30 November 2023

Ausgrid’s 2024-29 Revised Proposal

Attachment 5.8.2: Operational Technology Core Refresh and Security programs

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

Ausgrid

Contents

Introduction

The purpose of this attachment is to provide a response to the Australian Energy Regulator's (AER) Draft Decision for the Operational Technology Core Refresh and Security programs. Ausgrid has proposed two key investment programs related to our Operational Technology (OT).

These programs seek to:

- Maintain the ongoing reliable operation of the control system by undertaking the necessary investments in hardware and software; and
- Undertake prudent investments to enhance Ausgrid's OT security to protect and manage against cyber threats, including enhancing our capability to meet the increasing sophistication, frequency, and severity of those threats.

The AER's Draft Decision did not approve our Initial Proposal (see **Figure 1**) because the AER wanted additional information on:

- Drivers behind the forecast increase in expenditure relative to recent historical spend.
- The prudency and efficiency of investing in a higher security profile level without a legislated obligation.
- Options analysis and the underlying scope of works to support the optimal timing of different investments.

Ausgrid has revised its Initial Proposal, seeking the full amount of expenditure for our OT Core Refresh Program and a reduced amount ($7.7m lower) for the OT security program (see **Section 3**).

Figure 1 Summary of changes to OT investment programs ($ million, real FY24)

	Initial Proposal	Draft Decision	Draft Decision (variance)	Revised Proposal
OT security program	26.0	12.5	(26.7)	18.3
Control system core refresh	13.4			13.4
Total	**39.4**	**12.5**	**(26.7)**	**31.7**

The AER’s Draft Decision

The AER’s Draft Decision includes $12.5m for both OT core refresh and security capex, which is $26.5m (68%) lower than Ausgrid’s Initial Proposal.

The AER considered the Draft Decision to be in line with historical expenditure, and that:

- There was insufficient information to demonstrate expenditure beyond this level is justified to satisfy the capex criteria; and
- The link between our planned investment and regulatory obligations could have been more clearly explained.

Revised OT Core Refresh program

In response to the AER’s Draft Decision, Ausgrid has reviewed the OT Core Refresh program. Ausgrid is seeking the full amount of expenditure for our OT Core Refresh program as outlined in our Initial proposal, totaling $13.4 million.

In response to the AER’s feedback, this attachment provides additional information to clarify the information that should be used to compare our forecast with our historical OT Core System refresh costs. This additional information centres on how to treat historical OT Core Refresh costs that were incorporated into larger projects in the 2019-24 period. Ausgrid did not clearly provide this information in our Initial Proposal so these costs wrapped up in larger projects were not considered in the AER’s trend analysis at the Draft Decision stage.

Over the current regulatory period Ausgrid has undertaken one-off major projects that have impacted OT assets, and resulted BAU asset lifecycle refresh activity being inadvertently picked up by those projects (i.e. OT infrastructure assets performing key network functions receiving investment that otherwise would have been required and funded under this BAU program).

The major projects that incorporated elements of OT infrastructure and software spend in the current regulatory period, which were not included in the AER’s trend analysis at the Draft Decision stage, include:

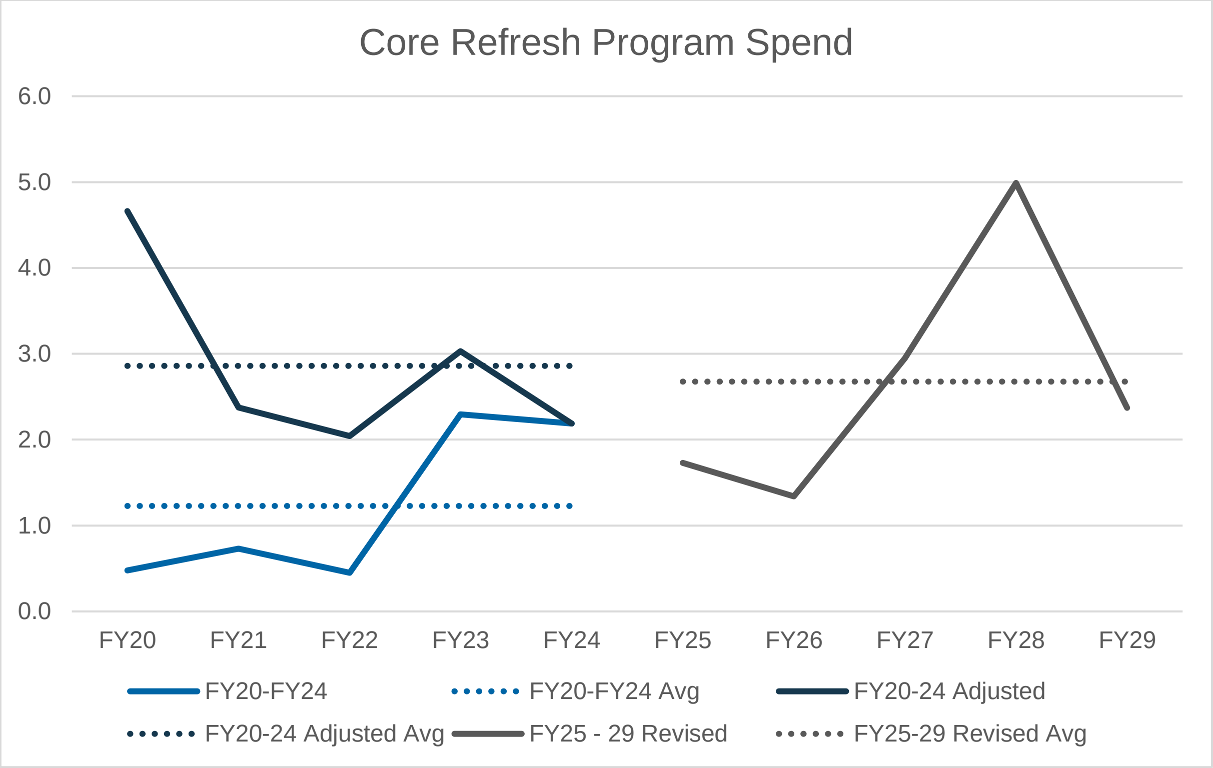
1. **Sydney Control Room Relocation:** Relocating Ausgrid’s Sydney Control Room and OT data centre included a greenfield infrastructure deployment to allow the staged operational relocation of the Sydney Control Room. This required new workstations, data centre infrastructure, and control room wallboard systems of which $0.85m was within FY19.

   This was a specific and non-recurring circumstance resulting in an infrastructure lifecycle refresh that is not captured in historical expenditure against the OT Core Refresh program.

2. **ADMS Phase 1:** During the delivery of ADMS Phase 1, the infrastructure hardware, design and deployment related activities cost $7.49 million between FY20 and FY23. The ADMS project infrastructure work enabled the retirement of a significant portion of the aged infrastructure that made up the OT core system, which otherwise would have required replacement under the OT Core Refresh program.

Figure 2 below is a graphical representation of the historical spend on the OT Core System refresh program inclusive of the spend associated with the core refresh components of the Control Room Relocation and ADMS Phase 1 core system spend.

Figure 2 - Core Refresh Program Spend Historical corrected and Proposed



Our risk analysis has determined that the forecast OT core refresh investment is required to maintain the ongoing and reliable operation of the control system. These investments in hardware and software are required to maintain the operational integrity and high availability requirements of this 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, failure patterns, or lack of ongoing vendor support (lack of availability of replacement parts and software or firmware updates to maintain availability or security).

Ausgrid considers this forecast represents the prudent and efficient expenditure required to meet the capital expenditure objectives under the NER, including but not limited to our regulatory obligations such as:

- Ausgrid's Distribution Network Service Provider (DNSP) Ministerially Imposed Licence Conditions – Appendix 2, Clause 1 & 2 – 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.

Consistent with other OT investments, we have identified the most efficient means of delivering this capability, with the highest net present value (NPV) of $13.0m, as our proposed approach.

Revised OT Security program

Following the AER's draft determination, Ausgrid has reviewed the OT Security program. Ausgrid's Revised Proposal is seeking a reduced amount of expenditure for the OT security totaling $18.3 million (30% reduction).

The OT Security program has been reduced with a rephasing of an OT communications system (PDH Mux) upgrade. The replacement of this legacy communications system provides a security enhancement to the Operational Technology communications environment and physical segregation of the OT communications network.

Ausgrid has tested alternative replacement parts from the vendor and tested backwards compatibility of components, which will extend the life (including security outcomes) of the asset type by an estimated 2 years, based on current failure rates.

It is proposed to defer the start of this project by two years. Design work will commence in the FY24-29 regulatory period with field delivery now planned to commence in the following regulatory period.

In response to the AER's feedback, Ausgrid do not believe that using historical data for the OT security program is appropriate. Historical trends of expenditure on this program does not capture the full historical expenditure that has been required to manage Ausgrid's OT security risks.

Over the current regulatory period Ausgrid has undertaken major projects that have resulted in asset lifecycle refreshes which have enhanced security architectures. These projects have uplifted and introduced enhanced security capabilities for core OT systems performing key network functions. These investments would otherwise have been covered under this program.

The major projects that incorporated OT security spend in the current regulatory period, but which do not appear to have been included in the AER's trend analysis at the Draft Decision stage, include:

Sydney Control Room Relocation:

Relocating Ausgrid's Sydney Control Room and OT data centre included a greenfield infrastructure deployment to allow the staged operational relocation of the Sydney Control Room.

This was a specific and non-recurring circumstance resulting in an infrastructure lifecycle refresh, new technology and security capabilities that is not captured in historical expenditure against the OT security program.

ADMS Phase 1:

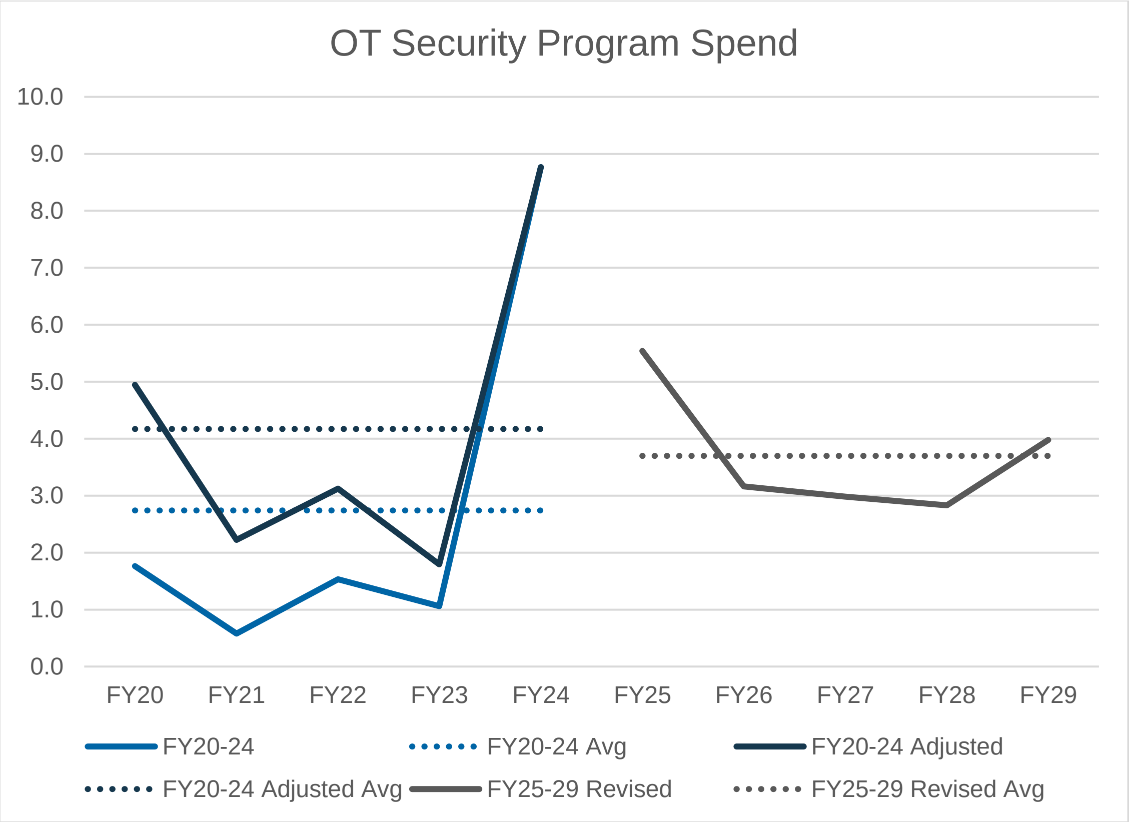
During the delivery of ADMS phase 1, the security architecture, security capabilities and design and deployment related costs of $7.49 million between FY20 and FY23. The ADMS project provided a security uplift and enhanced capabilities which otherwise would have required replacement under the OT Security program.

The ADMS project has addressed many legacy security constraints outside of the OT Security expenditure. As part of the ADMS project, software and infrastructure that had inherent security limitations have been retired. As well, it has replaced legacy software that would have otherwise required significant version upgrades to address known and exploitable security vulnerabilities. These would have taken significant expertise, resources, and costs to address in the absence of the ADMS project.

In addition, Ausgrid's risk analysis shows that forecasting OT Security future investments based on historical expenditure appropriately reflects future needs due to:

- The unmitigated risks to Ausgrid's OT environment are increasing due to geo-political environment, security landscape and threat profile to Critical Infrastructure operators deteriorating[1].
- New specific advanced threat actors, tools and techniques have emerged and are directly targeting OT environments and critical infrastructure operators in Australia;
- New security technology and tools are now available that are suitable for OT, which were not available in prior regulatory periods, resulting in an advancement of the position of 'industry best practice' required by current licence conditions.
- Additional security devices required for contemporary security solutions to adapt to evolving security landscape and threat profile.

Figure 3 – OT Security Program Spend Historical corrected and Proposed



Ausgrid's risk analysis shows that the proposed OT security program investments are necessary for Ausgrid to protect and manage Ausgrid's OT environment against known and likely future cyber threats. It describes a necessary increase in capability to meet the increasing level and

[1] The Australian Cyber Security Centre (**ACSC**) states that approximately 76,000 incidents of cyber crime were reported in 2021-22 - one quarter of which affected entities associated with Australia's critical infrastructure. Cyber-attacks are increasing in frequency, with a 13% increase in cyber-attacks reported by Australian entities to the ACSC in 2020-21.

severity of threats. Ausgrid have identified the most efficient means of delivering this higher level of capability, with the highest economic benefit for customers.

The program of works has been established presents the most favorable NPV for customers as it includes a portfolio of projects (largely related to technology-based controls) that deliver the highest net benefits and is able to demonstrate compliance with Ausgrid’s obligations for management of OT so far as is reasonably practicable (SFAIRP).

This program option will proactively reduce cyber risk within the OT domain to mitigate all known risks SFAIRP and within Ausgrid’s appetite while fully meeting licence conditions requiring the ‘best practice’ management of OT.

Each project included in the OT security program has been assessed individually through a cost benefit analysis identifying a positive NPV for implementation when compared to a do nothing case. These projects have also been assessed as a program holistically to minimise the potential for overinvestment and confirm that both OT security projects and program are SFAIRP in line with Ausgrid's obligation.

Ausgrid considers this forecast represents the prudent and efficient expenditure required to meet the relevant capital expenditure objectives under the NER, including but not limited to our regulatory obligations such as:

- Ausgrid’s Distribution Network Service Provider (DNSP) Ministerially Imposed Licence Conditions – Appendix 2, Clause 1 & 2 – 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.