to customers in the longer term through reduced costs for energy.</p>	<ul style="list-style-type: none"> Cost savings are quantified through cost build up (e.g. hours of labour saved <i>times</i> average cost of labour per hour). These costs saved or inefficiencies avoided are quantified in monetary terms where related to a direct event causing this cost. The likelihood of an event considers the likelihood of a malicious actor succeeding in penetrating through the layers of defence in the OT systems. This is calculated as the multiplication of the likelihood of passing each defence from the point of entry.
Reduced capital required to replace damaged equipment (avoided capex)	The cost avoided if a malicious actor were to succeed in gaining control inside the OT environment and damaging hardware or irrevocably changing the hardware into an inoperable state	<ul style="list-style-type: none"> Risk based benefits are quantified by estimating the change in the expected cost of the risk, where the expected cost of the risk is estimated as the likelihood of the event (%) multiplied by the consequence of the event (\$) The likelihood of an event considers the change in likelihood of a malicious actor succeeding in penetrating through the layers of defence in the OT systems following an investment. This is calculated as the multiplication of the new likelihood minus the old likelihood of passing each defence from the point of entry.
Customer benefit related to avoided unserved energy	The customer impact from a supply of electricity interruption for a particular duration as a result of a OT security breach and the acts of that malicious actor.	<ul style="list-style-type: none"> The consequence is calculated as the loss of supply, which is measured using an estimate of the unserved energy and the value of customer reliability (VCR) for Ausgrid's distribution area. I.e. multiplying the value of customer reliability by the duration of the supply interruption and the number of customers without supply for each scenario.

APPENDIX C – INDUSTRY BEST PRACTICE FOR OPERATIONAL TECHNOLOGY

Purpose

This appendix outlines the recent history regarding the cyber security uplift to Ausgrid's Operational Technology (OT) domain, including a summary of obligations and background to the introduction of the Critical Infrastructure Licence Conditions, the Critical Infrastructure Act 2018 and associated implications to Ausgrid's Operational Technology environment. This document also outlines Ausgrid's interpretation of 'best industry practice for electricity network control systems' as referenced in Ausgrid's Licence Conditions.

Background

The industrial control systems within the electrical network industry, known as OT, are defined as the application of information technology systems for the purpose of directly operating or managing devices on the electricity network, including the integration of remote devices (field and substation) with supervisory control and data acquisition (SCADA) systems using communications links to provide a platform that is used to monitor and operate the underlying asset.

It includes any hardware or software which detects or causes a change to network operation through the direct monitoring and/or control of physical devices, processes and events in the distribution system. This is often referred to as the 'cranking path' by practitioners in determining what action could related to a change in the configured electricity network state.

Historically, industrial control systems utilised specialised, bespoke hardware and dedicated communication channels. However, in the last 25 years, SCADA systems have moved away from bespoke hardware to utilising similar or identical Information Technology (IT) platforms. These platforms provide improved functionality, flexibility and redundancy for lower cost, however, require different skills and capability to manage. Importantly these systems share some security vulnerabilities that can affect corporate IT systems that bespoke industrial systems were not exposed to historically. Management of these security vulnerabilities in the OT environment is a fast-evolving area and has become a significant focus of utilities and governments around the world.

Challenges of OT/IT Convergence

The term OT/IT convergence reflects patterns of similarity between the two environments. There are two common industry trends that are reflective of OT/IT convergence but are quite different in their impacts on cyber security. The first is the use of IT hardware systems within the OT environment. As systems rely on more commonplace technologies, we witness OT hardware being similar to that which is employed in the IT space. The systems might appear the same but have quite different purpose and function. The second trend is business enablement which sees the controlled interaction between OT and IT systems to support operational activities and business insight.

Whilst the benefits of this convergence exist, there remain a number of important differences in the architecture, configuration and purpose between the two domains. Traditional IT security objectives (heavily influenced by the banking and financial sectors) typically follow the priorities of confidentiality, integrity and availability. In the case of control systems, and particularly electricity networks, the consequences of a security breach are very different and therefore the priorities are different.

The combined importance of safety, availability and integrity within an OT system mean that nothing must be done on the active control system network that would interfere or disrupt the time-critical operations of the system where there are potentially adverse safety outcomes. In the control systems environment, the security objectives of the IT world are replaced by human health and safety, availability of the system, and timeliness and integrity of the data.

Table 1 illustrates the key differences in the priority of various system objectives and the key consequences from the loss of system function from a cyber security intrusion. This is exaggerated by

the difference in non-time critical applications/systems compared to those with time criticality with direct implications to people and infrastructure.

Table 1 - IT / OT Cyber Security Differences

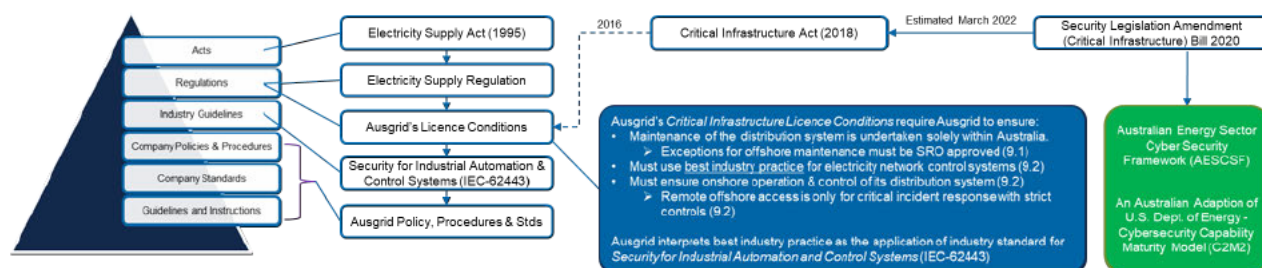
IT / OT Cyber Differences	Operational Technology	Information Technology
Objectives: Information & Operational Technology systems and processes have differing objectives given their differing purposes	Objectives by priority 1. System Availability 2. System Integrity 3. Information Confidentiality	Objectives by priority 1. Information Confidentiality 2. System Integrity 3. System Availability
Consequences: The criticality and type of realised consequences differ between information and operational systems for a failure or potential cyber intrusion.	<ul style="list-style-type: none"> Power Outages Damage to Assets Injury / Death Secondary impacts: <ul style="list-style-type: none"> Reputational Damage Regulatory Fines Work Cover Investigations Court actions and/or Coroner's court directions 	<ul style="list-style-type: none"> Loss of Privacy Loss of Productivity Financial Loss Reputational Damage Loss of Data Regulatory Fines Court Actions

Due to these differences, while the OT and IT domains often use similar or identical technology, differences in focus between the two domains drives the need for specific industry-aligned approaches appropriate to cyber security for the OT domain.

Ausgrid's Regulatory Environment

Ausgrid operates in a highly regulated environment. Ausgrid's cyber security governance, at a high level, is shown below in Figure 1.

Figure 1 - Ausgrid Compliance Requirements



Ausgrid's Critical Infrastructure Licence Conditions

Ausgrid has key obligations in its Distributor's Licence to operate a distribution system under the Electricity Supply Act 1995 (NSW). The NSW Minister for Industry, Resources and Energy grants the distribution licence under section 14 of the Electricity Supply Act 1995 (NSW). The Minister also imposes on Ausgrid a schedule of Licence Conditions for the Operator (Ausgrid) of a Transacted Distribution System.

On 1 December 2016 Ausgrid transitioned to a 50.4% long term lease with private ownership. As part of the lease transaction, the NSW Minister updated the schedule of Licence Conditions for the Operator (Ausgrid).

A key change at this point in time was the introduction of additional 'Critical Infrastructure Licence Conditions' (Conditions 9, 10 and 11). These requirements describe the significance of infrastructure being managed by Ausgrid, as described in the excerpt below:

CRITICAL INFRASTRUCTURE LICENCE CONDITIONS

... the assets which the Licence Holder operates may constitute "critical infrastructure" being those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the security, social or economic wellbeing of the State of New South Wales ... These licence conditions will be reviewed by the Minister from time to time (and where necessary) in consultation with responsible Ministers of the Commonwealth ...

The Critical Infrastructure Licence Conditions included in the schedule of Licence Conditions were developed by NSW Government and Commonwealth agencies. This review included Foreign Investment Review of the Licence Condition provisions. The licence conditions require a:

- Substantial presence must be held in Australia and prevent operation or control of the control systems or the supporting ICT from outside of Australia (Condition 9); and
- Data Security must be maintained that prevents access to operational technology, ICT or bulk load and customer information from outside of Australia or from unauthorised persons (Condition 10).

Condition 9 contains clear requirements for Ausgrid to use industry best practice. As industry best practices are evolving, Ausgrid interprets best industry practice in a manner consistent with industry participants, such as the Australian Energy Market Operator (AEMO). This includes adoption of a hierarchy of industry standards, guidelines and advice as outlined in Table 2 – *Hierarchy of reference material representing industry best practice*, and the best practice reference list attached in Appendix 1.

Condition 9 also recognised that compliance with the requirements involved a significant uplift in the Cyber Security capabilities of the OT domain. This condition allowed for a ministerially approved implementation plan that provided a 12 month program of works to uplift the OT infrastructure, capability, policies and procedures. Ausgrid's implementation plan focused on key areas including:

- Control System Isolation and Segregation;
- Control System Distribution Network Management System Improvements;
- Control System Security Architecture; and
- Security Information and Event Management (SIEM).

The implementation plan required an investment of around \$10m in 2017 to achieve the required uplift in the infrastructure, capability, policies and procedures in the OT domain.

In the last regulatory period, Ausgrid has continued to uplift the maturity of OT security to further align with Licence Conditions requirement to use best industry practice. An annual plan is developed to maintain compliance in line with the evolving frontier of industry best practice. Ausgrid consults with industry participants and bodies continuously and incorporates feedback into each annual planning cycle.

Ausgrid's Critical Infrastructure Licence Conditions were revised and re-issued in December 2017 following the first IPART audit against the conditions in 2017, and subsequent detailed engagement with IPART, the NSW Minister for Industry, Resources and Energy, and relevant Commonwealth agencies.

The key revisions to the Critical Infrastructure Licence Conditions were:

- Introduction of the Remote Access Protocol; and
- Adjustment of Data Security requirements and definitions.

The Remote Access Protocol was originally developed and agreed between the Commonwealth Representative and Ausgrid and was based on the CERT – ICS Remote Access Protocol⁶. Ausgrid Specific adaptations have been identified and agreed in the ‘Ausgrid Industrial Control System Remote Access Protocol Agreement’ agreed in June 2022.

The CERT – ICS Remote Access Protocol was developed to allow specific external parties (vendors) to securely remotely connect to critical infrastructure control networks. This includes design principles for the technology to enable secure remote access, implementation principles to provide guidance on approaches for satisfying the design principles and the specified protocol, or procedure, for remote access.

Further work has been undertaken between Ausgrid and the Commonwealth agencies to refine the required Remote Access Protocol for Ausgrid and significant work has been undertaken to commence deployment of this capability.

Critical Infrastructure Act 2018 and Amendments in 2021 and 2022

The Security of Critical Infrastructure Act 2018 commenced in July 2018, to provide a framework for managing risks to national security relating to critical infrastructure through:

- improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and
- facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.

A critical Infrastructure asset is defined to include critical electricity assets, which are defined broadly to include a network, system, or interconnector, for the transmission or distribution of electricity. Ausgrid’s distribution system is a critical electricity asset and its entire network is captured by the definition within the Act.

The act includes powers of direction and information provision.

The Critical Infrastructure Centre has been formed to administer the Act and carry out the following high-level activities:

- Conduct national security risk assessments to support the Foreign Investment Review Board;
- Develop and implement targeted mitigations in concert with industry, states and territories; and
- Develop improved best practice guides for industry.

Ausgrid has closely engaged with the Critical Infrastructure Centre during the development of the Act, the 2017 revision to the Ministerial Distributor’s Licence Conditions and the ADMS project. All of these engagements have informed and refined Ausgrid’s understanding of what constitutes industry best practice for electricity network control systems.

This engagement has continued with the energy sector co-design working groups and the proposed Security Legislation Amendment (Critical Infrastructure) Bill 2021. The aim of the Bill is to provide a framework for managing risks to national security relating to critical infrastructure. On advice from the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in September 2021, this bill was broken into two complimentary smaller bills to pass in sequence. The first bill aims to support Govt involvement and intervention in the event of a major cyber incident affecting critical infrastructure. The second is responsible for guiding the security and resilience uplift among identified operators of critical infrastructure and national significance.

During Energy Sector co-design working groups for the Critical Infrastructure Bill (2021), the use of Australian Energy Sector Cyber Security Framework (AESCSF) or other equivalent standard to drive the intended risk management framework was well supported by the Energy Sector participants. While not accurately reflected in the first Bill and associated rules, Commonwealth agencies have indicated that there is an appetite to introduce requirements for Critical Infrastructure Operators to comply with AESCSF SP-2 and SP-3 requirements at a future time likely inside the 2025-29 regulatory period. It is expected this will be in the form of the rules associated with this second bill.

⁶ https://www.cert.gov.au/sites/g/files/net3281/f/remote_access_protocol.pdf

Ausgrid is uplifting the OT Cyber governance framework to align to AESCSF SP-2 and SP-3 capability and maturity where there is demonstrable value in doing so.

In support of this approach is the Risk Management Program Rules provided with the Bill, including the requirement to identify and mitigate the risks and hazards associated with a cyber attack resulting in prolonged outages to the electrical network. These various risks are to be managed in accordance with industry best practise.

Industry Best Practice

In 2016 Ausgrid developed an OT / Control System Security Strategy which was further refined with the introduction of the Critical Infrastructure Licence Conditions and its subsequent revision. This strategy has informed the Operational Technology Security Strategy and the cyber security program.

This strategy references current good and best practice in SCADA systems and, where applicable, IT Cyber Security practices from the following key reference material outlined in the best practice reference list attached in Appendix 2. This approach is in alignment with Ausgrid's obligations under Critical Infrastructure Licence Condition 9.2.

A hierarchy of reference material has been developed with the most relevant and authoritative source being IEC-62443 – Security for Industrial Automation and Control Systems as depicted in Table 2 – *Hierarchy of reference material representing industry best practice*. In cases where the primary reference offers no (or insufficient) guidance, secondary and more detailed reference materials are utilised.

In addition to using IEC-62443, Ausgrid has adopted the use of the Australian Energy Sector Cyber Security Framework (AESCSF) to assist in assessing Ausgrid's OT cyber security capability and maturity and identifying further areas for improvement.

Table 2 – Hierarchy of reference material representing industry best practice

Hierarchy of Preferred Best Practice Standards	Applicable Standard
Primary Reference Standards <ul style="list-style-type: none"> International standard for control systems Widely accepted across energy sector to protect critical infrastructure from cyber threats 	IEC-62443 – Security for Industrial Automation and Control Systems
Governance framework standard	Australian Energy Sector Cyber Security Framework (AESCSF).
Secondary Reference Standards <ul style="list-style-type: none"> Authoritative (US Government) guide for control systems 	NIST SP800-82 – Guide to Industrial Control Systems (ICS) Security
Detailed References <ul style="list-style-type: none"> Authoritative Government guide for specific issues and where relevant vendor recommendations 	Generic Cyber Security Government Guides and Standards <ul style="list-style-type: none"> NIST Special Publications ASD Strategies & Guidance Vendor Recommendations <ul style="list-style-type: none"> Recommended configurations Reference architectures Support notices

Note, the above list represents a current view of industry OT cyber best practice and will be refined as the cyber threat landscape continues to evolve and industry and general cyber security best practice changes. In support of continuous improvement and supported by

IEC62443 standard, Ausgrid will continue to monitor and update this reference list during the periodic review of policy, procedures and standards.

APPENDIX D – BEST PRACTICE IN OT – REFERENCE STANDARDS

International		
ISA	International Society for Automation	<ul style="list-style-type: none"> TR99.00 01-2007 Security Technologies for Industrial Automation and Control Systems, TR99.00 02-2004 Integrating Electronic Security Into The Manufacturing And Control Systems Environment
IEC	International Electrotechnical Commission	<ul style="list-style-type: none"> 62443-1-1 Security for Industrial Automation and Control Systems – Models and Concepts, formerly ISA-TR99.00.01 IEC 62351 (TC57, WG15) – Security standards for the power system information infrastructure
ISO	International Organization for Standardization	<ul style="list-style-type: none"> Common Criteria for Information Technology Security Evaluation
Australia		
ASD	Australian Signals Directorate Formerly Defence Signals Directorate (DSD)	<ul style="list-style-type: none"> Strategies to Mitigate Targeted Cyber Intrusions ASD Top 35 Mitigation Strategies ASD Top 4 extending to the Essential 8 CERT – Industrial Control System Remote Access Protocol
AEMO	Australian Energy Market Operator	<ul style="list-style-type: none"> Australian Energy Sector Cyber Security Framework (AESCSF).
TISN	Trusted Information Sharing Network	<ul style="list-style-type: none"> Generic SCADA Risk Management Framework For Australian Critical Infrastructure Risk Management for Industrial Control Systems (ICS) And Supervisory Control Systems (SCADA) Information For Senior Executives SCADA Security Good Practice Guide - Hardening of SCADA ICT Systems
AGD	Attorney Generals Department	<ul style="list-style-type: none"> Critical Infrastructure and Protective Security Policy
	Edith Cowan University Research Online	<ul style="list-style-type: none"> Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption
United States of America		
NERC	North American Electric Reliability Corporation	<ul style="list-style-type: none"> NERC-1200 - North American Electric Reliability Corporation Cyber Security Standards NERC 1300 – Cyber Security <ul style="list-style-type: none"> C P-002 –Critical Cyber Assets C P-003 –Security Management Controls C P-004 –Personnel and Training C P-005 –Electronic Security C P-006 –Physical Security C P-007 –Systems Security Management C P-008 –Incident Reporting & Response Management C P-009 –Recovery Plans
NIST	National Institute of Standards and Technology	<ul style="list-style-type: none"> SP 800-82, Guide to Industrial Control Systems (ICS) Security SP 800-77, Guide to Psec VPNs SP 800-30, Risk Management Guide for Information Technology Systems SP 800-40, Creating a Patch and Vulnerability Management Program
SANS	SANS Institute - Escal Institute Of Advanced Technologies, Inc	<ul style="list-style-type: none"> Security for Critical Infrastructure SCADA Systems
DOE	U.S Department of Energy	<ul style="list-style-type: none"> 21 Steps to Improve Cyber Security of SCADA Networks Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems The Department of Energy (DOE) developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
DHS	U.S. Department of Homeland Security	<ul style="list-style-type: none"> Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies Good Practice Guide: Cyber Security Assessments of Industrial Control Systems
DISA	Defense Information Systems Agency	<ul style="list-style-type: none"> The Security Technical Implementation Guides (STIGs)
CIS	Center for Internet Security	<ul style="list-style-type: none"> Cyber Security Procurement Language for Control Systems
EEI	Edison Electric Institute	<ul style="list-style-type: none"> Patch management strategies for the Electric Sector
United Kingdom		
CPNI	Centre for the Protection of National Infrastructure	<ul style="list-style-type: none"> Good Practice Guide on Patch Management Configuring and Managing Remote Access for Industrial Control Systems Cyber security assessments of industrial control systems Process control and SCADA security - General Guidance Firewall deployment for SCADA and process control networks Process Control and SCADA Security Guides 1- 7