INFORMATION AND COMMUNICATIONS TECHNOLOGY

NETWORK MANAGEMENT SYSTEMS

UE BUS 7.05 – PUBLIC
2026–31 REGULATORY PROPOSAL

Table of contents

1. Overview

Our network management systems include a suite of core operational systems that play a critical role in ensuring that we can safety and reliability manage our electrical distribution network.

Our network management systems include the functionality supporting real time access and management of network performance, including the ability to identify customer faults, automatically switch feeders to avoid customer outage time, and communicate to our customers when they are experiencing an outage. Network management systems also provide the tools to ensure network, employee and public safety is maintained.

During our stakeholder engagement program, customers consistently highlighted the importance of a reliable energy supply as well as the importance of effective communication during outages.

During the 2026-2031 regulatory period, the existing versions of our network management systems will require upgrades, refreshes, maintenance releases and patching to ensure currency. Maintaining currency ensures our systems remain within vendor support to safeguard the delivery of a safe and reliable supply of electricity and ensure compliance with the Distribution Code.

We considered three options related to maintaining our market systems:

1. **do not maintain currency** – Under this option we would not apply any updates to our systems over the 2026–31 regulatory period
2. **maintain currency** – Under this option we would undertake prudent upgrades to maintain minimum core currency
3. **maintain currency with more frequent upgrades** – Under this option we would perform all upgrades as recommended and released by the vendor.

Option two is recommended as it ensures the continuity of critical business and market processes, maintains compliance and provides the best value to customers.

The following table provides a summary of our options analysis for the 2026-2031 regulatory period.

TABLE 1 OPTIONS ANALYSIS SUMMARY ($M, 2026)

OPTION		CAPEX	OPEX	NPV
1	Do not maintain currency	-	1.9	-
2	Maintain currency	53.7	-	26.7
3	Maintain currency with more frequent upgrades	63.1	-	21.8

2. Background

The safety and reliability of our electrical distribution network are reliant upon functioning and dependable IT systems. We refer to this collection of systems as our network management systems. They provide the functionality to support real time access and management of network performance, including the ability to identify customer faults, automatically switch feeders to avoid customer outage time, and communicate to our customers when they are experiencing an outage. Network management systems also provide the tools to ensure network, employee and public safety are maintained.

Our network management systems play a critical operational role in ensuring that we can effectively and efficiently manage our electrical distribution network. These systems have a real-time 24/7 requirement to provide control and monitoring of customers' supply reliability and network performance as well as providing tools to ensure network, employee and public safety is maintained.

These systems are integrated all across our business, from managing network telemetered devices (e.g., remotely controlled switches that affect customers' supply if operated) through to smart meters that derive real-time information for our business to more effectively monitor and manage our customers' supply.

The network management systems can be categorised into three groups. Further information on each system and the functionality associated is provided in the tables below.

- Network management core
- Network geospatial
- Network reporting and data processing

TABLE 2 NETWORK MANAGEMENT CORE SYSTEMS

SYSTEM	DESCRIPTION
Advanced Distribution management System (ADMS)	ADMS monitors and controls the electricity distribution network and is tightly integrated with the Supervisory Control and Data Acquisition System (SCADA) by retrieving real-time data from network field devices through SCADA to enable more informed operational decision-making and control. ADMS also provides functions and modules to support the following critical services: • Fault Detection Isolation Restoration (FDIR) – automatically switches the network to restore as many customers as possible in a matter of seconds. • High Voltage Distributed Energy Resource Management (HV DERMS)[1] - allows new renewable generators to access existing network capacity more efficiently without requiring poles and wires upgrades. Our previous outage management system (OMS) functionality has been incorporated into ADMS.

[1] HV DERMS - CitiPower Powercor's world-first system to support large scale renewables

Electricity Distribution Network Access Register (EDNAR)	EDNAR enables the network access request process for planned work on the CitiPower and Powercor electrical distribution networks and associated switching operations. This platform is necessary to manage planned works on the network including those that require supply interruptions to those customers who will be off supply in order for the works to safely proceed. It includes workflow management, the initiation of the customer notification process, audit trail, attachments and internal notification processes. It ensures that only those authorised to work on the network can generate an access request.
Historian (OSI Pi)	The Historian system supports network operational and planning activities including: • Ability to view and chart historical data, validate network models used to simulate network scenarios, and determine augmentation works required. • Preparation of regulatory report submissions including the RIN, DAPR, TAPR and calculating Distribution Loss Factors. • Extensive use in the access management process. i.e. permit approval.
PRISM	This software is used by the Asset Management team to manage power quality and field relay settings that assist in ensuring the distribution network is optimised and operated within network safety limits.
Sensor IQ (SIQ)	SIQ is used to perform real time effective analysis of the low voltage network. The Itron SIQ solution integrates with our Advanced Metering Infrastructure (AMI). SIQ enables us to perform real-time voltage assessment and can proactively identify quality of supply issues. Granular power quality data is available via voltage, current and power factor sampling of all meters.
Supervisory Control and Data Acquisition (SCADA)	SCADA is used to manage the real-time interface with field devices in the high voltage (HV) distribution network via the telemetry communications network. This is the core system that underpins the monitoring and control of the electrical distribution network.
Energy Workbench (EWB)	EWB is a data aggregation, customer and electrical network modelling platform used to support critical Network Planning activities including design scopes, network scenario modelling and forecasting for augmentation. It also underpins front-end applications including EDNAR (Electrical Distribution Network Access Register) and Network Viewer. By 2030, our networks are forecast to incur significant increases in residential solar PV connections, residential batteries, and electric vehicles. Energy Workbench was selected as the core technology to meet these new requirements and provide the required capability, with industry leading ‘whole of network’ modelling, allowing us to drill down into our network data and make targeted investment decisions.

Operating technology security integration platform (OTSIP)	A new OT integration service, OTSIP, will be implemented during 2024/25. The prior OT integration service was built on technology that was significantly aged, becoming increasingly less resilient and did not meet security requirements. The new integration service, as well as providing improved stability, delivers an improved security posture by being able to segregate OT systems and improve resilience and performance. Future OT initiatives will also benefit from this from a resilience, security and performance perspective once this platform is fully implemented.
Low Voltage Distributed Energy Resource Management (LV DERMS)	On 1 October 2024 the Victorian Government introduced a requirement to enable the remote disconnection of customer generation during minimum demand events. This is being enabled in new, upgraded or replacement rooftop solar systems. This change was introduced to ensure our customers can safety continue to install solar and greater levels of renewable energy will be available at other times, enabling our network to avoid large scale blackouts. This capability was enabled through implementation of our LV DERMS solution which is comprised of several systems. • Salesforce – our existing customer gateway service is used by solar installers for registration and testing of a device at a customer's premise. Currency of this system is covered by the Customer Enablement business case. • Scheduler - is the key interface to Salesforce providing the ability to issue controls to customer devices. • Utility Server – Is the secure communication platform between our systems monitoring and sending controls to customer devices. A connection between our Utility Server and the customer's premise can be direct to the inverter, via a gateway device, through an aggregator or a combination of the two.

TABLE 3 NETWORK GEOSPATIAL SYSTEMS

SYSTEM	DESCRIPTION
Geospatial Information System (GIS - (Electric Office)	GIS provides a spatial view and captures electricity asset information relating to the network. It also provides connectivity modelling across the electrical network for purposes of identifying customers that are affected by planned and unplanned outages.
GIS Connect - Smallworld business integrator	Provides synchronisation/enables mapping Smallworld products and Oracle. Both systems have their own way of defining data and geometry field types. Our IT architecture is based on Oracle. Our asset data is based on GE Smallworld. Provides a solution to make the Smallworld managed data available on Oracle database technology.

Network Viewer	Smallworld Network Viewer (NV) is utilised as the enterprise solution for Geospatial Network Visualisation based on Geographical Information System (GIS). The software is currently utilised by UE Service Delivery, UE Customer and Strategy group and external service provider, Zinfra.
Physical Network Inventory (PNI)	PNI provides a spatially based, end-to-end view of the network. This comprehensive and integrated view combines the fully connected inside and outside plant of the physical network with the ability to integrate logical inventory to deliver an integrated inventory capability. The underlying geospatial platform allows the user to understand where the network is and how it is connected.

TABLE 4 NETWORK REPORTING AND DATA PROCESSING SYSTEMS

SYSTEM	DESCRIPTION
Geospatial Analysis Warehouse (GSAW)	This software provides synchronisation/enables mapping between GE software products and Oracle. Both systems have their own way of defining data and geometry field types. Our IT architecture is based on Oracle. Our asset data is based on Smallworld GIS. GSAW provides a solution to make the Smallworld GIS managed data available on Oracle database technology. GSAW replaced existing technology called ‘SWEG’[2].

[2] SWEG – Smallworld Enterprise Gateway

Network Analytics Platforms	The platforms consume and review near real-time data from electricity meters and multiple other systems across the distribution network and translates the data into an information asset which drives improvements in network reliability, network safety and operational efficiencies.
Outages and Emergencies Suite	A collection of systems which assist in the effectively manage escalation events through the provision of communications, reporting and dashboards. Data derived from the network management core systems is utilised for operational and management reporting around reliability performance. This also informs any supply reliability or restoration compensation awarded to customers who have incurred outages above set regulatory thresholds for outage frequencies and durations over a 12-month period.

2.1 Value provided by network management systems

Our network management tools support the control and monitoring of customers' supply reliability and network performance while maintaining regulatory compliance. They also provide tools to ensure network, employee and public safety is maintained. They have a significant impact on our ability to manage safety events as well as proactively identifying potential safety issues before they occur, so that rectification work can be undertaken. Our customers expect us to continue to provide a safe, dependable, flexible and affordable supply of electricity.

2.1.1 Safety event management

Our AMDS supports the management of safety events. When a customer calls our Contact Centre, to report a safety event (e.g. wire down, leaning pole) a ticket will be raised in AMDS. Public safety faults are considered a priority, and through the ADMS our field crew engineers will be promptly dispatched to attend. Generally, the issue will be addressed on site. As safety is always our paramount concern, in some cases it may be necessary for the premise to be taken off supply until rectification can occur.

2.1.2 Proactive identification of safety issues

With the support of our network management systems, the incidence of electric shocks reported by customers has steadily reduced in recent years. Our customers have an electricity service line (overhead or underground) that runs from the street to their property. Traditionally based on regulations[3], these lines have been inspected every ten years. In 2020 Sensor IQ (SIQ) was implemented and has been used to identify power variations in the supply to customer premises. The power quality data obtained by SIQ has been used to show voltage variations and impedance in the supply to customer premises outside acceptable safety tolerance limits (standard 240 volts at the customer's point of supply).

We are constantly looking for new ways to utilise our network management systems to improve safety outcomes. By developing new algorithms which utilise power quality from AMI data we have been able to identify potential safety hazards and imminent asset failures, enabling us to improved safety outcomes for our customers. As an example, in late 2020 we implemented new algorithms which utilise power quality data from AMI meters and SIQ to detect and rectify neutral faults. This has

[3] Electricity Safety (Network Asset) Regulations, administered by Energy Safe Victoria.

resulted in a downward trend in the number of electric shocks reported as the faults are proactively identified and rectified before a customer is impacted.

2.1.3 Network reliability

Our customers have told us they want a safe and reliable supply of electricity. This is the essence of network management systems. Our network management tools support the control and monitoring of customers' supply reliability and network performance.

Our network management systems allow us to efficiently manage a network of over 13,000 kilometres of power lines. We distribute electricity to more than 700,000 customers with greater than 99.99% reliability. We are proud of this result and will continue to invest in our network management systems both to maintain and improve our service delivery.

Supporting network reliability, our IT disaster recovery strategy has identified that in the event of system failure, the following applications have very high priority for restoration across the business:

- ADMS - manages planned and unplanned network outages and is the key source of outage information provided to customers
- GIS - provides a spatial view of electricity asset information, relating to the network and connectivity modelling that is used for the purpose of identifying customers affected by an outage.

As an indication of the significance these applications have in supporting continued business operations, the maximum period of tolerable disruption before severe business, network, or customer impact occurs is 24 hours, and the recovery time objective is 12 hours.

2.1.4 Meeting regulatory obligations

To meet our customers' expectations of dependable, flexible and affordable electricity, as an electricity distributor we are required to ensure reliable electricity supply in accordance with:

- the Essential Services Commission's Distribution Code[4]
- the Australian Energy Market Commission's (AEMC) National Electricity Rules (Rules)[5]
- the AEMC's national electricity objective.[6]

The Essential Services Commission (ESC) establishes and maintains the Distribution Code of Practice[7] which outlines the rules relating to the distribution of electricity Victoria. The code regulates distributing and connecting electricity to consumers so that it is undertaken in a safe, efficient and reliable manner. As an electricity distributor in the National Electricity Market (NEM), we are required to ensure compliance with the code. This includes meeting our obligations around planned and unplanned interruptions of electricity, the disconnection of electricity to customers and the disconnection or interruption of supply to life support customers. Our Network Management systems support the management of these functions. Further detail on the sections of the code which are supported by our Network Management Systems are provided in Appendix A.

---

4 Essential Services Commission, Electricity Distribution Code of Practice, version 2, May 2023. Electricity Distribution Code of Practice | Essential Services Commission

5 Australian Energy Market Commission, National Electricity Rules, version 211, June 2024.

6 Australian Energy Market Commission, The National Electricity Objective (NEO)

7 Commonly referred to as the Code.

The reliability of our network management systems is critical to support our business so that we can continue to meet these obligations. This reliability depends on us maintaining currency of the systems through the application of upgrades, refreshes, patches or maintenance releases as necessary.

Maintaining currency of our network management systems will continue to underpin our ability to satisfy key regulatory obligations including:

- providing performance data in regard to the STPIS so this can be reported to the AER.
- management of GSL associated with supply reliability and supply restoration.
- notification of planned outages to customers within a prescribed period of 4 business days in accordance with the Distribution Code.
- Ensuring currency of our network management systems will ensure we can continue to meet our regulatory obligations in relation to network safety and reliability outcomes and information reporting.

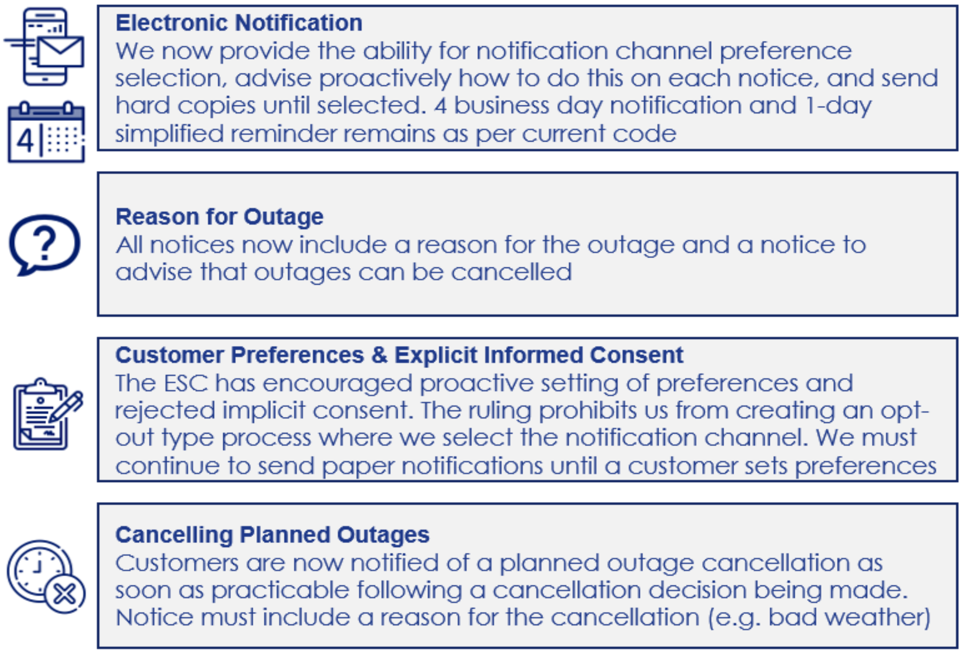
Case Study

Ensuring currency of our network management systems provides the flexibility to adapt to regulatory changes in the market. As an example, recent changes by the ESC[8] to the Electricity Distribution Code required us to alter the way we engage with customers before and during planned outages.

In response, the changes shown below were completed and compliance was assured. If these changes had not been made, significant compliance fines could have been rendered. The system impacts were identified and implemented in late 2021, thereby ensuring compliance with our regulatory obligations.

[8] ESC - Essential Services Commission

FIGURE 1 CHANGES IMPLEMENTED TO ENSURE COMPLIANCE



2.1.5 Enabling customer energy resource integration

We have a responsibility to all our customers to ensure roof top solar and other consumer energy resources (CER) can be safely integrated into our electricity network. Our challenge is to make sure that while accommodating excess energy from rooftop solar, we continue to provide the high standards of reliability and power quality all our customers expect.

Over recent years we have implemented changes in our network management systems aimed at supporting the connection of renewable energy. These systems assist by providing insights and recommendations to improve management of the network. Network planning engineers determine the capacity for additional CER integration using these tools while still managing minimum demand. The network management systems are vital to this process include the geographic information system, energy work bench and data analytics platforms.

2.1.6 Delivering incremental functionality and technical improvements

The application of software upgrades provided by the vendor has delivered new and improved functionality while addressing existing issues. These changes to the core software are provided as part of the standard software purchase and are distinct from market driven enhancements requested to meet non-recurrent requirements. Examples of new functionality delivered to Network Management Systems by the vendor during recent upgrades to core software are provided in Appendix B.

Within a software upgrade package, the vendor may also provide technical improvements relating to performance, security or traceability.

TABLE 5 TECHNICAL IMPROVEMENTS

IMPROVEMENT TYPE	DESCRIPTION
Performance	An upgrade can result in an improvement to the background processing of a transaction resulting in reduced wait time for the end user.

Security	Security patches are generally provided with a software upgrade to reduce vulnerabilities and minimise the risk of a data breach.
Traceability	Increased traceability of transactions to assist with audit processes, prevent fraud and minimise risk.

Examples of technical improvements delivered to Network Management Systems by the vendor during recent upgrades to core software are provided in Appendix C.

3. Identified need

As an electricity distributor, our customers expect us to continue to provide safe, dependable, flexible and affordable electricity supply while maintaining regulatory compliance. We continue to invest significantly in the development and maintenance of our network management systems to ensure we can maintain a high level of service.

Maintaining currency through software upgrades ensures that we receive the latest version of the software as provided by the vendor. The latest version of the system is effectively under warranty by the vendor, which means they have responsibility for fixing issues in a timely manner. As a result, there is less disruption to the reliability of our systems, and hence the reliability and safety of our customers' electricity supply is maintained. If our network management systems were to fall out of vendor support, they would no longer be covered by vendor warranty support. Should a failure occur in one of our network management systems, we would not be able to guarantee a safe and reliable supply of electricity to our customers or the safety of our electrical workers.

During the 2026-2031 regulatory period, the existing versions of our network management systems will require upgrades, refreshes, maintenance releases and patching to ensure currency.

Failure to maintain the currency of our network management systems could result in:

- lost management of the electrical distribution network impacting supply reliability
- significant increases to supply restoration times
- an increased safety risk to our workforce
- an inability to effectively and safely perform planned maintenance work
- missed guaranteed service levels to our customers
- the Essential Services Commission (ESC) issuing energy industry penalty notices (EIPNs) due to non-compliance with the Distribution Code of Practice, EIPNs commencing from $39,518 per instance.[9]

[9] Refer to Appendix A for further information.

4. Option analysis

We have considered three options to ensure currency of our network management systems:

1. **do not maintain currency** – under this option we would not apply any updates to our systems over the 2026–31 regulatory period
2. **maintain currency** – under this option we would undertake prudent upgrades to maintain minimum core currency
3. **maintain currency with more frequent upgrades** – under this option we would perform all upgrades as recommended and released by the vendor.

The costs and associated net present value of each of the options is presented in Table 6, and set out in further detail in our attached NMS cost and risk models.[10]

TABLE 6 OPTIONS ANALYSIS SUMMARY ($M, 2026)

OPTION		CAPEX	OPEX	NPV
1	Do not maintain currency	-	1.9	-
2	Maintain currency	53.7	-	26.7
3	Maintain currency with more frequent upgrades	63.1	-	21.8

4.1 Risk monetisation framework

To assess our investment options, we worked with EY to develop an ICT risk monetisation framework. This provides a standardised approach for identifying, classifying, and quantifying risks associated with potential IT investments.

The framework aims to support value-based decision making by translating risks into monetised values, facilitating consistent evaluation of cost-benefit analyses across potential investment scenarios.

Figure 2 sets out the steps we have taken to quantify risks associated with this business case. Further information on each of these steps is included in the risk monetisation framework attachment.

[10] UE MOD 7.09 - Network management systems cost - Jan2025 - Public; UE MOD 7.10 - Network management systems risk - Jan2025 - Public

FIGURE 2 RISK MONETISATION STEPS

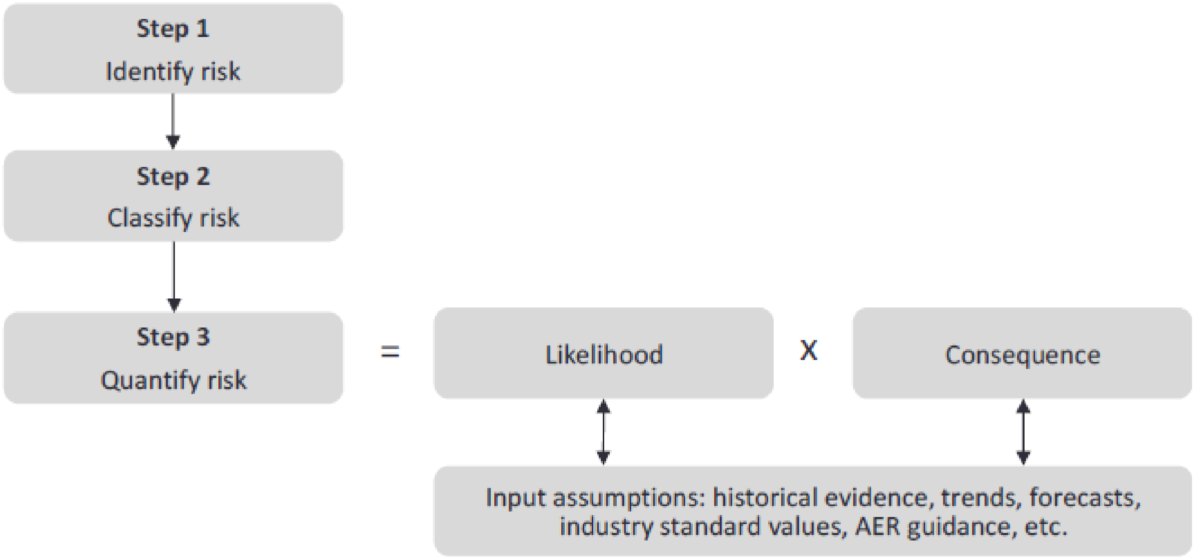


Table 7 provides a summary of each risk category included in our risk monetisation framework, which is itself attached with our regulatory proposal.[11]

TABLE 7 RISK FRAMEWORK SUMMARY

CATEGORY	DESCRIPTION
Reliability	Risks related to events or failures that cause unforeseen impacts to electricity supply or export capability. For example, customer supply or solar export
Compliance	Risks of regulatory, legal, or financial penalties due to failure in meeting compliance obligations, such as delays in publishing key market data or unauthorised access to sensitive data
Bushfire	Risks that outages of critical operational systems may increase bushfire likelihood by impairing visibility of the network and timely decision-making
Safety	Risks affecting public and staff safety, such as loss of supply impacting life-support customers or disruptions to protective systems
Customer experience	Risks where customer interactions are impacted, such as outages of customer-facing IT systems
IT outage	Risks of systems becoming unavailable due to poor infrastructure maintenance or resource constraints, resulting in prolonged downtimes or outages

[11] UE ATT 7.02 - EY - IT risk monetisation framework - Jan2025 - Public

Suitability and sustainability	Risks arising from legacy systems that are prone to failures, inefficiencies, and incompatibilities. These systems may lead to increased maintenance costs, failures, and cyber vulnerabilities if not updated

For each risk identified in the table above we have developed a list of sub-category risks. Each of these sub-category risks is set out in our framework alongside methodologies explaining how each of these risks are quantified.

For this business case key quantified risks relate to:

- reliability
- compliance
- safety
- IT outage, and
- IT suitability and system sustainability.

4.2 Option one: do not maintain currency

Under this option, software currency updates provided by the software vendor would not actively be applied. The software would become of out of date and consequently at a higher risk of failure

Software vendors recommend that we refresh and upgrade software to the latest version upon release. They rarely invest in previous software versions, and generally withdraw support beyond the published end of life support date. When we do not maintain currency and perform the recommended refreshes, then we are not able to take advantage of defect fixes and new functionality. Being on an older software version can restrict our ability to perform necessary upgrades to other systems and inhibits our ability to meet changing industry requirements such as those around CER.

Under this option we would be required to enter an extended vendor support arrangement which carries additional vendor support and maintenance charges. As time progresses and software currency has not been maintained, there is an increasing risk of a critical software event failure resulting in supply interruptions, safety risks and non-compliance. It should be noted that reliance on the provision of extended support for Network Management Systems carries a risk which cannot be mitigated if the vendor chooses to withdraw this arrangement.

Should a high severity IT system failure occur, this could prevent us from effectively operating the network for the duration of the IT system failure. For example, a SCADA system failure would cause a loss of visibility of the operational status of the electricity network. In this case, we would not be able to perform remote switching to facilitate supply restoration and would need to locate an authorised field crew member to attend the fault site to patrol, detect and manually operate switches to safely isolate and restore supply. All of this would have an impact on customers.

Currently FDIR[12] functionality within the ADMS will automatically switch the network to restore as many customers as possible in a matter of seconds. If this functionality was not available, the period a customer is off supply could increase to be several hours. Any network interruptions during the period of the software failure would only become apparent through customer reports into our Contact Centre. We would need to invoke manual procedures across the Contact Centre, Dispatch and Field Crews for customer reported faults and emergencies. The ability to respond and restore supply in a coordinated manner would be severely hindered. Planned work would also be significantly impacted as centralised visibility of the network activity would be unavailable.

In order to resolve the software failure, the vendor would be engaged to provide support to rectify the issue. Additional charges for labour would be rendered to develop work arounds or resolve the software issue. The timeframe and cost to resolve would depend upon the underlying issue and work required to resolve. The vendor may charge a higher rate to dedicate resources for emergency support rectification.

Trying to support technology which has become old and out of vendor support also leads to increased costs, which very quickly exceed the cost to invest in an upgraded system. Increased costs include:

- Higher support and maintenance charges from the vendor.
- Higher labour costs to develop work arounds and develop fixes.
- Higher vendor charges for emergency support for rectification and to restore our systems to a supported version.

---

[12] Fault Detection Isolation Restoration

Any subsequent upgrades would be more significant, and at greater cost than if currency had been maintained. In not actively maintaining the health of our network systems, this option prioritises the avoidance of capital expenditure over risks to electricity supply reliability, the safety of customers and electrical workers and regulatory compliance. This option carries a high risk of the Network Management Systems developing issues that cannot be rectified (or rectified in a timely way).

The table below summaries an assessment of option one against our key risk criteria.

TABLE 8 OPTION ONE RISK SUMMARY

#	RISK	DESCRIPTION
1	Reliability	When the currency of core network management systems has not been maintained and an extended vendor support arrangement is in place, this introduces a significant risk to running the electricity network. A high severity failure of a critical system such as SCADA would compromise our ability to monitor and manage the network to deliver a safe and reliable supply of electricity. If there was an event on the electricity network during this period, then there would be a significant risk of being unable to effectively respond and restore supply to customers in a safe and timely manner. We rely on SCADA/DMS to help automatically diagnose/rectify faults, and to remotely switch customers to different feeders so that supply reliability can be restored. A failure of the Network Management Systems would render us unable to: • Monitor and control the electricity distribution network and ensure continuity of supply. • Retrieve real time data from field devices to enable informed operational decision making and control. • Plan and conduct preventative system maintenance to avoid future unplanned outages to customers. • Provide timely and effective outage information to customers.
2	Compliance	This option has a high risk of regulatory compliance breaches and associated financial penalties. For example, not maintaining system currency would render us unable to maintain compliance with changes to the ESC Distribution Code of Practice within required timeframes. As a result of regulatory non-compliance, financial penalties associated with EIPNs[13] would be rendered causing reputational damage to our business. Regulatory reporting for SAIDI and SAIFI would also be impacted.
3	Bushfire	If the ADMS system was unavailable, the Rapid Earth Fault Current Limited (REFCL) technology, would not automatically activate, thereby increasing the risk of a fallen power line causing a bushfire during Summer.

[13] EIPN – Energy Industry Penalty Notice

4	Safety	System outages would delay our ability to respond to electrical faults which have a public safety risk. Unless customer-reported faults were called through, we could not immediately identify network impacts. This would result in a delayed response and extension of public safety exposure. In the event of a system failure, we would lose visibility of life support customer locations in relation to the electricity supply assets. We would also lose the ability to use this information to prevent outages, prioritise supply restoration or provide communications. If system currency was not maintained, we would be unable to develop new algorithms which use AMI data to identify and address potential safety risks on the network.
5	Customer experience risk	System failures or defects occurring when the software is out of support would result in a disruption to our business operations and could result in customers being unable to receive services including: • planned outage notifications. • unplanned outage restoration and updates. • remote energisation and de-energisation of customer premises. When we are unable to restore power to customers in a timely manner a prolonged supply outage will result in a negative customer experience. If our analytics platforms were unavailable, we would be unable to investigate customer queries or complaints around quality of supply and reliability.
6	IT system outage	Increased NMS outages are likely to impact internal productivity as employees that utilise these systems are unable to effectively undertake their responsibilities. This could result in employees being unable to undertake their tasks or a reversion to manual processes that are significantly slower. In addition, more frequent outages due to a lack of upgrades would require additional rectification work to repair the systems when they suffer outages.
7	IT suitability and system sustainability	Not maintaining software currency makes difficult to apply changes to adapt to the emerging requirements to support CER integration and NEM reforms. Vendors usually will not develop code changes on old unsupported versions of software. If they do, implementation of the required changes on old, out of date software leads to increased costs, which can quickly exceed the cost to invest in an upgraded system. This would decrease the suitability and sustainability of our systems.

The table below sets out the expenditure associated with option one.

TABLE 9 OPTION ONE EXPENDITURE FORECAST ($M, 2026)

OPTION ONE	FY27	FY28	FY29	FY30	FY31	TOTAL
United Energy	0.3	0.3	0.4	0.4	0.5	1.9

4.3 Option two: maintain currency

Under this option we would perform prudent technical upgrades to maintain minimum core system currency. Maintaining prudent currency of our Network management Systems will deliver a fully supported platform which will maintain our level of security, performance and stability. The software warranty is protected and vendor support/maintenance is assured.

Through the application of technical software upgrades, application support teams will have access to improved performance tools and additional system health checks. Software faults and bugs will be rectified by the vendor resulting in reduced disruption to our business units.

From a security perspective, this option will maintain current security posture of the Network Management Systems and reduce the risk of a breach by ensuring all patches are applied and known vulnerabilities are remediated.

It also enables continued regulatory compliance with current requirements while maintaining reliability and safety of the electricity network. By maintaining compliance with the ESC Distribution Code of Practice our reputation is maintain while fines associated with non-compliance are avoided.

Option two maintains our ability to effectively monitor and manage the network. This option entails a rolling refresh program of the network management systems spread over the five-year regulatory reset period. By performing regular system upgrades we avoid high remediation costs in the future and likely reduce the required investment to upgrade or replace our systems in the future. The lower cost of this option when compared to option three strikes an appropriate balance between risk and cost.

Ensuring currency of our network management systems will also:

- maintain the quality, reliability and security of the distribution system to achieve operational requirements and power quality standards.
- ensure we can continue to provide a centralised and automated supply isolation and restoration approach in response to high voltage faults detected, which in turn limits the number of customers impacted by an outage and the duration of the outage.
- provide customers with relevant and timely information regarding interruptions to supply.
- maintain the safety of the distribution system through the real-time monitoring of network status and field activities on the network.
- be proactive in the identification and resolution of issues to keep our customers safe, including enabling us to develop algorithms using AMI data which better detect safety risks on our network.
- avoid unsupported or end-of-life systems that cannot be modified to meet operational and/or regulatory requirements such as the Distribution Code. Refer to Appendix A for further details.

The benefits of this approach include:

- software defects are resolved with the new release.
- The development of new algorithms to identify safety risks on the network
- hardware compatibility with newer software versions

Our expenditure forecast for option two reflects the efficient cost of refreshing our IT systems:

- our timing profile is based on prudent and timely investments aligned with roughly every second vendor product release to ensure we remain within vendor support.
- our forecast cost per refresh is based on previous refresh costs incurred in 2021-2026 as well as projected infrastructure hardware replacement cycles.

This option maintains prudent currency of the core Network Management Systems, applying upgrades when deemed necessary, whilst delaying upgrades wherever possible, taking into account:

- the number and nature of software defects resolved with the new release.
- the end-of-life status of the current software version.
- hardware compatibility with the newer software version (i.e., if a new release requires additional expenditure to ensure a compatible database).
- the degree to which all of the above relate to regulatory compliance.

The table below summarises an assessment of option two against our key risk criteria. While the risk of a system issue arising is not eliminated, when compared to option one, there is a reduced risk of system issues arising and therefore impacting our key risks.

TABLE 10 OPTION TWO RISK SUMMARY

#	SYSTEM	DESCRIPTION
1	Reliability	By continuing to invest in reliable, stable and tested solutions we maintain supportable technology platforms to manage the electrical distribution network so that reliability and safety can be maintained. The risk of not being able to effectively respond and restore supply to customers in a safe and timely manner is reduced when compared to option one. Our network management systems enable automatic identification of outages and prompt rectification. We can also manage the network in a way which enables alternative supply sources and therefore can avoid some supply outages. They also enable identification of preventative system maintenance which avoids future unplanned outages. There would also be a decreased risk of delays to supply restoration.
2	Compliance	Maintaining system currency of network management systems means that when new regulatory compliance changes are defined, we can identify the system changes needed and request these from the software vendor. The risk of a system issue preventing generation of SAIDI and SAFI regulatory reporting is also reduced. We can also continue to provide timely and effective advice around planned and unplanned outages in line with the ESC Distribution Code of Practice.
3	Bushfire	Ensuring currency and stability of the ADMS system reduces the risk of system issues and functionality such as REFCL being unavailable.
4	Safety	Our ability to respond to electrical faults and reduce public safety risk in a timely manner is reduced in Option two as it has a lower risk of system outages or issues. Availability of our network management systems will ensure life support customers can be identified so that outages can be prevented, or restoration prioritised while communicating updates to the customer. Safety risks can be reduced through the development of algorithms to identity issues and subsequent action to address the cause.

5	Customer experience risk	The risk of disruption to our business operations and customer services would be reduced under this option when compared to option one.
6	IT system outage	There is a decreased likelihood of system outages compared to option one reducing the impact of system outages on employee productivity. Rectification costs will also be lower due to a lower number of expected outages.
7	IT suitability and system sustainability	Changed or emerging business requirements such as CER or new NEM reforms can be met through vendor provided code changes when the software is on a supported version.

The table below sets out the expenditure associated with option two.

TABLE 11 OPTION TWO EXPENDITURE FORECAST ($M, 2026)

OPTION TWO	FY27	FY28	FY29	FY30	FY31	TOTAL
United Energy	11.9	14.0	7.4	11.6	8.8	53.7

4.4 Option three: maintain currency with more frequent upgrades

Under this option we would maintain currency on all core network management systems applications by performing system upgrades as released and recommended by vendors. This option also maintains pace with the newest available versions, security, functionality and industry trends.

Applying software upgrades as released by the software vendors would deliver a fully supported platform which will provide an operational environment of greater security, performance and stability. A high level of system currency and compliance would be maintained. However, the full value of each upgrade may not be realised, and the resourcing load is high.

Applying the latest software version will provide earlier access to defect fixes, performance improvements and new functionality. However, when applying the latest upgrades there is also a greater likelihood of encountering unknown bugs or issues.

Similar to option two, ensuring software currency makes it easier to request and apply changes to adapt to the emerging requirements. For administration and financial reasons, vendors are reticent to make code changes to previous software versions. Client requested changes may only be available on the latest code base. Being on an older software version may require upgrades prior to installation of the requested change.

Performing vendor recommended software upgrades ensures we are on the latest product and security vulnerabilities are minimised.

Option three provides a small reduction of risk together with increased expenditure associated with more frequent application of upgrades, patching and maintenance. It also carries the following disadvantages:

- Cutting edge/untried software may introduce new technical defects.
- The pace of upgrades creates a high resource load and reduces the ability to complete targeted changes/improvements during the program of work.

Our expenditure forecast for Option three reflects the cost of refreshing our IT systems with the latest upgrades:

- Our timing profile is based on timely investment aligned with vendor product releases.
- Our forecast cost per refresh is based on historical refresh costs incurred in 2021-2026 as well as projected infrastructure hardware replacement cycles

The risk reductions associated with option two are also applicable to option three. However, the application of more frequent upgrades results in minor additional risk reductions as outlined in the table below.

TABLE 12 OPTION THREE RISK SUMMARY

#	SYSTEM	DESCRIPTION
1	Reliability	Through continuous investment in the latest software version, we may reduce the risk of an issue with availability of our NMS and in turn reduce risks associated with prompt identification and restoration of supply. We may reduce the risk of losing visibility, monitoring and control the electricity distribution network. It also may reduce the risk of losing functionality which: • Identifies supply alternatives to avoid outages. • Identifies where preventative maintenance can avoid a future outage. However, there is likely to be little, if any, further reduction in risk compared to option two.
2	Compliance	Being on the latest software version provided by the vendor reduces the risk of non-compliance with new requirements as the vendor will support the provision of code changes. Requests to the vendor to meet new compliance requirements are able to be developed and deployed straight away without the need to first upgrade to the latest software version. However, by deploying the latest upgrades there is a possibility that upgrades are not sufficiently debugged and will likely have a slightly higher risk of not meeting compliance obligations compared to option two.
3	Bushfire	Same as option two
4	Safety	Similar to option two, availability of our network management systems will ensure life support customers can be identified so that outages can be prevented, or restoration prioritised while communicating updates to the customer. Safety risks are reduced through the development of algorithms to identity issues and subsequent action to address the cause.
5	Customer experience risk	Similar to option two, will reduce the risk of system failures or defects with a flow on impact to business processes and customer services including: • Planned outage notifications. • Unplanned outage restoration and updates. • Remote energisation and de-energisation of customer's premise. • Prompt restoration of supply • Customer initiated investigations into quality of supply and reliability.
6	IT system Outage	The risk of a system outage is reduced further through more frequent application of vendor provided upgrades. As new security threats are identified, vendors will incorporate suitable barriers to cyber-attack within the latest software version. However, implementing vendor upgrades as they are released can result in additional outages as these upgrades have not been sufficiently debugged. This likely means limited additional risk reduction benefits compared to option two.

7	IT suitability and system sustainability	Similar to option two, being on the latest software version provided by the vendor reduces the risk of not being able to pivot to meet emerging customer or industry needs. The vendor will support the provision of code changes on the latest software version. Requests to the vendor to meet new requirements are able to be developed and deployed straight away without delays associated with upgrading to the latest software version.

The table below sets out the expenditure associated with option three.

TABLE 13 OPTION THREE EXPENDITURE FORECAST ($M, 2026)

OPTION THREE	FY27	FY28	FY29	FY30	FY31	TOTAL
United Energy	16.0	9.1	10.9	15.4	11.7	63.1

5. Recommendation

Following our option analysis, we recommend progressing option two – performing prudent technical upgrades which delivers the best value for our customers, maintains the health and currency of our network management systems, and enables continued regulatory compliance, network reliability and safety.

In line with our IT deliverability plan, our recommendation also considered a number of general factors (e.g. project concurrency, resource availability, etc.) to ensure that the option selected and upgrade timing was pragmatic, actionable, and would have the highest probability of delivering a successful outcome.

Our proposed expenditure profile is provided in Table 14.

TABLE 14 RECOMMENDED OPTION EXPENDITURE FORECAST ($M, 2026)

OPTION TWO	FY27	FY28	FY29	FY30	FY31	TOTAL
United Energy	11.9	14.0	7.4	11.6	8.8	53.7

A Delivering on regulatory requirements

The table below provides information on regulatory obligations and the Network Management Systems which enable compliance.

TABLE 15 COMPLIANCE WITH REGULATORY OBLIGATIONS

CLAUSE	OBLIGATION	OBLIGATION DESCRIPTION	NMS[14]	PENALTY
Distribution Code 11.3 [15]	Unplanned interruptions: customer communications	Provide information on unplanned outages on our website including the nature of the interruption and estimated time of restoration. Wherever reasonable and practicable, a distributor must provide prior information to customers who may be interrupted by load shedding.	DMS ADMS	EIPN min $39,518[16]
Distribution Code 11.4	Planned interruptions: customer communications	11.4.1 To enable customers to nominate a preferred methods of communication to receive notices about interruptions. 11.4.2 Record keeping requirements in relation to preferences and any update. 11.4.3 Requirements around planned interruption notices to customers – the methods and style of communication. Also around informing customers how to nominate or update their preferred communication method.	EDNAR	
Distribution Code 11.5	Planned interruption	11.5.1 In the event of a planned interruption we must provide at least 4 business days written notice by the customers chosen communication method. If the affected customer is a life support customer, the distributor must provide at least 4 days written notice unless the customer has requested a longer period of notice. We must provide a life support customer with written notice in addition to the customers preferred method of communication.	EDNAR	

14 Network Management Systems involved in delivery of the requirements.
15 Reference to the clause within the Electricity Distribution Code of Practice version 2, 1 May 2023.
16 Electricity Industry Penalty Notice (EIPN). Penalty taken from Essential Services Commission Act 2001, part 7, section 5T, notice penalties. ESSENTIAL SERVICES COMMISSION ACT 2001 - SECT 54T Notice penalties (austlii.edu.au). The notice penalty for a contravention of a civil penalty requirement by an energy licensee is generally 200 penalty units at a value of $197.59 = $39,518. Indexation of fees and penalties | Department of Treasury and Finance Victoria (dtf.vic.gov.au)

		11.5.2 The notice must specify the expected date, time and duration of the interruption. It must also include a 24-hour telephone number for fault enquiries and emergencies, the charge for which is no more than the cost of a local call for enquiries. The reason for the planned outage and potential for the interruption to be cancelled and rescheduled must also be provided. 11.5.3 A reminder must be sent one day prior to the planned interruption using the same method as the original notice. 11.5.4-8 If the customer has provided explicit informed consent to the interruption occurring between identified hours on a specified date then notice is not required. A customer can withdraw their consent at any time. A record of consent must be retained for at least two years and provide a copy to the customer if requested at no cost.	
Distribution Code 12	Life Support Equipment	When notified a Life Support Customer is residing at a supply address, within 1 business day the distributor must update system records and advise the retailer. Before 5 business days we must provide information to the customer, advise of their obligations and request a medical confirmation form. Where a retailer advises us of a life support customer, the requirements shown above still apply. There are also requirements around return of the medical confirmation, the provision of reminders and deregistration. We must not disconnect the supply address other than in the case of an interruption or emergency.	ADMS EDNAR
Distribution Code 13	Reliability Targets	Distributor Targets: Before 30 June each year the Distributor must public on its website the targets for reliability of supply for the following year. This includes SAIDI, SAIFI, MAIFI and CAIDI. This information must also be provided to a customer or retailer on request. Reliability of Supply: Outlines requirements of the Distributor in regard to the communication of supply reliability data.	ADMS DMS
Distribution Code 14	Guaranteed Service Levels	Minimum service levels must be met by Distributors in regard to minimum service levels to customers and payments must be made where those service levels are not met. It also defines eligibility and timeframes for	AMDS DMS

		payment. GSLs which the Network Management Systems are involved with are: Supply restoration & low reliability payments Major event day payments	
Distribution Code 18	Complaints and dispute resolution	A distributor must manage a complaint according to the Australian standard and include information about the process on our website. Complaints regarding supply reliability or supply quality must be managed in this way. Network Management Systems will be utilised to source underlying data to the complaint. For example, OMS would be utilised to confirm or deny a period of outage.	ADMS DMS SCADA Analytics Map Insights/ Network Viewer
Distribution Code 19	Asset Management & Planning	Obligations to develop and implement plans to ensure security and reliability of supply. In particular, requirements around assets and records of their location, condition and performance. GIS provides asset location data to systems which manage asset inspection, public lighting and vegetation management. This enables those systems to ensure maintenance can take place. GIS, SCADA and PRISM (relay settings) provides source data to enable the development of planning reports.	GIS SCADA PRISM Map Insights/Network Viewer SIQ OSI PI
Distribution Code 20	Quality of Supply	The obligations of a distributor in respect to maintaining quality of supply and when a distributor must compensate any person whose property is damaged due to excessive voltage variations. The requirements are defined in relation to supply frequency, voltage, power factor, harmonics, inductive interference, negative sequence voltage, load balance, disturbing supplies and monitoring quality of supply.	Analytics platform SIQ SCADA DMS EWB LV DERMS OSI PI

B Functional improvements delivered by maintaining currency

Examples of functional improvements delivered to the core software as part of a recent vendor upgrade are shown below.

TABLE 16 NEW FUNCTIONALITY

SYSTEM	FUNCTIONALITY DELIVERED
ADMS	The UE ADMS upgrade delivered the following: • Extended and more accurate Fault Location, Isolation and Service Restoration (FLISR) calculations to increase the automated restoration of service outages. • Probable fault location identification for outages, thus shortening sustained outage restoration time • System suggested switching steps for de-energising and re-energising a selected device, assisting Planners to generate HV and LV switching sheets • Enable Active Network Management Scheme capability to support contingent switching use cases (including protection of transformers via automated execution of predefined load shedding switching plans at peak thresholds and lower cost safer Anti Islanding scheme for 1-5MVA inverter-based generators).
Energy Workbench	A new capability to enable detailed forecasting and scenario modelling on network hosting capacity for Customer Energy Resources (CER) will be implemented by the end of the current EDPR period.

C Technical improvements delivered by maintaining currency

Examples of technical improvements delivered to the core software as part of a recent vendor upgrade are shown below.

TABLE 17 TECHNICAL IMPROVEMENTS

IMPROVEMENT CATEGORY	SYSTEM	IMPROVEMENT
Security	Network Viewer upgrade to v5.3	Penetration testing conducted in October 2021 revelated security vulnerabilities in the application. Upgrade of the software to version 5.3 addressed security risks and delivered performance, functional and long-term support benefits. The previous version of Network Viewer also exposed the business to lengthy outages impacting operational downtime and causing reputational damage due to known support and security risks. Upgrading to Network Viewer 5.3 series minimised the operational downtimes resulting in increased system availability and stability, favourably impacting user experience. The 5.3 series also enables ease of transition to future upgrades with options to introduce new functionality such as mobility tools for field engineers.
Performance	SCADA Modernisation	The SCADA to ADMS Interface was upgraded to increase the throughput of digital and analog SCADA data, so that data can be sent more efficiently from SCADA to ADMS. Deadbanding was also introduced to enable data updates over a certain percentage change threshold to be sent through to the ADMS, to stop the system being flooded with data updates.

For further information visit:

Unitedenergy.com.au

United Energy

United Energy

United Energy