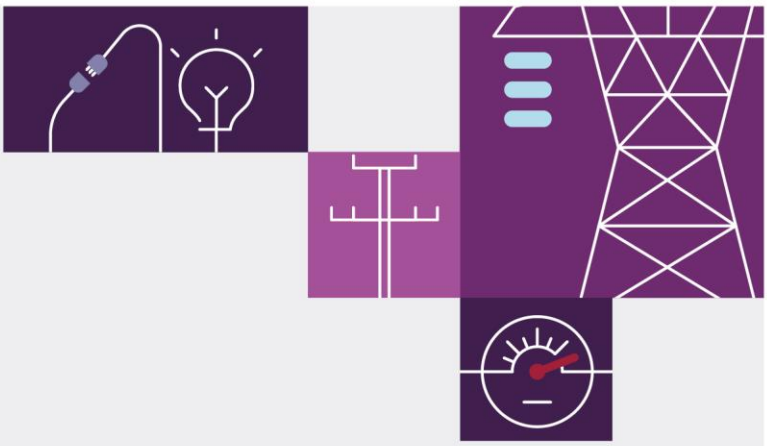
Multiple incidents impacting NEM SCADA between 24 January 2021 and 18 November 2023

March 2024

Reviewable Operating Incident Report under the National Electricity Rules



Important notice

Purpose

AEMO has prepared this report in accordance with clause 4.8.15(c) of the National Electricity Rules, using information available as at the date of publication, unless otherwise specified.

Disclaimer

To inform its review and the findings expressed in this report, AEMO has been provided with data by Registered Participants as to operational events and the performance of equipment and processes leading up to, during, and after the incidents described. In addition, AEMO has collated information from its own observations, records and systems. Any views expressed in this report may be based on information given to AEMO by other persons.

AEMO has made reasonable efforts to ensure the quality of the information in this report but cannot guarantee its accuracy or completeness.

Accordingly, to the maximum extent permitted by law, AEMO and its officers, employees and consultants involved in the preparation of this document:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability, or completeness of the information in this document; and
- are not liable (whether by reason of negligence or otherwise) for any statements or representations in this document, or any omissions from it, or for any use or reliance on the information in it.

Copyright

Contact

If you have any questions or comments in relation to this report, please contact AEMO at system.incident@aemo.com.au.

AEMO acknowledges the Traditional Owners of country throughout Australia and recognises their continuing connection to land, waters and culture. We pay respect to Elders past and present.

Abbreviations

Abbreviation	Term
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AEST	Australian Eastern Standard Time
AGC	Automatic Generation Control (EMS Functionality)
BESS	Battery Energy Storage System
DCF	Data Communications Facility
DCP	Data Communications Provider
DMS	Distribution Management System
DNSP	Distribution Network Service Provider
EMS	Energy Management System
GridNet	Wide Area Network managed by AEMO for SCADA data from Network Service Providers
ICCP	Inter-Control Centre Communications Protocol (also known as TASE.2 in Europe, an ISO Standard)
IT	Information Technology
KPI	Key Performance Indicator
NEM	National Electricity Market (eastern and southern states)
NEMOC	National Electricity Market Operations Committee
NER	National Electricity Rules
NMS	Network Management System (includes DMS and EMS)
NSP	Network Service Provider
OT	Operational Technology
PSDCS	Power System Data Communications Standard
SCADA	Supervisory Control and Data Acquisition
TNSP	Transmission Network Service Provider
WAN	Wide Area Network
WEM	Wholesale Electricity Market (WA)

Contents

1 Overview

This report relates to 18 SCADA incidents that occurred throughout the NEM between 24 January 2021 and 18 November 2023.

Given the significant impact SCADA incidents have on power system operation and security, AEMO has conducted a review under clause 4.8.15(a)(3) of the National Electricity Rules (NER)[1]. The review evaluated overall SCADA performance and compliance with relevant obligations[2], and investigated the potential for systemic issues of significance to the NEM. To support the investigation, AEMO also conducted a review of National Electricity Market (NEM) and Wholesale Electricity Market (WEM) Network Service Providers' (NSPs') SCADA systems, processes, resilience and supporting capabilities against industry best practice. This report includes a summary of that review's findings.

The findings and recommendations are informed by engagement with NEM and WEM NSPs and international system operators and input from AEMO's expert consultant, Power Systems Consultants (PSC).

The investigation has concluded that the primary contributors to incident occurrence and impact are:

- Processes, controls, training and monitoring (Processes).
- Response to incidents (Response).
- Incident reporting and follow up investigation (Investigation).
- Resilience and capabilities (Resilience).

AEMO considers that the recent trend of an increasing number and growing impact of SCADA incidents poses a significant and unacceptable risk to power system operations, and therefore makes eight key recommendations to address the most significant risks identified during the investigation.

Focused effort is required from AEMO, NSPs and participants to promptly act on these recommendations and significantly enhance overall SCADA system reliability and resilience.

The findings and recommendations from AEMO's review are summarised in Table 1 below[3].

Table 1 Summary of findings and recommendations

ID	Finding	Action/Recommendation
1	**Finding category – Multiple** AEMO identified areas for improvement for NSPs in the SCADA baseline questionnaire findings outlined in Section 7.2 of this report. AEMO also concluded that two incidents had significant delays in rectification due to the lack of available after-hours SCADA support. Effective after-hours support for SCADA and energy management	• AEMO will meet with each NSP individually by the end of Q2 2024 to share relevant SCADA questionnaire findings and identify areas for potential improvement. NSPs and AEMO will progress additional actions or recommendations identified during these discussions as appropriate. • At these meetings, AEMO will also confirm with NEM SCADA operators that existing after-hours support arrangements are aligned with meeting the requirements of the Power System Data Communication Standard (PSDCS).

[1] AEMO may review any power system events that it considers of significance to the operation of the power system, including recurring incidents of this type, consistent with the Reliability Panel Guidelines for identifying reviewable operating incidents, September 2022, paragraph 6(f). Available at https://www.aemc.gov.au/sites/default/files/2022-09/Final%20guidelines.pdf

[2] As such, the scope is focused on regional/NEM-wide SCADA, with issues relating to individual generators outside the scope of this review.

[3] As appropriate AEMO has omitted findings and recommendations with potential cyber security implications from this public report. These findings and recommendation will be monitored and progressed with affected parties directly.

ID	Finding	Action/Recommendation
	systems is critical to ensure service continuity and minimise outage durations. **Relevant findings: 7.2 and 9.2.3**	
2	**Finding category – Processes** AEMO has concluded that the majority of incidents were influenced by inadequacies in change management, processes and procedures, training, knowledge sharing, monitoring of SCADA operations, and overall situational awareness. Addressing these challenges necessitates a co-ordinated and continued effort between AEMO and NSPs to enhance SCADA system resilience and reliability. **Relevant findings: 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 9.3.1**	• AEMO will establish a SCADA working group with representatives from NEM and WEM NSPs, to report to the NEM Operations Committee (NEMOC). The group will be tasked with improving SCADA system resilience and reliability, across the NEM and WEM. The expected outcome is a measured reduction in SCADA outages. • The SCADA working group should be established by May 2024 and will initially meet monthly. The SCADA working group Terms of Reference (ToR) will be agreed by June 2024 and will include the following: – Ensure consistent understanding of SCADA requirements in the NER and the PSDCS, including recommending changes where appropriate. – Review of learnings from SCADA incidents (including incidents in which backup systems prevented an outage), causes, recommendations, and lessons learned. – Review of SCADA minutes lost monitoring and trends analysis. – Sharing of outcomes/learnings from backup/failover system testing completed by SCADA working group members. – Monitoring of NSP and AEMO ability to meet PSDCS requirements (including review of any proposed revisions or amendments to the PSDCS). – Continued support for the development of processes for notification of SCADA work to control rooms and AEMO. – Review and (if applicable) implementation of change management process improvements. – Monitoring of NSP and AEMO progress against identified improvement actions/initiatives related to strategic focus areas (see below). • NSPs and AEMO will undertake a comprehensive review of the following prioritised strategic focus areas and report the outcome to the SCADA working group by the end of August 2024: – Assessment of change management processes related to SCADA and identification of opportunities for improvements. – Review of existing root cause investigation frameworks and processes to confirm that investigation method has clear guiding principles and adaptable methodologies for analysis across different incidents and teams. – Assessment of policy and procedure management related to SCADA and identification of improvement opportunities. – Evaluation of capability to monitor and analyse SCADA system downtime (minutes lost) and identification of improvement opportunities. – Prioritisation of the identified opportunities for improvement and an indicative timeline for completion of any improvement actions. Ongoing progress of improvement actions/initiatives will be monitored via the SCADA working group. • The SCADA working group ToR will also include the following as future strategic focus areas for review: – Evaluation of staffing, including after-hours support, and training practices in alignment with the risk profile and compliance expectations in the PSDCS. – Evaluation of testing processes of backup facilities and redundant systems, improvements to sharing of testing results/findings with SCADA working group members, and testing guideline development. – Evaluation and improvement of incident management frameworks. – Evaluation of situational awareness capabilities and areas for improvement.

ID	Finding	Action/Recommendation
		– Evaluation of contingency analysis and power system security monitoring capabilities[4] at NSPs and identification of improvement opportunities. • The SCADA working group will assign accountable working group leaders for each prioritised strategic focus area (as required).
3	**Finding category – Processes** AEMO has concluded that in seven of the 18 incidents reviewed there was a lack of awareness in the AEMO and/or NSP control room(s) regarding planned SCADA system works. AEMO considers that had control rooms been aware of the planned work, SCADA could have been returned to normal service more promptly. **Relevant finding: 9.1.2**	• By the end of Q4 2024, AEMO, in consultation with NSPs, will establish a standardised process for the notification of planned works on NSP and AEMO SCADA systems. • To support this process, AEMO will create a set of guidelines which outline when and how NSPs and participants should notify AEMO of higher risk planned SCADA work.
4	**Finding category – Processes** AEMO has concluded that the predominant factor contributing to the loss of SCADA data to AEMO, in 16 of the 18 incidents reviewed, was the failure of redundant/backup systems. While this was not necessarily the root cause, in many cases if redundant/backup systems had responded in line with expectations, a full SCADA failure would have been avoided. This finding is consistent with observations from the international review, which suggested that while SCADA issues do occur, the effective operation of redundant/backup systems often prevented issues from escalating. **Relevant finding: 9.1.1**	NSPs and AEMO to review existing automated backup and failover system testing procedures and identify opportunities for improvements by the end of Q3 2024. *Note: AEMO has previously recommended NSPs undertake routine failover testing of their SCADA systems, in the published Victorian Market Suspension market event report[5].*
5	**Finding category – Processes** AEMO has concluded that six of the 18 SCADA failures investigated were caused by external telecommunications systems issues or internal network issues at the NSPs. The ability to monitor SCADA delivery and "downtime" from or by the NSPs is an important function. Early detection of "downtime" alerts the AEMO/NSP support teams that investigation and action is required. Similarly, collecting longer-term availability data allows AEMO to monitor long-term performance and compliance with the PSDCS. AEMO also concluded that five of the 18 SCADA failures investigated did not trigger alarms, with AEMO's or an NSP's control room manually identifying the SCADA issue. Early problem detection is key for swift resolution, and by employing a multi-faceted monitoring approach, the system's overall capacity to detect anomalies is significantly enhanced. Finally, AEMO identified two incidents that were likely, but not confirmed, to be caused by telecoms reliability issues. The lack of monitoring capability for these services can impact identification and resolution of the root-cause. **Relevant findings: 9.1.5, 9.2.1, 9.4.2**	• By the end of Q4 2024, AEMO and NSPs to complete a review of existing SCADA monitoring tools to ensure they are able to promptly identify "downtime" of SCADA services to AEMO at: – The telecommunications level (including telco WAN monitoring at the bearer and the application-level utilising dedicated tools (where possible)), – The network level, and – The SCADA application level. Monitoring should occur in real time and allow tracking of trends in historical data. • During the above review, AEMO and NSPs should: – Investigate and, wherever feasible, implement multiple and overlapping Energy Management System (EMS)/SCADA System monitoring capabilities. These should be deployed within and outside the EMS, including telco bearer monitoring, Inter-Control Centre Communications Protocol (ICCP) Application monitoring, "heart-beat" monitoring and "stale" SCADA data monitoring. – Where possible (and appropriate), consider adding alarms/alerts to monitoring systems to notify operators and support teams whenever "downtime" or other issues are detected. *Note: AEMO has previously recommended implementation of suitable alarms and heartbeat displays to alert operators in the published NSW market*

[4] Contingency analysis and system security monitoring capabilities encompass suites of tools and processes that enable operators to monitor the power system and maintain power system security.

[5] Please see https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-report-vic-market-suspension.pdf?la=en.

ID	Finding	Action/Recommendation
		suspension market event report and the total loss of NEM SCADA incident report[6].
6	**Finding category – Processes** This review identified a prevalent lack of familiarity with the PSDCS and its requirements among NSPs. AEMO concluded that in seven of the 18 incidents investigated there was a failure to comply with the applicable version of the standard. **Relevant finding: 9.1.6**	AEMO will address the lack of familiarity with the PSDCS and its requirements among NSPs via the SCADA working group and through the preparation and distribution of training material by Q3 2024.
7	**Finding category – Investigation** AEMO identified a notable deficiency and variation in the detail provided by NSPs and AEMO concerning the incidents. The issue was compounded by significant inconsistencies and variations in the timing, format, identification of root cause and level of detail in the reports submitted to AEMO. **Relevant findings: 9.1.6 and 9.3.1**	• By Q4 2024, the SCADA working group will review and update AEMO's proposed standard SCADA incident report information form. Once the proposed standard SCADA incident report information form is finalised by the working group, information related to any SCADA incidents should be recorded in the approved format to ensure consistency. • By Q4 2024, the SCADA working group to review the PSDCS and consider: – Inclusion of a template SCADA Incident Report information form (based on the agreed template above). – A requirement for NSPs to complete and submit the SCADA Incident Report information and root cause identification within 20 business days of the incident date (for incidents where the outage time exceeded the allowable time in the PSDCS). *Note: a 20-business day requirement would align SCADA incident investigation and reporting timeframes with the existing response timeframes under NER clause 4.8.15(g).* – In cases where a SCADA incident leads to a complete loss of data from a NSP or participants, mandate a comprehensive investigation to identify the causes and implement corrective actions within an agreed timeframe. – Whether any requirements outlined in the PSDCS should be reflected in the NER.
8	**Finding category – Resilience** AEMO identified during the review, and in discussions with international system operators, a significant dependence on third party telecommunications, suggesting the need to evaluate the advantages of implementing key AEMO-owned infrastructure for enhanced control and reliability. **Relevant findings: 9.4.1, 9.4.2, 9.4.3**	• By Q1 2025, AEMO and the transmission network service providers (TNSPs), distribution network service providers (DNSPs) and participants from which AEMO receives SCADA data should review their telecommunications systems and consider implementing changes (as required) to allow each entity to have a reliable, independent means of communication with AEMO in the event of a major network outage at their respective sites. • By the end of Q4 2024 AEMO to: – Investigate the communications connections between its New South Wales control room and Transgrid's network to provide alternative communication links for New South Wales region data. – Investigate the communications connections between its Queensland control room and Energy Queensland's network and onto Powerlink to provide alternative communication links for Queensland region data.

This report is prepared in accordance with clause 4.8.15(c) of the NER. It is based on information provided by AusNet, ElectraNet, Essential Energy, EVO Energy, Hydro Tasmania, Powercor, Powerlink, Transgrid, TasNetworks, and Western Power (WEM TNSP) and available through AEMO systems.

NEM time (Australian Eastern Standard Time [AEST]) is used throughout this report.

[6] Please see https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-suspension-nsw.pdf?la=en and https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/final-report-total-loss-of-nem-scada-data.pdf?la=en.

2 Acknowledgements

AEMO would like to acknowledge and thank all participants who made their staff available and who assisted with this review, notably AusNet, ElectraNet, Essential Energy, EVOenergy, Hydro Tasmania, Powercor, Powerlink, Transgrid, TasNetworks, and Western Power.

AEMO would also like to thank Power Systems Consultants (PSC), who assisted with the investigation, development of recommendations and reporting.

In addition, AEMO would like to acknowledge the time and contribution of the following international organisations: California independent System Operator, EirGrid, Electric Reliability Council of Texas (ERCOT), General Electric (Digital Grid), National Grid UK, 50Hertz, North American Electric Reliability Corporation (NERC)(documentation) and the Uptime Institute (documentation and reprinting of material).

3 Relevant systems and standards

The following section provides a contextual overview of the key systems and standards relevant to the operation of SCADA in the NEM.

3.1 SCADA systems

SCADA control systems are a specialised framework designed for monitoring and controlling an electrical grid. These systems play a crucial role in ensuring the stable and efficient flow of electricity across vast networks, from power generation sites to end users. By collecting real-time data from substations and transmission lines, a SCADA system allows operators to manage load distribution, detect and respond to faults, and maintain optimal operating conditions, thus ensuring the reliability and safety of the power transmission infrastructure.

SCADA systems are critical in the secure operation of power systems, providing control room operators with power system information. In the NEM, SCADA data points are sourced from field devices and input into operational systems for use by operational staff to monitor and control the electrical grid. Furthermore, SCADA data feeds into and enables the operation of power flow state estimation and subsequent real-time contingency analysis used to manage power system security.

This SCADA data is used to manage both power system security and the electricity market.

3.2 Energy Management System

The Energy Management System (EMS) is a suite of sophisticated analytical applications. The EMS provides analysis tools for AEMO control room staff to monitor and assess the status of the power system in real time, and in advance (based on forecasts), to help ensure the power system remains in a secure operating state. The EMS is critically dependent on SCADA data to update in a timely fashion and with the correct information, otherwise the information it displays and the advisory solutions it produces will not accurately represent the status of the power system. The EMS is also the primary source for real-time data for AEMO's Electricity Market Management Systems (MMS).

3.3 Electricity Market Management Systems

The Electricity MMS has a critical dependency on "dispatch data" from the EMS. Dispatch data includes interconnector line flows and all generation output. This data is an important input to central dispatch which occurs every 5 minutes and allows the MMS to automatically determine a security-constrained economic dispatch and issue dispatch instructions to participants in the NEM.

3.4 Power System Data Communications Standard

The AEMO Power System Data Communications Standard[7] (PSDCS) developed under clause 4.11.2(c) of the NER sets out the standards and protocols applicable to the recording, transmission or receipt of telemetered data required for the purposes of monitoring and managing central dispatch and power system security and reliability, including indications, signals, and instructions (Operational Data).

Naturally it is desirable to avoid SCADA outages and, where they do occur, to minimise their duration. The key relevant requirements of the PSDCS are:

- a Data Communication Provider (DCP) must rectify issues with the Data Communications Facility (DCF) promptly;
- DCFs must have sufficient redundant elements to reasonably satisfy the reliability requirements set out in the standard; and
- Operational Data outages must not exceed the limits summarised in Table 2.

Table 2 Maximum critical outage times for intervening facilities

Category of operational data	Max aggregate outage time in 12 month period	Max time per critical outage
Dispatch Data	2 hours	30 minutes
System Security Primary Data and System Security Secondary Data	6 hours	1 hour

Notes

- The current version of the PSDCS (version 3) was published on 24 November 2022 and became effective on 3 April 2023.
- One of the key changes to the PSDCS was to Table 5 and the reduction of the maximum time allowed for a critical outage of Intervening Facility Dispatch Data (as defined in the PSDCS) from 2 hours to 30 minutes.
- Incidents investigated as part of this review were assessed against the PSDCS applicable at the time of the incident. Version 3 of the PSDCS applied for incidents 10-18. Version 2 applied for the remainder.
- The PSDCS is a NEM standard. There is currently no equivalent standard for the WEM.

[7] For full details of the Power System Data Communication Standard please see https://aemo.com.au/-/media/files/electricity/nem/network_connections/transmission-and-distribution/aemo-standard-for-power-system-data-communications.pdf

4 Incidents investigated

Table 3 provides a summary of the incidents considered in this review.

Table 3 Incidents Investigated as part of this report

Date	ID	Region	Impact	Cause	Met the PSDCS?	Rectification
24 Jan 2021	1	NEM	Loss of AEMO SCADA in all regions. TNSPs managed system security. Initiated a review of the market suspension procedures.	Software bug in the AEMO SCADA EMS.	Yes (v2)	Vendor provided software patch applied to the EMS on 28/01/2021 (Brisbane) and 29/01/2021 (Sydney). For further details see AEMO published reviewable incident report[8].
16 Feb 2021	2	VIC	Loss of Ausnet SCADA in VIC. Loss of visibility for AEMO	Solid state drive runtime error.	Yes (v2)	The drives were not repairable or reusable. To restore service at the time of the incident the system was rebuilt with a combination of virtual machines and repurposed pre-production server. Subsequently due to the age of the servers, they were replaced. For further details see AEMO published reviewable incident report [9].
18 Feb 2022	3	SA	Loss of ElectraNet SCADA in SA. Loss of visibility for AEMO. Market suspension.	During decommissioning of ElectraNet communications equipment an ElectraNet contractor cut an in-service SCADA cable.	Yes (v2)	The severed cables were repaired and the in-service redundant communication cables re-routed away from the decommissioned plant. For further details see AEMO's published Market Event report[10].
1 Mar 2022	4	TAS	Loss of AEMO SCADA in TAS. TNSP managed system security and frequency. Market suspension.	Two separate civil works (one in Victoria and one in Tasmania) damaging Bass Strait fibre cables during their works.	No (v2)	Telstra repaired both cables. For further details see AEMO's published Market Event report[11].

[8] See https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/final-report-total-loss-of-nem-scada-data.pdf?la=en.

[9] See Section 9.1 at https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/final-report-total-loss-of-nem-scada-data.pdf?la=en.

[10] See https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2022/preliminary-report-sa-market-suspension-18-feb-2022.pdf?la=en.

[11] See https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2022/preliminary-report-tas-market-suspension.pdf?la=en.

Date	ID	Region	Impact	Cause	Met the PSDCS?	Rectification
5 Apr 2022	5	TAS	SCADA links from TAS Hydro to TasNetworks failed for 28 minutes. AEMO and TasNetworks could not monitor the status of individual units.	A known software issue at Hydro's end. The solution in place is for action to be taken by operators to restart a process – which did not occur in this instance.	Yes (v2)	If a similar issue should arise again, the on-shift controllers were advised of the restart process to resolve the issue expediently.
3 May 2022	6	VIC	Loss of SCADA from Powercor in VIC. Declared Transmission System Operator maintained visibility and assisted in coordinating system security.	Planned work affecting a single ICCP link, which inadvertently affected both links to AEMO.	Yes (v2)	Quarterly reboot of the ICCP servers in order to avoid any re-occurrence of this issue.
14 Sep 2022	7	NSW	Dispatch errors during planned SCADA work resulting in incorrect telemetry and subsequent dispatch errors.	Planned works on Transgrid SCADA front end processor	Yes (v2)	AEMO has investigated why AEMO was not advised of the SCADA work.
29 Oct 2022	8	NSW	Transgrid lost SCADA visibility for approximately 20 minutes. AEMO maintained visibility.	Failure of all Transgrid's online SCADA servers.	Yes (v2)	Bug fixes within the SCADA system were implemented and additional administrative controls put in place for the control room to detect and respond to this event should it reoccur.
17 Mar 2023	9	NSW	Loss of AEMO SCADA visibility in NSW TNSP maintained visibility Market suspension.	Transgrid planned activities on non-live SCADA system mistakenly applied to live SCADA system.	Yes (v2)	Transgrid has implemented changes which limit staff ability to navigate to the runtime (online editor) page when running model tests. Transgrid has added additional controls on access to the runtime (online editor) screens and additional displays to increase the operator's situational awareness of testing activities and possible ICCP failures. For further details see AEMO's published Market Event report 12.
22 Apr 2023	10	VIC	Loss of Ausnet SCADA in VIC. Loss of visibility for AEMO. Market suspension.	Communication lost when primary switch failed due to a firmware bug. The nature of the bug prevented failover to the secondary switch. Vendor patch applied to fix the bug.	No (v3)	Vendor provided patch applied to fix the bug. AusNet to undertake a broader review of the procedures relating to SCADA system operation and control to identify any additional controls to be implemented to improve reliability, availability and restoration times of SCADA services. For further details see AEMO's published Market Event report 13.
18 May 2023	11	SA	Loss of SA Region SCADA data due to connection issues and loss of ICCP.	AEMO's communications link between ElectraNet and Norwest suffered intermittent	Yes (v3)	Intermittent comms link problem with GridNet at the SA end. No root cause identified. The SA ICCP link to NOR resumed to be stable.

[12] See https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-suspension-nsw.pdf?la=en.

[13] See https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-report-vic-market-suspension.pdf?la=en.

Date	ID	Region	Impact	Cause	Met the PSDCS?	Rectification
				connection issues and ICCP was rejected by ElectraNet's system		
5 Jul 2023	12	VIC	Loss of Dispatch data for renewable generation in Western Vic.	While restarting the ICCP Services on Network Management System (NMS) the NMS Server, Primary and Secondary ICCP servers were not accepting connections from GE's NMS (VPN SCADA) servers.	No (v3)	Improve the process for Certificate Testing, including testing the new AEMO Certificates on both AEMO's and Powercor's Development Environments.
13 May 2023	13	NSW	Loss of Dispatch data for renewable generation in Western NSW and HVDC interconnector data	Core distribution switch configuration failure within the Port Macquarie data centre.	No (v3)	Following diagnostics, a further configuration change on the switch stack to further mitigate any risk was carried out without any impacts on 10 August 2023.
27 Jun 2023	14	AEMO	Loss of SCADA from Transgrid.	Both AEMO ICCP links via Optus to Transgrid failed.	Yes (v3)	Intermittent Optus comms link problem with GridNet to Transgrid. No root cause identified. The ICCP link to NOR resumed to be stable.
25 Oct 2023	15	AEMO	AGC Dispatch to generation in QLD impacted. Automatic frequency control could not be performed.	A new scripting tool / process was used to create input files used to build Powerlink's SCADA ICCP database. This process inadvertently misaligned the mapping for 81 SCADA ICCP points (out of 12000 points), most of them AGC controls.	No (v3)	Change management process identified for improvement.
8 Nov 2023	16	NSW	SCADA in Southern NSW, Sydney and parts of Northern NSW had failed. Energy Australia informed AEMO that Mt Piper units had lost AGC signal. Riverina BESS confirmed they lost AGC signal as well.	Network switch upgrade by Transgrid where there was a bug in the new firmware being installed.	Yes (v3)	Applied Vendor supplied patch to network switch for problem known to Vendor.
16 Nov 2023	17	NSW	Loss of data from EVOenergy (and also sub-transmission lines in parallel with interconnectors)	Internal network fault between their master station (SCADA) servers and their ADMS servers.	No (v3)	There was an internal network fault between their master station (SCADA) servers and their ADMS servers. Specific further actions not reported at the time of writing this report.
18 Nov 2023	18	TAS	SCADA issue effecting TAS generation resulting in violating raise and lower regulation constraint violations.	ICCP fail-over and delays investigating and rectifying the issue by HT.	No (v3)	Training refresher for involved technician and ongoing bi-weekly meetings with all on-call technicians. Review on-call documentation in regards to ICCP, update to be clear on primary vs secondary vs backup links where needed.

5 AEMO's risk management methodology

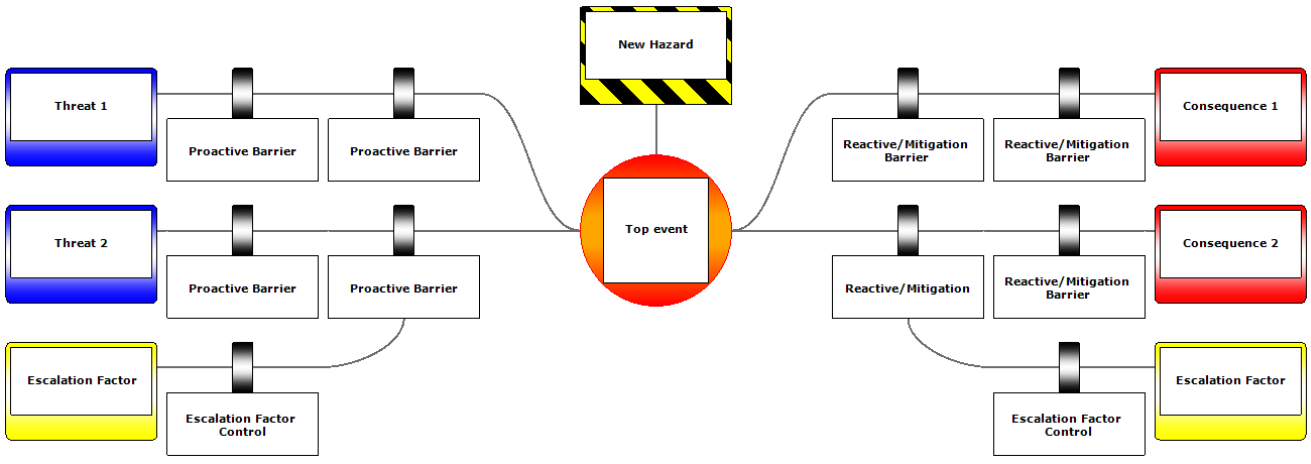
To effectively identify and manage risks associated with operating the power system, AEMO applies the principles of the AS/ISO 31000 risk management framework, undertakes root-cause analysis for major power system events, and has adopted the Bow-Tie risk assessment method, which has the following benefits:

- Provides a graphical representation of all aspects of risk.
- Is simple to understand and effective.
- Gives a logical, structured approach to risk management.
- Is increasingly seen as best practice, especially in high-risk industries.
- Allows interdependencies to be recognised and assessed (vertically and horizontally).

Figure 1 presents a diagram of the Bow-Tie risk assessment method. In the centre of the Bow-Tie is the hazard – hazards can be operations, activities or situations. A hazard has the potential to cause harm, but cannot do so as long as adequate controls are in place. When control of a hazard is lost, a normal situation changes to an abnormal situation. In the Bow-Tie, this event/change is called the top event and appears in the centre of the diagram. For example, a top event could be a frequency excursion on the power system. To the far left of the top event are the threats, the things that could cause a top event to occur. Between the top event and the threats are the proactive barrier controls (which prevent or reduce the likelihood that a threat will cause a top event).

Given that SCADA systems are critical for the safe and secure operation of the power system and operation of the NEM, a loss or impairment to SCADA would appear as a top event in the Bow-Tie risk assessment.

Figure 1 Bow-Tie risk evaluation diagram



6 Review methodology

The methodology undertaken for this review can be summarised below.

Initial incident analysis

Initial review of 18 incidents that occurred between 24 January 2021 and 30 November 2023. This involved an examination of each incident's investigation reports, findings, and the corrective actions taken. Where necessary, additional information was requested from relevant participants/NSPs to ensure a comprehensive understanding of each incident and its contributing factors.

Causal factor assessment

Each incident was assessed against a comprehensive set of potential contributing factors. A scoring system was applied to quantify the contribution of each factor, allowing for an aggregated analysis to identify any trends or themes among the incidents.

SCADA baseline questionnaire

A SCADA questionnaire was developed to audit various aspects of SCADA and EMS systems, server, and network environments. This questionnaire was distributed to NSPs within both the NEM and WEM, and to the relevant AEMO teams. The survey results allowed an understanding of the current state of SCADA systems across these SCADA operators.

Assessment of SCADA systems and capabilities against best practice

Building on the findings from the SCADA baseline questionnaire, the subsequent phase involved analysis and comparison against established best practices, based on PSC's experience of 29 years of SCADA and EMS design, deployment, configuration, and management for network service operators globally. The assessment also considered the outcomes of discussions with international operators. This comparison identified areas where SCADA systems aligned well with these best practices and areas where there was potential room for improvement. The results were then compared against the incidents and trends of contributing factors.

Review of International Incidents

AEMO conducted a targeted review of publicly reported SCADA incidents in the electricity sector, particularly focusing on occurrences in the UK/EU and North America.

Review of international SCADA standards and best practices

AEMO also conducted a review of available international standards and best practices in SCADA communications, including discussions with international system operators in the UK/EU and North American regions. This allowed for benchmarking against global norms and identifying areas for potential improvement in the NEM.

Development of findings and recommendations

AEMO considered the investigation results, incident trends and SCADA baseline questionnaire results to develop key findings and recommendations. AEMO then mapped its findings and recommendations to the SCADA failure Bow-Tie diagram shown in Figure 1 to identify any additional trends across different hazards. Finally, AEMO reviewed recommendations to ensure they sufficiently addressed the trends identified across the incidents and improvement identified from AEMO's international reviews.

7 Analysis

7.1 Incident and causal factor analysis

The initial step involved a comprehensive analysis of the 18 incidents included in this review. Each incident was evaluated against a broad set of criteria, composing various escalation factors, to gauge their respective impacts on the incidents as summarised in Table 4 below.

Table 4 SCADA incident contributing factors

Contributing Factor	Category
Dependence on 3rd party telecoms providers External factors outside AEMO/TNSP control	External
Training	People
Change Management Procedures Testing	Process
Backup/redundant system failure EMS/SCADA App environment Fault not alarmed/ Fault undetected ICCP IT environment (incl servers) Network environment	System
Vendor – EMS or Network equipment	Vendor

For each incident, each escalation factor was scored as follows:

- 0 = No contribution to the incident,
- 1 = Low contribution to the incident,
- 2 = Medium contribution to the incident,
- **3 = Significant contribution to the incident.**

The analysis identified that at least one of the top three escalation factors made a significant contribution to 17 of the 18 incidents assessed. In addition, the top eight escalation factors all had an average contribution to the 18 incidents reviewed above 0.5. This breakdown highlights the critical areas where improvements are likely to have the greatest impact on overall NEM SCADA reliability.

To aid with the assessment, incidents were classified as major where there was a NEM-wide loss of AEMO SCADA or a market suspension in a region of the NEM. All other incidents were classified as reviewable.

Table 5 below summarises the key factors which contributed to the 18 SCADA incidents investigated by AEMO.

Table 5 Incident analysis summary

Incident No	Incident classification	Region	Date	Company	Backup/redundant system failure	Procedures	Training	ICCP	Vendor - EMS or Network	Change Management	Dependence on 3rd party telecoms providers	Fault not alarmed	EMS/SCADA App environment	Fault undetected	Testing	Network environment	External factors outside AEMO/TNSP	Met the AEMO Standard for PS Data Comms	Applicable version of AEMO Standard for PS Data Comms
1	Major	NEM	24-Jan-21	AEMO	3	2	2	1	3			2		2				Yes	v2
2	Major	VIC	16-Feb-21	AusNet	3	2			3			2	1	1				Yes	v2
3	Major	SA	18-Feb-22	ElectraNet	3	3	3			2								Yes	v2
4	Major	TAS	1-Mar-22	AEMO	3			1			3						3	No	v2
5	Reviewable	TAS	5-Apr-22	Hydro Tasmania	3	2			3			1						Yes	v2
6	Reviewable	VIC	3-May-22	Powercor	3	1		3		2			2					Yes	v2
7	Reviewable	NSW	14-Sep-22	Transgrid		3	3			2		2		2				Yes	v2
8	Reviewable	NSW	29-Oct-22	Transgrid	3								3					Yes	v2
9	Major	NSW	17-Mar-23	Transgrid	3	3	2	1		2		1	2	1	1			Yes	v2
10	Major	VIC	22-Apr-23	AusNet	3	2			3	2		1		1	2	2		No	v3
11	Reviewable	SA	18-May-23	ElectraNet				3			3							Yes	v3
12	Reviewable	VIC	5-Jul-23	Powercor	3	3	3	3		2								No	v3
13	Reviewable	NSW	13-May-23	Essential Energy	3											3		No	v3
14	Reviewable	NEM (NSW)	27-Jun-23	AEMO	3			1			3					1	2	Yes	v3
15	Reviewable	NEM (QLD)	25-Oct-23	AEMO	3	2	3			1					3			No	v3

Incident No	Incident classification	Region	Date	Company	Backup/redundant system failure	Procedures	Training	ICCP	Vendor - EMS or Network	Change Management	Dependence on 3rd party telecoms providers	Fault not alarmed	EMS/SCADA App environment	Fault undetected	Testing	Network environment	External factors outside AEMO/TNSP	Met the AEMO Standard for PS Data Comms	Applicable version of AEMO Standard for PS Data Comms
16	Reviewable	NSW	8-Nov-23	Transgrid	3	1	1		3						1			Yes	v3
17	Reviewable	NSW(ACT)	16-Nov-23	EVO Energy	3			2			3							No	v3
18	Reviewable	TAS	18-Nov-23	Hydro Tas	3	2	2	3										No	v3
				Average	2.67	1.44	1.06	1.00	0.83	0.72	0.67	0.50	0.44	0.39	0.39	0.33	0.28		

7.2 SCADA baseline questionnaire analysis

The SCADA baseline questionnaire was distributed to NSPs responsible for the communication of SCADA dispatch data in the NEM or WEM, as well as AEMO[14]. Analysis of the questionnaire responses revealed a generally positive outlook on the state of SCADA capabilities with the majority of respondents indicating that their systems were well-managed and in alignment with industry best practice and expectations (based on PSC's experience of 29 years of SCADA and EMS design, deployment, configuration, and management for network service operators globally. The assessment also considered the outcomes of discussions with international operators). However, AEMO identified several potential opportunities for improvement.

7.2.1 SCADA and EMS

- **Aging software:** Three NSPs have SCADA/EMS software that is potentially lagging behind current versions with diminishing vendor support.
- **Testing limitations:** Two NSPs advised that their test or QA environments do not have a real-time SCADA feed, which limits the effectiveness of testing system changes.
- **Recovery time objective:** One NSP reported a recovery time objective in the case of loss of the primary site which AEMO considered excessively long. The NSP also indicated that the backup site is checked by their control room operators infrequently, although the systems are monitored continuously.
- **On-call support:** One NSP required a phone response from support staff that would likely make it challenging to meet the requirements of the PSDCS under certain conditions.

7.2.2 Server

- **Asset management:** One NSP does not have a comprehensive asset management system for their server infrastructure.
- **Pre-production environment:** One NSP does not have a pre-production environment that is an exact replica of production that changes pass through before the final step into production.
- **Hardware age:** Three NSPs reported SCADA or EMS server hardware that is currently likely outside of vendor warranty and support arrangements. Given the budget and timeframes required, planning for the replacement of older production hardware systems is strongly recommended.
- **Monitoring gaps:** Two NSPs did not have monitoring of downtime for server performance against the requirements of the PSDCS.

7.2.3 Network

- **Asset management:** One NSP did not respond as to whether they had a comprehensive asset management system for their network infrastructure.
- **Test environments:** Two NSPs did not have network test or QA environments.

[14] A high level summary of the questionnaire completed by NSPs and AEMO is included in Appendix A1

- **Remote access:** Two NSPs did not have remote access for network support personnel, although it is acknowledged this is a balance required between cyber security and response time considerations.
- **Monitoring gaps:** Two NSPs did not have monitoring of downtime for network performance against the requirements of the PSDCS.
- **After-hours support:** One NSP had no formal process for its network support team's response.

7.2.4 Procedures, training, resourcing

- **Unusual task management:** One NSP did not have a process or risk mitigation approach for infrequent or unusual tasks for which procedures do not exist.
- **Adherence to procedures:** One NSP reported there was not a strong adherence to procedures for routine tasks or the company did not undertake audits to validate the use of procedures and to reinforce the requirement.
- **Procedure gaps:** One NSP did not have procedures for the server team, and another did not have them for the network team.
- **AEMO standard:** For the majority of NSPs, the PSDCS has not been distributed to relevant staff nor the KPIs and implications explained.
- **Staffing:** One NSP reported its staffing levels were inadequate for ongoing daily activities.
- **Training and Skills:** Three NSPs indicated no formal training or induction program for new staff, nor verifying of staff competencies or the availability of a skills matrix or similar.
- **Knowledge sharing:** One NSP indicated that it did not foster knowledge sharing within its SCADA/EMS team. For the majority of NSPs, there is no knowledge sharing program or forums among industry peers.

8 International review

8.1 Reportable SCADA incidents

AEMO's review of international incidents found limited information related to SCADA failures. Most system operators maintain confidentiality, leading to limited availability of detailed reports in the public domain. AEMO did identify some major incidents which were reported publicly, but did not directly correlate with SCADA failures. However, AEMO identified in available incident reports that reduced situational awareness was a significant contributing factor. The reports confirmed that deficient situational awareness impacts system operators' ability to identify and respond effectively to power system incidents; this was also observed in the NEM incidents reviewed by AEMO. These observations reinforced that ensuring the accuracy, timeliness, and reliability of SCADA data is fundamental to maintaining high levels of situational awareness and effective power system management.

8.2 SCADA standards and best practice

It is common for system operators to maintain a wide range of detailed standards related to their management of assets and control of their power systems. Although detailed standards were found during the review for primary and secondary equipment, they were not found for their SCADA and communications systems specifically, at least in the public domain. The PSDCS was the only standard found that provided specific requirements to the performance and reliability of SCADA communications.

8.3 International system operator discussions

In discussions with international system operators and regulators, the key points discussed below were noted.

8.3.1 SCADA system redundancy and resilience

It was observed that while SCADA failures occur internationally, the impact of these events is often mitigated by the presence of robust redundancy/backup systems which successfully failover. These systems are designed to seamlessly failover to backup operations when needed, thereby preventing the escalation of an event into a more serious incident. Similar systems are in place in the NEM, however, in the majority of incidents investigated by AEMO, these redundant/backup systems failed to operate correctly and prevent complete SCADA failure or loss. Additionally, one international operator highlighted that the NSPs in its country have contingency analysis and basic power system security monitoring capabilities in their control rooms. This means that if the system operator experiences a SCADA failure NSPs can effectively take over management of system security in their regions.

8.3.2 Change management

A notable aspect of other system operators' practices was the rigorous change management processes implemented for their SCADA systems. These processes encompass the careful planning, testing, and deployment of changes to the SCADA systems, while ensuring continuous clear communication with all stakeholders and appropriate governance. Notably, change management and issues during or shortly after changes were identified as a contributing factor in many of the incidents reviewed by AEMO.

9 Findings

These findings are based on a detailed review and analysis of identified incidents, SCADA questionnaire responses, international review, and the experience of the SCADA/EMS professionals involved in the preparation of this report.

9.1 Processes, controls, training and monitoring

9.1.1 Automated backup site and system testing

AEMO has concluded that the predominant factor contributing to the loss of SCADA data to AEMO in 16 of the 18 incidents reviewed (incident 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18) was the failure of redundant systems. While this was not necessarily the root cause, in many cases if redundant systems had responded in line with expectations, a full SCADA failure would have been avoided. This finding is consistent with observations from the international review, which suggested that while SCADA issues do occur, the effective operation of system operators' redundant systems often prevented issues from escalating.

AEMO and NSPs are already performing failover tests, but there is a lack of requirements for reporting test outcomes, identifying deficiencies, and documenting corrective actions. As such, AEMO recommends the SCADA working group evaluates existing SCADA testing processes, develop testing guidelines and identify improvements to enable sharing of testing results/findings with SCADA working group members. In addition, AEMO recommends that SCADA operators conduct various non-standard automated failover tests to ensure that backup systems can operate under challenging conditions.

9.1.2 Change management and planned SCADA works

AEMO has concluded that in seven of the 18 incidents reviewed (incidents 3, 6, 7, 9, 10, 12, 15) there was a notable lack of awareness in the AEMO and/or NSP control rooms regarding planned work activities on the SCADA system. This lack of awareness contributed to delays in restoring SCADA to normal service, highlighting a gap in change management processes.

To mitigate this issue, it is essential that AEMO, NSPs and participants adopt comprehensive change management processes. These processes must ensure that changes to SCADA systems are documented and communicated thoroughly to internal teams , and to AEMO for significant changes. This will enhance overall situation awareness, allowing for more effective coordination and quicker resolution of potential issues.

AEMO EMS team's approach of obtaining formal permission to proceed and keeping the control room informed serves as a best practice model. This approach ensures the coordinated planning for system maintenance and updates, particularly for activities that could impact control room operations.

This finding aligns with the international review, in which system operators underscored the importance of robust change management processes and awareness of changes with control rooms to prevent and respond to SCADA incidents effectively.

9.1.3 Process, procedures, and training

AEMO has concluded that 12 of the 18 incidents reviewed (incidents 1, 2, 3, 5, 6, 7, 9, 10, 12, 15, 16, 18) were linked to personnel actions that deviated from, or occurred in the absence of, established processes. Specifically, four of these incidents were primarily due to procedural deviations, with an additional three where this was a contributing factor.

Operational technology systems, such as SCADA and EMS, are highly complex, necessitating significant investment in staff capability. Specialising team members in various aspects is crucial to ensure robust coverage and mitigate the reliance on key individuals. This specialisation must be underpinned by comprehensive training programs and clearly defined processes and procedures.

Regular maintenance and updates of policies and procedures is vital to minimise operational errors and risks. AEMO's practice of continually revising these policies, coupled with fostering a culture of strict adherence, sets a high standard for procedural compliance. AEMO’s approach to documentation management, ensuring a reliable audit trail for all procedures, serves as a best practice model that could be considered for other NSPs and participants.

In line with AEMO’s findings, the Uptime Institute’s outage analysis report has also highlighted that a significant proportion of data centre errors can be attributed to issues in process, procedures, and training. Further details of the Uptime Institute’s findings can be found in Appendix A2. This further underscores the critical importance of these areas in operational technology environments.

An integrated approach that includes effective training (identified as a major or contributing factor in 8 of the incidents), updated procedures, and comprehensive documentation management is key to enhancing operational reliability and effective risk management in SCADA and EMS operations.

9.1.4 Knowledge sharing on software vulnerabilities

AEMO has concluded that vendor software or firmware issues were related to five of the 18 incidents reviewed (incidents 1, 2, 5, 10, 16). Incidents were either precipitated by delayed software/firmware patch application or by the patches themselves causing issues. This highlights the need for improved knowledge sharing across NSPs and communication about potential vulnerabilities.

Therefore, AEMO recommends that NSPs and AEMO ensure that learnings from an incident handled and resolved by one team/company at one site should be shared across all teams at all sites via regular internal meetings and via the Power System Security Working Group and through the establishment of a SCADA working group.

9.1.5 SCADA outage monitoring and metrics

AEMO has concluded that six of the 18 of the incidents reviewed (incidents 4, 10, 11, 13, 14, 17) occurred as a result of either telco communication issues or internal network issues at the NSPs. In some of these incidents, identification of the SCADA issue relied on the relevant control room identifying slow or frozen SCADA and escalating to relevant SCADA teams. AEMO considers that robust, automated outage monitoring and alerting by both AEMO and the NSPs improves incident response and resolution times.

Early detection of “downtime” alerts the AEMO/NSP support teams that investigation and action is required. To support its processes AEMO monitors the long-term performance of systems and compliance with the PSDCS.

AEMO also monitors all Inter-Control Centre Communications Protocol (ICCP) links in real time in an independent system (PI) and has automated processes for capturing “Frozen data alarms” from all regions and producing automated monthly reports. The Frozen data alarm captures the loss of all data from the identified region/NSP or individual site. The review confirmed that the ability to monitor SCADA delivery and “downtime” from the NSPs is an important function.

9.1.6 Power System Data Communications Standard

AEMO has concluded that seven of the 18 incidents investigated (incidents 4, 10, 12, 13, 15, 17, 18) failed to comply with the applicable version of the PSDCS (six of the eight incidents where version 3 of the PSDCS applied). SCADA outages across an entire region significantly impact power system security and market operation, often leading to substantial loss of system visibility and situational awareness for both AEMO and NSP control rooms. NSPs and AEMO should plan and operate their SCADA systems in a way which allows them to meet the requirements of the PSDCS. Where outages do occur the power system is at heightened risk until SCADA is restored and therefore all incidents necessitate prompt rectification and thorough investigation as a priority within the responsible organisation.

In addition, the review highlighted a prevalent lack of familiarity with the PSDCS and its requirements among NSPs. With the ongoing energy transition and the influx of new participants connecting to the grid, this unawareness poses a growing risk.

9.2 Incident response

9.2.1 Lack of alarming

AEMO has concluded that in five of the 18 incidents reviewed (incidents 1, 2, 7, 9, 10) the SCADA “failure” did not trigger alarms, with AEMO or NSP control rooms manually identifying the SCADA issue. Automatic issue detection is advantageous as it avoids unnecessary distractions in the control room and allows earlier problem detection and therefore quicker rectification.

AEMO notes there are instances where the EMS/SCADA system itself may be compromised, inhibiting the ability to raise an alarm. To address this issue implementing diverse monitoring methods can greatly increase the likelihood of problem detection, and this capability was highlighted as critical by system operators in the international review. These methods could include t elco bearer monitoring, ICCP application monitoring, 'heartbeat' checks, and monitoring for 'stale' SCADA data, such as real-time SML observations. By employing a multi-faceted monitoring approach, the system's overall capacity to detect anomalies is significantly enhanced.

9.2.2 Incident and situational awareness

AEMO has observed that feedback to the AEMO Control Room during SCADA incidents reviewed was at times inconsistent, varying with the time of day and incident severity. Prompt, consistent, and regular updates are crucial in allowing AEMO to make informed decisions regarding power system security[15]. When 'First Responders' are responsible both rectification and communications during incidents, they can lose track of time owing to the

[15] To meet the requirements of NER clause 4.2.6(b)(2), AEMO must return the power system to a secure operating state as soon as practical and in any event must do so within 30 minutes.

complexity of resolving the situation. AEMO identified that in some incidents communication about the incident cause, rectification action and expected rectification time was limited, reducing AEMO's incident awareness.

AEMO notes that the complete or substantial loss of SCADA data from a region immediately causes a significant loss of situational awareness within AEMO and NSP Control Rooms. In some incidents the deterioration in situational awareness may be gradual and may not be immediately recognised by operational personnel (increasing the complexity for Control Room Operators). Finally, incidents where SCADA is lost are comparatively rare, meaning Control Room staff might encounter them only a few times during their careers. Therefore, prompt communication and vigilance in maintaining situational and incident awareness throughout SCADA incidents is critical in limiting the impact of SCADA outages on power system security and the market.

9.2.3 After hours support

AEMO has concluded that two incidents (incidents 9, 18) were significantly delayed in rectification due to the lack of available after-hours SCADA support. Effective after-hours support for SCADA and energy management systems is critical to ensure service continuity and minimise outage durations. AEMO also notes that these complex systems often require expertise beyond the scope of an individual's comprehensive understanding. Therefore, it is crucial for the designated on-call personnel to have access to additional backup support from other knowledgeable team members. Fostering a culture of mutual support among team members, especially during after-hours, is essential.

Additionally, it is important to establish clear guidelines for on-call response times. Prompt response timeframes are critical given that AEMO is required to restore the power system to a secure state. Adhering to these guidelines would enable the AEMO and NSP Control Room's to have a clearer understanding of the incident implications and potential resolution time before needing to take further action.

9.3 Incident reporting and follow up investigation

9.3.1 Incident reporting and root cause analysis

AEMO has observed a notable deficiency and variation in the detail provided by NSPs and AEMO concerning the incidents. The issue was compounded by significant inconsistencies and variations in the timing, format, identification of root cause and level of detail in the reports submitted to AEMO. In addition, in at least 5 cases the root cause of SCADA failure was not identified or identified in significantly more than 20 business days.

Contrasting with international practices, incident reporting is typically standardised through the mandatory use of uniform incident report forms. Adopting a similar standardised approach could greatly improve the quality and uniformity of incident reporting.

9.4 Resilience and capabilities

9.4.1 Reliable and independent telephony

AEMO has observed during conversations with international system operators the criticality of maintaining verbal communications channels during major outages to enable coordinated recovery. Voice/telephone communications

are indispensable for the safe and secure operation of the NEM and WEM power systems. In the event of a major failure, maintaining verbal communication between AEMO, NSPs and participants allows for the continued operation of the power system for several hours under failure conditions, albeit with increasing difficulty and risk over time.

The necessity for highly reliable voice/telephone communications cannot be overstated, as it is fundamental to the power system's reliable operation and should be reviewed by each organisation to confirm voice/telephone communication system independence and robustness.

9.4.2 Telecommunications reliability

While not specifically reviewed as part of this investigation, Optus suffered a major telecommunications outage on 8 November 2023. As such, it is recommended that AEMO and NSPs in both the NEM and WEM review the scenario of a major failure of one of their telecommunications services providers and the potential impact on the operation of their operations and the power system.

Telcos can provide generic outage/failure rates but not specifically for any one WAN link. The first defence is to utilise diverse Telcos and monitor system performance metrics to enable early detection of network issues and faster resolution. This monitoring capability also supports with post incident investigation.

The ability to monitor WAN links and traffic is essential for early detection of network traffic issues, both at the Telco bearer level and the SCADA/EMS application level, as such AEMO recommends that NSPs review their own monitoring systems to ensure they can detect network issues promptly. In addition, the review recommends that AEMO collates existing monitoring data for internal use on a monthly and annual basis as part of its performance metrics.

9.4.3 AEMO and NSP owned telecoms infrastructure

AEMO reviewed two incidents (incidents 11 and 14) in which no specific root cause was identified other than intermittent/drop out of the communications link leading to loss of the ICCP links. In addition, dependence on third party telecommunications was raised as a significant issue to be monitored by system operators during the international review. These providers are not immune to outages that can affect operations. One possible solution is for AEMO (and NSPs) to own fibre or other telecommunication assets directly however, the cost and complexity of designing, installing, operating, and maintaining large interstate optic fibre Telco grade services is high and it would not be considered economically viable for AEMO to do so.

The NSPs operate optic fibre and digital microwave services as these are an essential part of their businesses and they have the infrastructure to provide these services. The AEMO Sydney and Brisbane control centres are located near to Transgrid and Powerlink communications infrastructure linking back to each NSPs network. AEMO recommends that additional potentially low cost back up communications links between AEMO and NSPs should be investigated utilising NSP communications infrastructure where economically viable.

10 Recommendations

With reference to the key investigation findings outlined in Section 9 of this report, the investigation has concluded that the primary contributors to incident occurrence and impact are:

- Processes, controls, training and monitoring (Processes).
- Response to incidents (Response).
- Incident reporting and follow up investigation (Investigation).
- Resilience and capabilities (Resilience).

AEMO considers that the trend in the number and impact of recent SCADA incidents poses a significant and unacceptable risk to power system operations which needs to be addressed as a priority. As such, AEMO makes eight key recommendations which address the most significant risks identified during the investigation and focussed effort is required from AEMO, NSPs and participants to promptly act on these recommendations to significantly enhance overall SCADA system reliability and resilience.

Table 6 Findings and recommendations

ID	Finding	Action/Recommendation
1	**Finding category – Multiple** AEMO identified areas for improvement for NSPs in the SCADA baseline questionnaire findings outlined in Section 7.2 of this report. AEMO also concluded that two incidents had significant delays in rectification due to the lack of available after-hours SCADA support. Effective after-hours support for SCADA and energy management systems is critical to ensure service continuity and minimise outage durations. **Relevant findings: 7.2 and 9.2.3**	• AEMO will meet with each NSP individually by the end of Q2 2024 to share relevant SCADA questionnaire findings and identify areas for potential improvement. NSPs and AEMO will progress additional actions or recommendations identified during these discussions as appropriate. • At these meetings, AEMO will also confirm with NEM SCADA operators that existing after-hours support arrangements are aligned with meeting the requirements of the Power System Data Communication Standard (PSDCS).
2	**Finding category – Processes** AEMO has concluded that the majority of incidents were influenced by inadequacies in change management, processes and procedures, training, knowledge sharing, monitoring of SCADA operations, and overall situational awareness. Addressing these challenges necessitates a co-ordinated and continued effort between AEMO and NSPs to enhance SCADA system resilience and reliability. **Relevant findings: 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 9.3.1**	• AEMO will establish a SCADA working group with representatives from NEM and WEM NSPs, to report to the NEM Operations Committee (NEMOC). The group will be tasked with improving SCADA system resilience and reliability, across the NEM and WEM. The expected outcome is a measured reduction in SCADA outages. • The SCADA working group should be established by May 2024 and will initially meet monthly. The SCADA working group Terms of Reference (ToR) will be agreed by June 2024 and will include the following: – Ensure consistent understanding of SCADA requirements in the NER and the PSDCS, including recommending changes where appropriate. – Review of learnings from SCADA incidents (including incidents in which backup systems prevented an outage), causes, recommendations, and lessons learned. – Review of SCADA minutes lost monitoring and trends analysis. – Sharing of outcomes/learnings from backup/failover system testing completed by SCADA working group members. – Monitoring of NSP and AEMO ability to meet PSDCS requirements (including review of any proposed revisions or amendments to the PSDCS). – Continued support for the development of processes for notification of SCADA work to control rooms and AEMO.

ID	Finding	Action/Recommendation
		– Review and (if applicable) implementation of change management process improvements. – Monitoring of NSP and AEMO progress against identified improvement actions/initiatives related to strategic focus areas (see below). • NSPs and AEMO will undertake a comprehensive review of the following prioritised strategic focus areas and report the outcome to the SCADA working group by the end of August 2024: – Assessment of change management processes related to SCADA and identification of opportunities for improvements. – Review of existing root cause investigation frameworks and processes to confirm that investigation method has clear guiding principles and adaptable methodologies for analysis across different incidents and teams. – Assessment of policy and procedure management related to SCADA and identification of improvement opportunities. – Evaluation of capability to monitor and analyse SCADA system downtime (minutes lost) and identification of improvement opportunities. – Prioritisation of the identified opportunities for improvement and an indicative timeline for completion of any improvement actions. Ongoing progress of improvement actions/initiatives will be monitored via the SCADA working group. • The SCADA working group ToR will also include the following as future strategic focus areas for review: – Evaluation of staffing, including after-hours support, and training practices in alignment with the risk profile and compliance expectations in the PSDCS. – Evaluation of testing processes of backup facilities and redundant systems, improvements to sharing of testing results/findings with SCADA working group members, and testing guideline development. – Evaluation and improvement of incident management frameworks. – Evaluation of situational awareness capabilities and areas for improvement. – Evaluation of contingency analysis and power system security monitoring capabilities[16] at NSPs and identification of improvement opportunities. • The SCADA working group will assign accountable working group leaders for each prioritised strategic focus area (as required).
3	**Finding category – Processes** AEMO has concluded that in seven of the 18 incidents reviewed there was a lack of awareness in the AEMO and/or NSP control room(s) regarding planned SCADA system works. AEMO considers that had control rooms been aware of the planned work, SCADA could have been returned to normal service more promptly. **Relevant finding: 9.1.2**	• By the end of Q4 2024, AEMO, in consultation with NSPs, will establish a standardised process for the notification of planned works on NSP and AEMO SCADA systems. • To support this process, AEMO will create a set of guidelines which outline when and how NSPs and participants should notify AEMO of higher risk planned SCADA work.
4	**Finding category – Processes** AEMO has concluded that the predominant factor contributing to the loss of SCADA data to AEMO, in 16 of the 18 incidents reviewed, was the failure of redundant/backup systems. While this was not necessarily the root cause, in many cases if redundant/backup systems had responded in line with expectations, a full SCADA failure would	NSPs and AEMO to review existing automated backup and failover system testing procedures and identify opportunities for improvements by the end of Q3 2024. *Note: AEMO has previously recommended NSPs undertake routine failover testing of their SCADA systems, in the published Victorian Market Suspension market event report*[17]*.*

[16] Contingency analysis and system security monitoring capabilities encompass suites of tools and processes that enable operators to monitor the power system and maintain power system security.

[17] Please see https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-report-vic-market-suspension.pdf?la=en.

ID	Finding	Action/Recommendation
	have been avoided. This finding is consistent with observations from the international review, which suggested that while SCADA issues do occur, the effective operation of redundant/backup systems often prevented issues from escalating. **Relevant finding: 9.1.1**	
5	**Finding category – Processes** AEMO has concluded that six of the 18 SCADA failures investigated were caused by external telecommunications systems issues or internal network issues at the NSPs. The ability to monitor SCADA delivery and "downtime" from or by the NSPs is an important function. Early detection of "downtime" alerts the AEMO/NSP support teams that investigation and action is required. Similarly, collecting longer-term availability data allows AEMO to monitor long-term performance and compliance with the PSDCS. AEMO also concluded that five of the 18 SCADA failures investigated did not trigger alarms, with AEMO's or an NSP's control room manually identifying the SCADA issue. Early problem detection is key for swift resolution, and by employing a multi-faceted monitoring approach, the system's overall capacity to detect anomalies is significantly enhanced. Finally, AEMO identified two incidents that were likely, but not confirmed, to be caused by telecoms reliability issues. The lack of monitoring capability for these services can impact identification and resolution of the root-cause. **Relevant findings: 9.1.5, 9.2.1, 9.4.2**	• By the end of Q4 2024, AEMO and NSPs to complete a review of existing SCADA monitoring tools to ensure they are able to promptly identify "downtime" of SCADA services to AEMO at: – The telecommunications level (including telco WAN monitoring at the bearer and the application-level utilising dedicated tools (where possible)), – The network level, and – The SCADA application level. Monitoring should occur in real time and allow tracking of trends in historical data. • During the above review, AEMO and NSPs should: – Investigate and, wherever feasible, implement multiple and overlapping Energy Management System (EMS)/SCADA System monitoring capabilities. These should be deployed within and outside the EMS, including telco bearer monitoring, Inter-Control Centre Communications Protocol (ICCP) Application monitoring, "heart-beat" monitoring and "stale" SCADA data monitoring. – Where possible (and appropriate), consider adding alarms/alerts to monitoring systems to notify operators and support teams whenever "downtime" or other issues are detected. *Note: AEMO has previously recommended implementation of suitable alarms and heartbeat displays to alert operators in the published NSW market suspension market event report and the total loss of NEM SCADA incident report*[18].
6	**Finding category – Processes** This review identified a prevalent lack of familiarity with the PSDCS and its requirements among NSPs. AEMO concluded that in seven of the 18 incidents investigated there was a failure to comply with the applicable version of the standard. **Relevant finding: 9.1.6**	AEMO will address the lack of familiarity with the PSDCS and its requirements among NSPs via the SCADA working group and through the preparation and distribution of training material by Q3 2024.
7	**Finding category – Investigation** AEMO identified a notable deficiency and variation in the detail provided by NSPs and AEMO concerning the incidents. The issue was compounded by significant inconsistencies and variations in the timing, format, identification of root cause and level of detail in the reports submitted to AEMO. **Relevant findings: 9.1.6 and 9.3.1**	• By Q4 2024, the SCADA working group will review and update AEMO's proposed standard SCADA incident report information form. Once the proposed standard SCADA incident report information form is finalised by the working group, information related to any SCADA incidents should be recorded in the approved format to ensure consistency. • By Q4 2024, the SCADA working group to review the PSDCS and consider: – Inclusion of a template SCADA Incident Report information form (based on the agreed template above). – A requirement for NSPs to complete and submit the SCADA Incident Report information and root cause identification within 20 business days of the incident date (for incidents where the outage time exceeded the allowable time in the PSDCS). *Note: a 20-business day requirement would align SCADA incident investigation and reporting timeframes with the existing response timeframes under NER clause 4.8.15(g).*

[18] Please see https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/market_event_reports/2023/preliminary-suspension-nsw.pdf?la=en and https://www.aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/final-report-total-loss-of-nem-scada-data.pdf?la=en.

ID	Finding	Action/Recommendation
		– In cases where a SCADA incident leads to a complete loss of data from a NSP or participants, mandate a comprehensive investigation to identify the causes and implement corrective actions within an agreed timeframe. – Whether any requirements outlined in the PSDCS should be reflected in the NER.
8	**Finding category – Resilience** AEMO identified during the review, and in discussions with international system operators, a significant dependence on third party telecommunications, suggesting the need to evaluate the advantages of implementing key AEMO-owned infrastructure for enhanced control and reliability. **Relevant findings: 9.4.1, 9.4.2, 9.4.3**	• By Q1 2025, AEMO and the transmission network service providers (TNSPs), distribution network service providers (DNSPs) and participants from which AEMO receives SCADA data should review their telecommunications systems and consider implementing changes (as required) to allow each entity to have a reliable, independent means of communication with AEMO in the event of a major network outage at their respective sites. • By the end of Q4 2024 AEMO to: – Investigate the communications connections between its New South Wales control room and Transgrid's network to provide alternative communication links for New South Wales region data. – Investigate the communications connections between its Queensland control room and Energy Queensland's network and onto Powerlink to provide alternative communication links for Queensland region data.

A1. SCADA baseline questionnaire

Table 7 summarises the technical/system component of the questionnaire sent to NSPs to establish a current baseline of their SCADA systems.

Table 7 SCADA baseline questionnaire summary – technical/system

Item	Primary category	Secondary Category	Question / area
1	System & infrastructure	N/A	EMS and Historian Vendor. Asset inventory
2	System & infrastructure	Asset age & support	What is the year the current version commissioned/cut-over for: SCADA/EMS/Historian etc
3	Asset age & support	Risk	What is the release date of current versions for: SCADA/Comms front ends/EMS/Database/Historian/ICCP and any other major applications
4	System & infrastructure	People & resources	What is the system size, including point count, number of operator and other user workstations
5	Redundancy	Risk	Is there full EMS redundancy at (a) the primary site, and (b) back-up site
6	Redundancy	Risk	Back-up site staffing & operation (i.e., fully staffed and/or operating continuously)
7	Redundancy	Risk	How is the back-up site kept up to date for: displays, databases, versions, procedures etc. Is there a risk assessment when work impacts on redundancy
8	Asset age & support	Risk	Are there vendor support contracts and vendor emergency response contractual requirements in place.
9	System & infrastructure	People & resources	What are the major EMS Apps in daily or frequent use
10	People & resources	Process & procedures	Are BAU support activities undertaken using (a) internal staff, and (b) third party providers
11	People & resources	Process & procedures	What is the patching cycle or timing of OS updates and application patches or infrastructure firmware updates
12	System & infrastructure	People & resources	Does the organisation have and routinely utilise a QA environment
13	Emergency Response	Cyber	Does the organisation allow remote access for support (especially after hours)
14	Emergency Response	Situational Awareness	Is there 24x7 automated system monitoring and reporting of performance issues or failures
15	Situational Awareness	Process & procedures	Is there routine monitoring of the system down time to track performance against AEMOs KPIs
16	Training & knowledge	Process & procedures	Is there established and agreed common terminology for communication between end user and the support or other teams.
17	Process & procedures	Risk	Are there processes for approving, managing and tracking system configuration changes, ie formal change management processes

Table 8 summarises the current processes, procedures, training, knowledge sharing and risk assessment aspects of the questionnaire sent to NSPs to establish a current baseline for their people and culture.

Table 8 SCADA baseline questionnaire summary – people, risk, processes and procedures

Item	Primary category	Secondary Category	Question / area
1	Process & procedures	People & resources	Does the company have documented: policies, standards and procedures
2	Risk	Process & procedures	When work is being undertaken that impacts on or may impact the SCADA/EMS system availability, are there defined processes for assessing risk, timing, back-out plans, escalation. Informing the control room, permission to proceed etc
3	Process & procedures	Risk	Describe the process for infrequent or unusual tasks for which procedures don't exist
4	Process & procedures	Risk	Is there a procedure management system
5	Process & procedures	Risk	Is compliance with procedures and procedure usage audited
6	People & resources	Process & procedures	Are staffing levels adequate to cover daily activities and/or extended leave
7	Training	People & resources	Are there defined induction, training, knowledge sharing and review practices. Does the organisation foster improvement and learning opportunities
8	Training	People & resources	Is there a skills matrix that identifies individual's skills and capability
9	Training	People & resources	Do managers, team-leaders and staff understand the obligations and allowable down times as described in AEMO's Power System Data Communication Standard.
10	Process & procedures	Risk	Does the organisation actively promote risk assessment and an understanding of the consequences of things going wrong when working on these systems

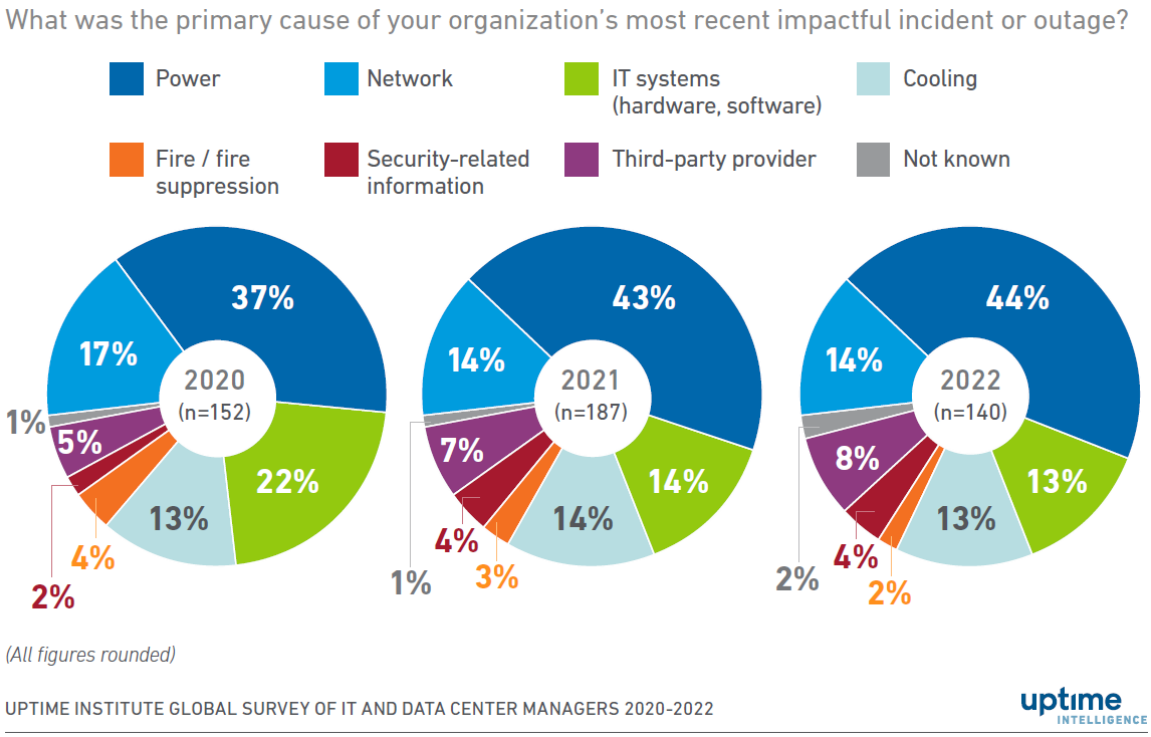
A2. Data centre incidents

The Uptime Institute is a recognised global authority in digital infrastructure, with over 25 years of experience setting standards and driving best practices. Their globally adopted Tier Standard Topology provides a benchmark for data centre reliability and design. Their extensive work with companies across various industries informs their Outage Analysis reports, which offer data-driven insights into the causes and consequences of data centre downtime.

While these reports primarily target traditional IT environments, their analysis can provide a valuable perspective for understanding potential risks within Operational Technology, including SCADA systems. The focus on robust infrastructure design and the emphasis on the causes of outages in the Uptime Institute's approach likely hold valuable parallels for enhancing SCADA system resilience.

Figure 2, from its 2023 report, while not necessary applying to OT environments, provides a good insight to a large data set of outages from the Uptime Institute's member base.

Figure 2 Uptime Institute – review of leading causes of significant outages



Source: Annual Outages Analysis 2023 - Uptime Institute, at https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023.

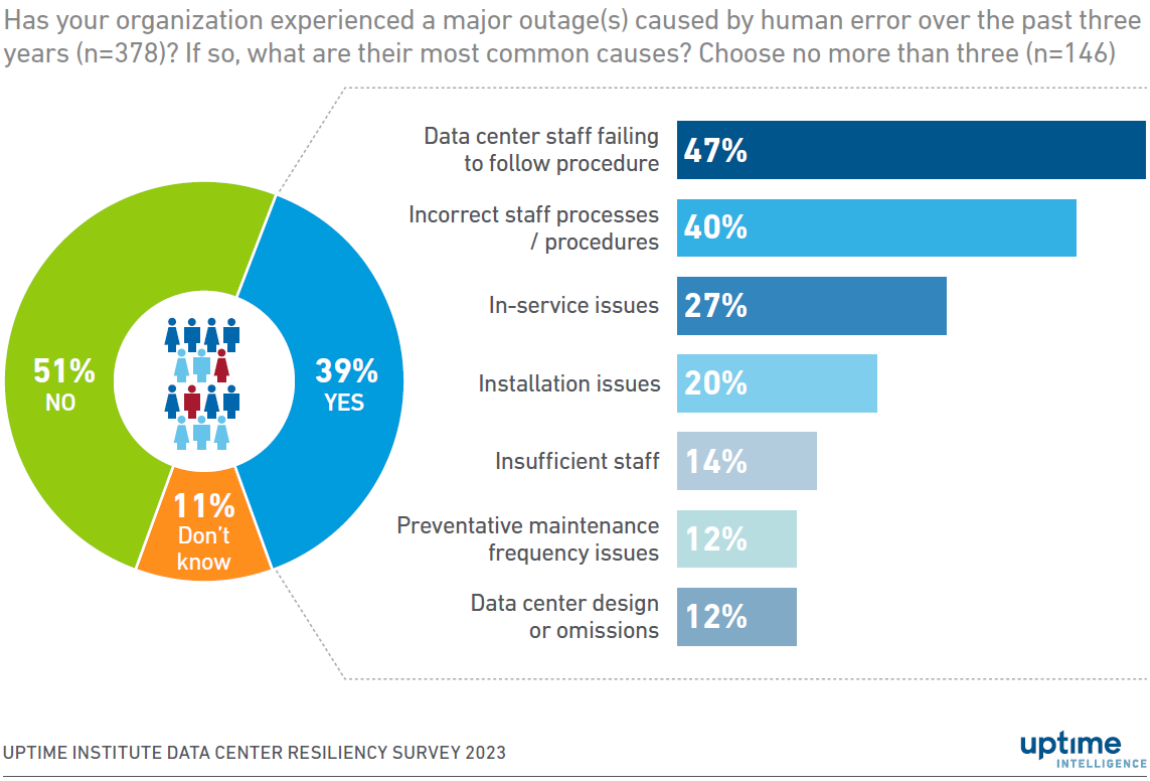
A key finding is that power-related issues have been the primary cause of significant outages over three consecutive years, and cooling loss also ranking high. While these issues were not prominent in the 18 incidents investigated for this report, they have been known to occur in previous years.

The next two leading causes identified by Uptime Institute – IT systems (hardware and software) and network failures – align closely with the findings of this report. However, it is important to note that this classification scheme does not distinguish between purely technical malfunctions and those stemming from human errors in

configuration or process. The Uptime Institute takes a more holistic view of human error, recognizing it as a contributing factor in 65% to 80% of all outages, but rarely the root cause. Its extensive data analysis suggests that the origins of human error are complex, ranging from inadequate training and staff fatigue to the inherent complexity of the systems being managed. Addressing and preventing human error remains a significant challenge for both data centre operators and those responsible for critical OT infrastructure.

Figure 3 below identifies the most common causes of human error related outages.

Figure 3 Uptime Institute – most common causes of human error related outages



Source: Annual Outages Analysis 2023 - Uptime Institute, at https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023.

It is noteworthy that the most common causes of outages are often linked to procedural lapses or incorrect processes. The Uptime Institute provides annual reports of major and severe data centre outages.