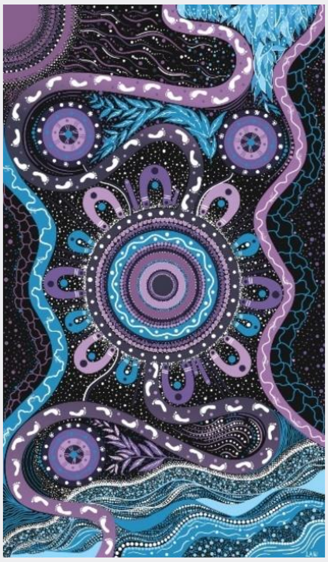
Learnings from industry implementation of emergency backstop mechanisms for distributed resources

Q2 2025

Insights from industry implementation experiences in Australia to date



We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country; and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have launched its first Reconciliation Action Plan in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation - a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Important notice

Purpose

The purpose of this publication is to facilitate knowledge sharing on the implementation of emergency backstop mechanisms to date in Australia, including in the Western Australian Wholesale Electricity Market (WEM) and National Electricity Market (NEM), so that learnings can be shared and built on in all regions. As noted in AEMO's earlier publications, work to implement operationally effective emergency backstop mechanisms is now required in all NEM mainland regions[1], as well as in the WEM[2,3]. AEMO is publishing this in line with its responsibilities under clause 4.3.1(n) and (v) of the National Electricity Rules, to provide information to participants in relation to a significant risk to the power system and to initiate action plans to manage any abnormal situations or significant deficiencies which could reasonably threaten power system security.

This publication is generally based on information available to AEMO as of May 2025 unless otherwise indicated.

Disclaimer

Copyright

[1] See https://wa.aemo.com.au/initiatives/major-programs/nem-distributed-energy-resources-der-program/managing-distributed-energy-resources-in-operations/managing-minimum-system-load.

[2] Government of Western Australia, Distributed Energy Resources Roadmap, https://www.wa.gov.au/government/distributed-energy-resources-roadmap.

[3] Government of Western Australia (July 2024), Distributed Energy Resources Roadmap, Third Progress Report, https://www.wa.gov.au/system/files/2024-07/248948epwaderrroadmap26_july.pdf.

Executive summary

In July 2024, Australia's Energy and Climate Change Ministerial Council agreed on a National Consumer Energy Resources (CER) Roadmap[4], building on advice from the Energy Security Board (ESB) around critical technical capabilities for ongoing power system security. The CER Roadmap sets out an overarching vision and plan to unlock CER at scale and identifies measures to "unleash the full potential of CER" by establishing the required mechanisms, tools and systems. This includes both:

- reforms to increase the opportunities for market participation of CER, including through enhanced coordination, allowing customers to respond to market-based incentives which will also help meet the challenges of low operational demand, and
- measures to support ongoing power system security, particularly the requirement for emergency backstop mechanisms to be in place by the end of 2025 to ensure the operational security of the power system when required.

Effective integration of CER will require the intersection of power system engineering, technological innovation, consumer choice and experience, and government policy and regulation.

Significant progress has been made already to unlock CER opportunities. Several workstreams have progressed under the National CER Roadmap, with outputs including consultation papers on CER Data Sharing Arrangements[5] and Roles and Responsibilities for Power System and Market Operations in a High CER Future[6]. These workstreams aim to embed an effective foundation for coordination of CER. Likewise, the Engineering Roadmap Priority Actions update[7] highlights progress on initiatives including electric vehicle (EV) standards, improved compliance, flexible trading arrangements and integration of price-responsive resources. Some of the capabilities discussed in this report provide a foundation to unlock these future pathways for better utilisation of distributed energy resource (DER) devices for customers, for example by facilitating CER orchestration or flexible solar exports.

The need for emergency backstop

This report builds on previous analysis published by AEMO which identified increasingly low operational demand events, during which a range of measures would be required to ensure power system security can be maintained in all National Electricity Market (NEM) mainland regions[8,9], and in the Western Australian Wholesale Energy

[4] At https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf .

[5] Australian Government, Department of Climate Change, Energy, the Environment and Water, National Consumer Energy Resources (CER) Roadmap – Data Sharing Arrangements – M2, https://consult.dcceew.gov.au/national-cer-roadmap-data-sharing-arrangements-m2.

[6] Australian Government, Department of Climate Change, Energy, The Environment and Water, National Consumer Energy Resources (CER) Roadmap – Redefine roles for market and power system operations – M3/P5, https://consult.dcceew.gov.au/national-cer-roadmap-redefine-roles-m3-p5.

[7] AEMO, Engineering Roadmap Strategy and Progress Reports, https://aemo.com.au/initiatives/major-programs/engineering-roadmap/reports-and-resources.

[8] AEMO (Q4 2024) *Supporting secure operation with high levels of distributed resources*, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en.

[9] In accordance with AEMO's responsibilities under the National Electricity Rules (NER) 4.3.1(n), to refer information of which AEMO becomes aware in relation to significant risks to the power system where actions to achieve a resolution of those risks are outside the responsibility or control of AEMO.

market (WEM)[10,11]. The full suite of measures, which include improved CER orchestration, is discussed further in previous reports[12]. This report focuses on one key measure to ensure power system security can be maintained – emergency backstop capability.

Defining emergency backstop capability

"Emergency backstop" capability refers to operational measures to reduce aggregate DER generation if required for system security, when other options have been exhausted. This is a critical tool to keep the power system secure under extreme conditions before higher customer impact measures are enacted.

Implementation of operationally effective emergency backstop mechanisms is an important component to support secure operation of a grid supplied by large amounts of DER which are not dispatched through the centralised market. As DER encompasses CER[13], this report refers to DER except where the term 'CER' is used in governance or other frameworks, or where the specific reference is only to resources owned by consumers[14].

Considerable effort has been invested to date by many industry participants, including distribution network service providers (DNSPs), utilities (such as Synergy), state and territory governments, original equipment manufacturers (OEMs), and others across industry, and ongoing work remains important.

Purpose of this report

To date, emergency backstop mechanisms have been implemented under jurisdictional requirements on urgent timeframes to address operational power system security risks identified by AEMO. As system operator, AEMO acknowledges developing emergency backstop capability is inherently complex given the millions of individual consumers and devices involved, the large number of stakeholders across the CER ecosystem and supply chain, and the extensive integration and coordination required across different systems and parties.

This report recognises the enormous body of work undertaken by a wide range of stakeholders in South Australia, the Western Australian South West Interconnected System (SWIS), Victoria and Queensland to support secure power system operation in periods of high generation from DER by implementing emergency backstop capabilities.

It aims to:

- consolidate and draw on common learnings across all jurisdictions, highlighting key challenges observed and solutions that have been developed and refined over time,

[10] Government of Western Australia, Distributed Energy Resources Roadmap, https://www.wa.gov.au/government/distributed-energy-resources-roadmap.

[11] Government of Western Australia (July 2024), Distributed Energy Resources Roadmap, Third Progress Report, https://www.wa.gov.au/system/files/2024-07/248948epwaderrroadmap26_july.pdf.

[12] AEMO (Q4 2024), *Supporting secure operation with high levels of distributed resources*, Section 2, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en.

[13] CER are consumer resources that generate, store or consume electricity (such as rooftop solar, batteries and loads). DER encompasses CER, and also includes other larger installations within the distribution system.

[14] For more details on the differences between CER and DER, see https://www.energy.gov.au/energy-and-climate-change-ministerial-council/working-groups/consumer-energy-resources-working-group.

- support jurisdictions, networks, central utilities, OEMs and industry in resourcing for and achieving operationally effective emergency backstop capabilities[15], including regions which are starting their journeys and those working on uplift of capabilities,
- highlight some key governance gaps that have become apparent, as a basis for consultation and collaboration with stakeholders on possible solutions to address these gaps, and
- build a transparent consolidated resource, and support national consistency (such as commonly agreed performance metrics and standards).

Stakeholder engagement on this report

AEMO has worked closely with DNSPs and utilities which have implemented or are about to implement emergency backstop in Australia (DNSPs in the mainland NEM, and Synergy in the SWIS), to analyse and distil learnings and themes from collective experiences to date. This has included AEMO's independent analysis, as well as collating lessons learned and insights shared in various forums. AEMO has also been working closely with state, territory and federal governments, and seeking feedback and input from OEMs, representative groups such as the Clean Energy Council (CEC), Energy Networks Australia (ENA) and the Smart Energy Council (SEC), and metering coordinators on their experiences. The development of AEMO's Minimum System Load (MSL) procedures in collaboration with DNSPs and transmission network service providers (TNSPs), and the Minimum Demand Threshold (MDT) Operations Protocol in collaboration with the TNSP, has also provided further insights.

This report aims to draw together the key themes from this engagement, outlined below.

Lessons learned on industry implementation of emergency backstop mechanisms

Across the jurisdictions and organisations implementing emergency backstop, several key lessons have surfaced multiple times which are applicable to all emergency backstop mechanisms, including Common Smart Inverter Profile – Australia (CSIP-AUS[16]), Generation Signalling Devices (GSDs[17]), proprietary application programming interface (API) platforms, smart meters, and Supervisory Control and Data Acquisition (SCADA). The report also outlines a specific learning on the important role of OEMs and other technology providers of active management of DER in internet-based pathways (including CSIP-AUS).

Balance gradual rollout pathways against urgent operational needs

Systems for active management of hundreds of thousands of DER sites at useful operational scale are inherently complex. Delivering robust, scalable, and reliable solutions to support this complexity remains in its early stages. Therefore, gradual and measured rollout pathways with proactive industry engagement and clear expectations and timelines are recommended, balanced against requirements to address urgent operational needs and ensure sufficient tools are available to manage system security.

[15] In accordance with AEMO's responsibilities under NER 4.3.1(n).

[16] The 'Common Smart Inverter Profile – Australia' (CSIP-AUS) was developed by the DER Integration API Technical Working Group, which aimed to develop a consistent technical approach to communicating dynamic export and import limits between DNSPs and customers or their aggregators. This culminated in the release of CSIP-AUS, an Implementation Guide of IEEE 2030.5. More information on CSIP-AUS is at https://www.csipaus.org/about.

[17] A device connected at the customer's site that enables the inverter to receive a signal to activate a standardised demand response mode which disconnects the DER inverter.

This may mean:

- jurisdictions commence concrete implementation efforts early, in anticipation of 3-5 years of lead time for learning-by-doing, and
- gradual implementation of active DER management alongside complementary measures which can be implemented in a shorter timeframe and deliver a significant amount of emergency response (for example, load shifting). Where tools are needed urgently at scale, it may be necessary to explore measures with potential for higher customer impact, such as emergency voltage management (EVM[18]), as a near-term stop gap until active DER management is operationally available at sufficient scale.

Significant resources are required for active and ongoing industry engagement and support

Pathways to ensure an appropriate level of resourcing should be considered, as significant resources are required in the lead up to and the years following implementation to support rollout of an effective emergency backstop mechanism. Resourcing and frameworks for active and ongoing industry engagement, education and support are particularly important. This involves engaging prior to emergency backstop mechanism implementation as well as post-rollout in anticipation of high support needs in the first few months of rollout, particularly in frameworks for change management, collaboration and engagement, installer education, training, and support, and a united approach from industry and government bodies. Some emergency backstop mechanism implementation pathways also have potential to unlock future capabilities for DER by facilitating CER orchestration or flexible solar export[19]. Engaging with industry and the public about this broader value can help smooth the pathway for emergency backstop mechanisms.

Address urgent governance gaps in emergency backstop mechanism performance requirements

In building this report, many stakeholders raised a range of governance gaps which have reduced their ability to resource for, support and enforce high compliance in emergency backstop mechanisms. Clearly defined roles and responsibilities are particularly important because of the number of parties involved (for example, jurisdictions,

[18] This term refers to the deliberate increase in voltage to curtail distributed PV generation during extreme conditions. As different DNSPs use different terms for this based on technology type, this report uses the term ‘emergency voltage management’ (EVM) for clarity and consistency. Where a different term is used by the DNSP it is noted in the accompanying text.

[19] For example:

- Flexible export limits (FELs) leverages capabilities SA Power Networks (SAPN) had sought and obtained revenue allowance for in its 2020-25 reset period (https://www.aer.gov.au/system/files/Final%20decision%20-%20SA%20Power%20Networks%20distribution%20determination%202020-25%20-%20Overview%20-%20June%202020_2.pdf) under its low voltage (LV) management program.
- AusNet Services’ 2026-31 Electricity Distribution Price Review (EDPR) submission on CER strategy (https://www.aer.gov.au/system/files/2025-02/ASD%20-%20AusNet%20-%20CER%20Integration%20Strategy%20-%2031%20Jan%2025%20-%20PUBLIC.pdf) notes that capabilities developed to meet the new Victorian Backstop Mechanism (VBM) requirements mean transition to Flexible Exports for all AusNet Services customers from 1 July 2026 comes at a lower incremental cost.
- Jemena’s Grid Stability and Flexible Services Program (https://www.aer.gov.au/system/files/2025-02/JEN%20%E2%80%93%20RIN%20%E2%80%93%20Support%20%E2%80%93%20Grid%20Stability%20and%20Flexible%20Services%20Program%20%E2%80%93%20Investment%20Brief%20%E2%80%93%2020250131.pdf) also notes that DER emergency backstop capability is foundational for the support of flexible exports.
- Flexible export is also raised in CPUE’s 2026-31 EDPR (https://media.powercor.com.au/wp-content/uploads/2024/09/09130856/Draft-proposal-2024-part-B-CitiPower.pdf), which notes that customers believe in the benefits of flexible exports as a means to maximise solar energy output and support future sustainability.

DNSPs, solar retailers and installers, OEMs, aggregators and customers) at different stages of emergency backstop mechanism implementation and delivery.

Key areas appear to be around governance gaps in formally assigned roles and processes, and national consistency in implementation. Some DNSPs noted that opportunities for improving consistency may need to be considered in the context of the costs and time to achieve that consistency.

There are a range of ongoing workstreams aiming to address these gaps, to which AEMO will continue to provide advice, including workstreams identified under the National CER Roadmap, and ongoing harmonisation efforts, including in the incoming New South Wales Emergency Backstop Mechanism (EBM) and the proposed Australian Capital Territory emergency backstop mechanism, to align implementation in these regions and foster national consistency more broadly.

A key learning from this work is the importance of active and ongoing engagement with the wide range of stakeholders involved in emergency backstop implementation. Hence, this report aims to articulate observed governance gaps as a basis for consultation with stakeholders to address these gaps.

Internet-based mechanisms: address critical governance gaps in OEM operational performance

OEMs and other technology providers of active DER management have become increasingly important in power system operations, now delivering critical functions which extend long after the initial manufacture of the device. One critical governance gap that has become apparent is the role of OEMs and technology providers in delivery of internet-based emergency backstop mechanisms (such as CSIP-AUS and application programming interface [API] platforms). Pathways to address this gap should be urgently explored.

Governance gaps in OEM and technology provider operational performance

OEMs and other technology providers of active DER management are a key component in every internet-based emergency backstop mechanism implemented in Australia to date (both CSIP and non-CSIP), whether through provision of servers/platforms or utility-to-device firmware through which emergency backstop is implemented. At present, there are no regulatory requirements or governance arrangements supporting OEMs and technology providers to invest in the systems necessary to deliver consistently high levels of server reliability. Significant delays in emergency backstop delivery (of 1-3 hours, with some devices taking up to 6 hours to respond) have been observed from four OEMs in historical emergency backstop at-scale activation events. AEMO sees the role of OEMs and other technology providers as a key governance gap that presents a high risk to successful emergency backstop delivery, and needs to be urgently addressed.

Installation compliance is a key component for operational effectiveness

Challenges with installation compliance are a consistent theme to date across all mechanisms for active DER management in Australia. Considerable work is ongoing to uplift installation compliance across many different areas, and there are inherent challenges of change implementation for hundreds of thousands of DER devices.

In the early stage of rollouts, several emergency backstop mechanisms in Australia have been observed to have installation compliance rates of about 30-50%. Later-stage emergency backstop rollouts (~2-3 years since implementation) typically achieve installation compliance rates of ~70-80%. In the most recent emergency backstop implementation, the Victorian Backstop Mechanism (VBM), requirements began in October 2024 for ≤200 kilovolt amperes (kVA) sites. Installation compliance levels have shown progressive improvements since rollout, and as at June 2025 (nine months from rollout), DNSP estimates indicate installation compliance has increased to later-stage rates of ~70-80%[20]. This reflects considerable resources and effort from Victorian industry, DNSPs and the Victorian Government Department of Energy, Environment and Climate Action (DEECA) to implement the VBM and progressively resolve challenges, including through Victoria's Emergency Backstop Reference Group, as well as successful building on learnings from other jurisdictions, for example through knowledge-sharing sessions by SA Power Network (SAPN).

Jurisdictions implementing emergency backstop mechanisms should plan to dedicate considerable resources and mechanisms to support improving installation compliance. These could include frameworks for compliance monitoring and management which have high visibility, and confirmation of compliance with static export limits.

Formal, regular at-scale testing

When emergency backstop is activated at scale, operational observations from historical at-scale activations of internet-based mechanisms indicate 70-85% of *correctly* installed and commissioned sites respond[21], for a variety of reasons outlined further in this report. This means that even at later-stage installation compliance rates of 70-80%, which require high levels of resourcing and engagement to achieve, a subset (70-85%) are expected to provide operational response to an at-scale activation – that is, ~50-68% of all DER devices required to have an emergency backstop mechanism may respond to an at-scale activation.

As at June 2025, two organisations have conducted at-scale activations of emergency backstop mechanisms in Australia:

- Synergy, which runs regular and comprehensive at-scale tests of their internet-based proprietary API platform in the Western Australian SWIS[22]. This includes an end-to-end test in coordination with AEMO and Western Power twice a year.
- SAPN, which has activated emergency backstop mechanisms via CSIP-AUS in its flexible export limits (FELs) pathway for extreme conditions, as well as during an at-scale 'fire drill' test in August 2024[23].

Observations from these at-scale activations indicate that 70-85% of *correctly* installed and commissioned sites respond – that is, approximately 15-30% of sites correctly installed and set up with the emergency backstop mechanism do not appear to respond to the curtailment signal[24]. Regular testing of the emergency backstop mechanism at a scale that could be used in a real event is a key pathway to identify and rectify challenges in

[20] Based on data provided by DNSPs to DEECA on the capacity of sites connected to their VBM servers, and AEMO's analysis of Clean Energy Regulator Register (CERR) data on the installed capacity of sites installed in Victoria.

[21] AEMO has independently confirmed this from at-scale activations in South Australia, and Synergy has observed this in its regular 'fire drill' tests.

[22] Synergy is intending to progressively roll out CSIP-AUS capability, with gradual migration from the API platform to CSIP-AUS servers.

[23] SAPN has also activated its Relevant Agent (RA) fleet for extreme conditions and in a 'fire drill' test, but equivalent analysis (the proportion of correctly installed RA sites which did not respond to the curtailment signal during an at-scale activation) could not be conducted, as their installation compliance rate is not known.

[24] Based on observations from Synergy in the SWIS, and AEMO's independent analysis of FELs sites based on SAPN data on which sites had passed capability tests. SAPN and Synergy note this could be due to a range of reasons, likely including scalability challenges, changes to site configuration post-installation, connectivity changes (for example, from customers switching internet provider), changes in the remote software solutions operated by technology providers, or updates to DER inverter software or firmware.

emergency backstop operation, prior to when emergency backstop mechanisms are needed to maintain system security. At-scale testing has not yet been conducted for other emergency backstop mechanisms, so it is not well understood if similar challenges may arise. It is recommended that at-scale testing be explored for all emergency backstop mechanisms where feasible, first at the DNSP level, and then coordinated across multiple regions.

Apply transparent and consistent reporting and performance definitions

At present, the installation compliance metrics noted in the previous section vary between regions. As emergency backstop mechanisms become increasingly important to address NEM-wide challenges, standardised consistent and precise metrics are needed to measure emergency backstop mechanism performance. This avoids confusion between organisations, and supports national consistency and equity in the use of emergency backstop mechanisms.

Emergency backstop mechanism design specifications for management of Minimum System Load conditions

Based on AEMO's experiences integrating emergency backstop mechanisms into MSL operational processes, key emergency backstop design specifications include rapid response (within ~60 minutes, as a practical initial target), certainty of response and expected behaviours if communications or signals are lost (known as 'fallback mechanisms' in CSIP-AUS implementations).

Consider and design for scalability

Many emergency backstop mechanisms use complex architecture. It is important that scalability is considered, projecting forward to potential scenarios where these mechanisms may be utilised simultaneously across the NEM to manage power system security in multi-region MSL conditions, or across the SWIS to manage operational demand above the MDT.

For all emergency backstop mechanisms, pathways need to be designed and resourced to provide high visibility to identify and resolve performance issues that may be encountered for at-scale activations of the emergency backstop mechanism. This is particularly important as emergency backstop expands to include hundreds of thousands of DER devices, growing to potentially tens of millions in some DNSP (and utility, in the case of Synergy) areas.

Other learnings for specific types of emergency backstop mechanisms

Other learnings that apply to specific types of emergency backstop mechanisms are summarised in Table 1.

Table 1 Summary of learnings for other emergency backstop mechanisms, including smart meters

Emergency backstop mechanism	Details
SCADA control	• SCADA control is an effective method for managing emergency backstop mechanism delivery from larger PV systems (such as photovoltaic non-scheduled generation [PVNSG]). • A portion of PVNSG sites appear to self-curtail in response to low wholesale prices.

Emergency backstop mechanism	Details
Smart meters	• Smart metering systems may support DER monitoring and emergency backstop mechanism functionality with scalability advantages. However, diverse configurations and current infrastructure limitations mean that confirming correct installation remains important and may be practically challenging. • To support effective implementation and safeguard core market functions, it is preferable that technical requirements for smart meters are integrated within the National Electricity Rules (NER) framework. Introducing requirements outside the framework may create implementation challenges and could complicate broader metering framework development. • The upcoming Flexible Trading Arrangements rule implementation may enhance the ability to separately measure and manage DER.
Generation Signalling Devices (GSDs)	• Where installed properly, GSD approaches use an established capability for delivering emergency backstop mechanisms, and are therefore more likely to be robust, reliable, cybersecure, and produce rapid at-scale delivery, with reduced risks of scalability challenges. • However, GSD approaches appear to be vulnerable to the same challenges identified for all emergency backstop mechanisms around poor installation compliance. • Significant installer engagement and education is required if new requirements are introduced.
Emergency voltage management (EVM)	• EVM can provide a large bulk response, with capabilities potentially introduced in a short timeframe, and has been a crucial mechanism for maintaining power system security in South Australia on two occasions. The large EVM response available in South Australia has allowed time for learning-by-doing in the staged rollout of active DER management. • DNSPs need to assess risks and conduct modelling, testing and/or trials as necessary to confirm this option is suitable for their network (including consideration of relevant regulations and legislation) and maximise capabilities, while ensuring safety and low risk to customer equipment.
Shedding of reverse flowing feeders	• If sufficient emergency backstop capability is not available, the only mechanism remaining to maintain system security is to shed entire distribution feeders that are in reverse flows. This involves loss of supply to the feeder and has very high customer impacts, and thus should only be used as a last resort measure when all other options have been exhausted. • Development of new schedules and processes are required to efficiently shed reverse flowing feeders if necessary, at the most granular level possible to minimise customer impact and maximise benefits. • Improvements may be required to deliver adequate visibility of reverse flows, and to facilitate automation and efficient rapid response in a complex power system event.

Recommendations

Table 2 summarises recommendations based on the learnings in this report.

Table 2 Recommendations

Stakeholders	Key actions
Governments	• Ensure regulatory frameworks in all NEM mainland regions that deliver capabilities to manage system security in extreme low demand conditions. • Ensure regulatory frameworks allow for regular at-scale testing of emergency backstop.
Governments and DNSPs	• Allow for the long lead-times for implementing operationally effective active management of DER at scale, with significant resourcing for change management frameworks and industry collaboration, engagement and support. Given that operational timeframes are urgent in the NEM mainland regions[A], this may mean progressing other complementary activities to deliver the necessary capability, including the possibility for expanded use of EVM if deemed appropriate for the network. • Consider opportunities for consumer engagement around the positive opportunities from increased CER coordination. • Develop engagement frameworks and incentives to support high installation compliance to emergency backstop mechanisms.
DNSPs	• In implementing emergency backstop measures, continue to draw on the considerable learnings from experiences to date (including but not limited to those outlined throughout this report), and continue active knowledge sharing between DNSPs. • Where feasible, design for: – high scalability of emergency backstop mechanisms, and – installer portals and systems to provide automatic notifications to installers (for example, if capability testing challenges are encountered), and – systems for data collection and provision to support consistent understanding of emergency backstop response rates across the NEM. • Prepare suitable schedules and processes to efficiently shed reverse flowing feeders if necessary, as a last resort measure, at the most granular level possible.
DNSPs and Australian Energy Regulator (AER)	• Anticipate significant levels of resourcing required to successfully implement emergency backstop mechanisms at operational scale, particularly for stakeholder engagement and support, scalable emergency backstop design and implementation, and testing to confirm correct setup to receive signals from the emergency backstop mechanism at the time of installation.
AEMO (with DNSPs, TNSPs, OEMs and other technology providers)	• Establish processes for routine at-scale testing of emergency backstop mechanisms across all NEM mainland regions.
All industry	• Continue to work towards national consistency in implementation of standards (such as CSIP-AUS), considering costs
Regulatory bodies	• Consider possible reform pathways to recognise and address governance gaps in: – defining and managing emergency backstop performance, – roles and responsibilities of assessing, enforcing and rectifying DER/CER compliance and conformance[B] with standards, such as emergency backstop and AS4777.2:2020, and – roles and responsibilities for ongoing customer protection, including ensuring return to service and continuity of connectivity. • Develop pathways to account for the important role of OEMs and other technology providers of active DER management (particularly for internet-based emergency backstop), and CER/DER integration and orchestration more broadly. OEMs and technology providers are now playing an essential and active role in real-time power system operation.

A. See https://wa.aemo.com.au/initiatives/major-programs/nem-distributed-energy-resources-der-program/managing-distributed-energy-resources-in-operations/managing-minimum-system-load.
B. The difference between conformance and compliance is outlined at https://www.safeworkaustralia.gov.au/law-and-regulation/duties-under-whs-laws/australian-and-other-standards.

Contents

Tables

Figures

1 Introduction

1.1 DER work programs

In July 2024, Australia's Energy Security and Climate Change Ministerial Council agreed on a National CER Roadmap[25], building on advice from the ESB around critical technical capabilities for ongoing power system security. The CER Roadmap sets out an overarching vision and plan to unlock CER at scale and identifies measures to "unleash the full potential of CER" by establishing the required mechanisms, tools and systems. This includes both:

- reforms to increase the opportunities for market participation of CER, including through enhanced coordination, allowing customers to respond to market-based incentives which will also help meet the challenges of low operational demand, and
- measures to support ongoing power system security, particularly the requirement for emergency backstop mechanisms to be in place by the end of 2025 for emergency response to ensure the operational security of the power system when required.

Effective integration of CER will require the intersection of power system engineering, technological innovation, consumer choice and experience, and government policy and regulation.

Significant progress has been made already to unlock CER opportunities. Several workstreams have progressed under the National CER Roadmap, with outputs including consultation papers on CER Data Sharing Arrangements[26] and Roles and Responsibilities for Power System and Market Operations in a High CER Future[27]. These workstreams aim to embed an effective foundation for coordination of CER. Likewise, the Engineering Roadmap Priority Actions update[28] highlights progress on initiatives including EV standards, improved compliance, flexible trading arrangements and integration of price-responsive resources. In the SWIS, AEMO continues to progress initiatives such as Project Jupiter[29] alongside the SWIS Engineering Roadmap[30], and will continue to contribute to the Western Australian Government's DER Roadmap[31]. Some of the capabilities discussed in this report provide a foundation to unlock these future pathways for better utilisation of DER devices for customers, for example by facilitating CER orchestration or flexible solar exports.

[25] At https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf.

[26] Australian Government, Department of Climate Change, Energy, the Environment and Water, National Consumer Energy Resources (CER) Roadmap – Data Sharing Arrangements – M2, https://consult.dcceew.gov.au/national-cer-roadmap-data-sharing-arrangements-m2.

[27] Australian Government, Department of Climate Change, Energy, The Environment and Water, National Consumer Energy Resources (CER) Roadmap – Redefine roles for market and power system operations – M3/P5, https://consult.dcceew.gov.au/national-cer-roadmap-redefine-roles-m3-p5.

[28] AEMO, Engineering Roadmap Strategy and Progress Reports, https://aemo.com.au/initiatives/major-programs/engineering-roadmap/reports-and-resources.

[29] More information on Project Jupiter is at https://aemo.com.au/initiatives/major-programs/wa-der-program/project-jupiter.

[30] In the SWIS, the Engineering Roadmap is to carry out assessment of any need to expand requirements for emergency backstop capabilities. More information about the Engineering Roadmaps is at https://aemo.com.au/initiatives/major-programs/engineering-roadmap.

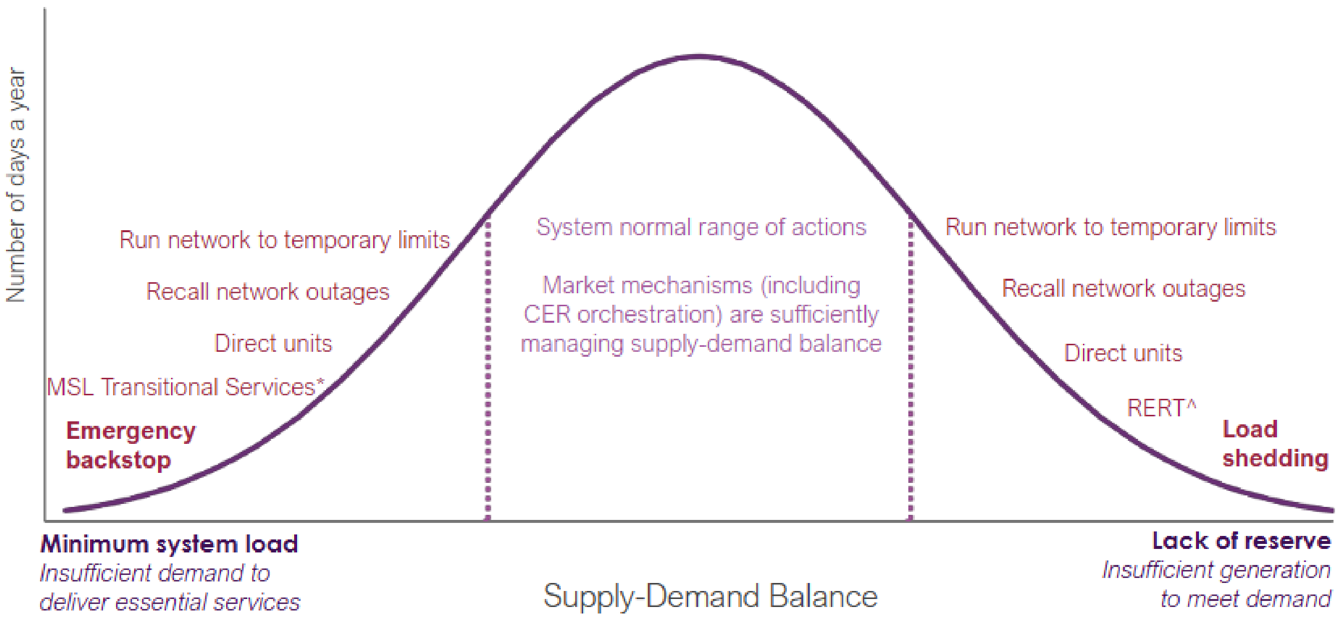
[31] Government of Western Australia, *Distributed Energy Resources Roadmap*, https://www.wa.gov.au/government/distributed-energy-resources-roadmap.

1.1.1 Other measures to support secure operation during low demand conditions

Emergency backstop mechanisms are just one element of a suite of measures required to ensure power system security can be maintained during MSL conditions in all NEM mainland regions[32,33], and when demand is reaching MDT in the Western Australian WEM[34,35]. Figure 1 provides a graphical illustration, with further detail in AEMO's previous reports[36].

Increasing the availability of other measures to maintain system security reduces the instances where emergency backstop mechanisms need to be used, but does not replace the need for these tools to exist. This report focuses on learnings for emergency backstop mechanisms because it is a foundational element required relatively early to support secure operation. Significant other workstreams are also in progress in parallel, and considerable work far beyond emergency backstop is required across a wide range of areas.

Figure 1 Suite of measures to ensure power system security during extreme conditions in the NEM



* Work on procurement of this measure is ongoing: https://aemo.com.au/consultations/tenders/minimum-system-load-transitional-services-for-victoria-and-south-australia.
^ RERT refers to the Reliability and Emergency Reserve Trader, a NER mechanism for AEMO to contract capacity electricity reserves when a reserve shortfall is projected up to nine months in advance.

[32] AEMO (Q4 2024) Supporting secure operation with high levels of distributed resources, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en.

[33] In accordance with AEMO's responsibilities under NER 4.3.1(n), to refer information of which AEMO becomes aware in relation to significant risks to the power system where actions to achieve a resolution of those risks are outside the responsibility or control of AEMO.

[34] Government of Western Australia, Distributed Energy Resources Roadmap, https://www.wa.gov.au/government/distributed-energy-resources-roadmap.

[35] Government of Western Australia (July 2024), Distributed Energy Resources Roadmap, Third Progress Report, https://www.wa.gov.au/system/files/2024-07/248948epwaderrroadmap26_july.pdf.

[36] Including Section 2 of AEMO's Q4 2024 report, *Supporting secure operation with high levels of distributed resources*, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en.

1.1.2 Emergency backstop capabilities

'Emergency backstop' capability refers to operational measures to reduce aggregate DER generation if required for system security, when other options have been exhausted. This is a critical tool to keep the power system secure under extreme conditions before higher customer impact measures are enacted.

If sufficient emergency backstop capability is not available, the only mechanism remaining to increase operational demand to the levels required are measures with higher customer impact, such as EVM[37] to deliberately increase voltage and curtail distributed PV generation, or shedding entire distribution feeders that are in reverse flows. This sheds all consumer load on the feeder, and therefore has a very high impact on homes and businesses.

1.2 Purpose of this report

This report recognises the considerable effort that has been invested by DNSPs, utilities, state and territory governments, technology providers, OEMs and others across industry to implement emergency backstop in South Australia, the Western Australian SWIS, Victoria and Queensland to support secure power system operation in periods of high generation from DER. It aims to:

- consolidate and draw on common learnings across all jurisdictions, highlighting key challenges observed and solutions that have been developed and refined over time,
- support jurisdictions, networks, central utilities, OEMs and industry in resourcing for and achieving operationally effective emergency backstop capabilities[38], including regions which are starting their journeys and those working on uplift of capabilities,
- highlight some key governance gaps that have become apparent, as a basis for consultation and collaboration with stakeholders on possible solutions to address these gaps, and
- build a transparent consolidated resource, and support national consistency (such as commonly agreed performance metrics and standards).

This report is published in accordance with AEMO's responsibilities under National Electricity Rules (NER) 4.3.1(n) and (v), to provide information to participants in relation to a significant risk to the power system and to initiate action plans to manage any abnormal situations or significant deficiencies which could reasonably threaten power system security.

1.3 Methods for delivering emergency backstop capability

There are a range of different methods that have been explored to date in Australia for enabling emergency backstop capability, as summarised in Table 3. Insights and analysis shared to date with AEMO on each of these methods are discussed in the following sections. Key themes have emerged multiple times across different jurisdictions and different DNSPs, discussed in sections 2 and 3.

[37] As different DNSPs use different terms for this based on technology type, this report uses the term 'emergency voltage management' (EVM) for clarity and consistency. Where a different term is used by the DNSP it is noted in the accompanying text.

[38] In accordance with AEMO's responsibilities under NER 4.3.1(n).

The various different delivery pathways for implementing emergency backstop capabilities are discussed in the following categories:

- **Internet-based mechanisms** – computer servers are used in one or multiple stages ('hops') to deliver active DER management signals via the internet to hundreds of thousands of individual DER sites. OEMs and other technology providers of active DER management play an important role. Internet-based methods are used in:
  - emergency backstop via Common Smart Inverter Profile – Australia (CSIP-AUS)[39] implemented in South Australia via Flexible Export Limits (FELs) and Victoria via the Victorian Backstop Mechanism (VBM), in the early stages of rollout in the SWIS, and incoming in the New South Wales Emergency Backstop Mechanism (EBM) and the proposed Australian Capital Territory EBM,
  - a proprietary application programming interface (API) platform used in the SWIS in Western Australia[40], and
  - most Relevant Agent (RA) technology providers in South Australia.

  Present implementations of these mechanisms typically utilise OEM (or other technology providers of active DER management) servers and platforms to convey signals to DER devices. A central server or platform at the utility is also often used (for example, CSIP-AUS utility servers).
- **Generation Signalling Devices (GSDs)** – devices connected at a customer's site that enable the inverter to receive a signal to activate a standardised demand response mode which disconnects the DER inverter.
- **Smart meters** – smart meters[41] have been included in their own category as they sit separately in the regulatory framework and have existing infrastructure and NER obligations related to operation and settlement of the retail market. Smart meters are capable of communicating via internet-based technologies as well as audio frequency load control (AFLC) communications pathways.
- **SCADA control** – SCADA control utilises DNSP SCADA systems to send a curtailment signal to PV systems.
- **Further mechanisms to ensure system security** – these measures have higher customer impacts and include EVM[42] and, as a last resort for management of system security when other options are exhausted, shedding of whole reverse flowing feeders (which interrupts electricity supply to consumers on those feeders).

Table 3 notes which of the various emergency backstop mechanisms are internet-based, since there are some common learnings that apply to all internet-based solutions, as discussed in section 3.

[39] The CSIP-AUS was developed by the DER Integration API Technical Working Group, which aimed to develop a consistent technical approach to communicating dynamic export and import limits between DNSPs and customers or their aggregators. This culminated in the release of CSIP-AUS, an Implementation Guide of IEEE 2030.5. More information on CSIP-AUS is at https://www.csipaus.org/about.

[40] Synergy is intending to progressively roll-out CSIP-AUS capability, with gradual migration from the proprietary API platform to CSIP-AUS servers.

[41] At present smart meters use meshed networks (within Victoria) or 4G (outside Victoria) to provide meter data for settlement to AEMO. While smart meters are capable of using internet-based communications, they are discussed separately to internet-based mechanisms because they sit separately in the regulatory framework, and have existing infrastructure and obligations which make them distinct from internet-based mechanisms such as CSIP-AUS.

[42] This term refers to the deliberate increase in voltage to curtail DER during extreme conditions. As different DNSPs use different terms for this based on technology type, this report uses the term 'emergency voltage management' (EVM) for clarity and consistency. Where a different term is used by the DNSP it is noted in the accompanying text.

Table 3 Methods for enabling capabilities for emergency backstop and complementary measures

Region	Overview of emergency backstop mechanisms or complementary measures in place	Internet-based solution?
SA	**SCADA control:** Since 2017, new PV sites exporting ≥ 200 kVA must have curtailment capability via SCADA.	No
	Since 28 September 2020, the South Australian Government's Smarter Homes regulations[A] require new electricity generating plant to have an RA responsible for its active management. This has led to two solutions: • **Relevant Agents (RA)**, since 28 September 2020. Most RA use internet-based technology. • **CSIP-AUS**, in the form of **Flexible Exports (FELs)**, an internet-based mechanism which began rollout on 1 July 2023. FELs has now taken over from RA as the main form of active management for new DER sites in South Australia, with FELs expected to be available to all new DER sites connecting across the state from 17 July 2025.	Yes
	EVM[B], also termed **Enhanced Voltage Management**[C] by SAPN as it is also used to support improved distribution voltage management in normal periods. SAPN has had EVM capability since January 2021, and has used it in two circumstances during challenging operational conditions, where it was a critical tool to maintain system security[D].	No
	Under the Smarter Homes regulations, **smart meters** were also intended to have the ability to remotely disconnect distributed PV.	Potential for internet-based approach
Vic	The **Victorian Backstop Mechanism (VBM)** is implemented under Ministerial Orders[E], and applies for new PV sites >200 kVA from 1 October 2023, and sites ≤ 200 kVA from 1 October 2024. Active management for PV sites ≤ 200 kVA is to be mostly conducted via **CSIP-AUS**[F].	Yes for sites ≤ 200 kVA
	Other emergency backstop mechanisms in Victoria include: • **Embedded generators:** All Victorian DNSPs can curtail some larger distribution connected (embedded) generators in their networks. • **Hot water load shifting:** One Victorian DNSP can shift some customer hot water load to daytime to increase demand if required to manage MSL conditions. Along with a further mechanism to ensure system security, **EVM**[B]: • Since spring 2024, CPUE has had the capability to enact EVM in its network, termed dynamic voltage management systems (DVMS) by the DNSP as they use a specific technology to deliver the capability. • AusNet Services is also implementing upgrades to enact EVM capability for spring 2025, using a range of technologies.	No
WA (SWIS)	Since 14 February 2022, new and upgraded PV systems ≤ 5 kVA which receive buyback payments through the Distributed Energy Buyback Scheme (DEBS)[G] must be on SWIS retailer Synergy's Emergency Solar Management backstop mechanism[H]. At present, >97% of emergency solar management capability is delivered via a proprietary **API platform**, and the remaining 2-3% managed via automated metering infrastructure (AMI). From 2025, Synergy is intending to progressively roll-out **CSIP-AUS** capability, with gradual migration from the proprietary API platform to CSIP-AUS servers.	Yes
	As part of emergency backstop capability, SWIS TNSP and DNSP Western Power can **curtail embedded generation** in its network and **trip off distributed network Private Power Generators** (PPGs).	No
Qld	Energex and Ergon Energy Networks have a technical standard STNW1175 for new HV connected generation 1.5 megawatts (MW) – 5 MW. In this standard there are a range of thresholds for **SCADA** and controlled switching devices. This means that in some cases non-scheduled generation 1.5 MW – 5 MW may be disconnected through a SCADA based scheme as per the standard[I].	No
	Since 6 February 2023, new inverter energy systems ≥10 kVA in Queensland must be installed with a **Generation Signalling Device (GSD)**[J], which enables the inverter to receive a signal to activate a standardised demand response mode which disconnects the inverter. In Queensland this is enacted via a powerline signalling system known as audio frequency load control (AFLC), whereby a signal is initiated from the DNSP substation to disconnect all GSD-enabled inverter energy systems on the relevant distribution zone substation.	No

Region	Overview of emergency backstop mechanisms or complementary measures in place	Internet-based solution?
NSW and ACT	New South Wales/Australian Capital Territory DNSPs can **curtail some embedded generation** in their network, and two New South Wales DNSPs can **shift hot water load** in their networks.	No
	Both the New South Wales and Australian Capital Territory Governments have released consultation papers in Q1 2025, considering the implementation of emergency backstop via **CSIP-AUS** for systems ≤200 kilowatts (kW)[K].	Yes

A. Per the Government Gazette published 24 September 2020, https://governmentgazette.sa.gov.au/2020/September/2020_076.pdf.
B. A range of terms have been used to describe the deliberate slight increase in distribution network voltages outside of the normal range to curtail distributed PV generation during extreme conditions. For consistency and clarity, the term ‘emergency voltage management’ (EVM) is used throughout this report. Where a different term is used by the DNSP it is noted in the accompanying text. EVM can have adverse impacts on customers and equipment if used frequently. It is therefore only recommended for use very rarely, and only if other active DER management methods are exhausted and further action is required to maintain system security.
C. SAPN’s EVM cost pass-through application and the subsequent AER determination is at https://www.aer.gov.au/industry/networks/cost-pass-throughs/sa-power-networks-cost-pass-through-emergency-standards-2021-22.
D. For more information see the incident reports for 14 March 2021 (https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/maintaining-operational-demand-in-south-australia.pdf?la=en) and 12 November 2022 (https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en&hash=A89F330CF6C979E52EF15EB86E5CF058).
E. For example, the latest Ministerial Order found here: State of Victoria 2024, Ministerial Order specifying licence condition 2024, No. S 31 Wednesday 31 January 2024, available at: https://www.gazette.vic.gov.au/gazette/Gazettes2024/GG2024S031.pdf.
F. Some exceptions apply, eg. for solar microgeneration units between 30 and 200kVA which can be remotely interrupted or curtailed without CSIP-AUS. More detail can be found in section 5(2)(b) of the Ministerial Order.
G. An overview of the Emergency Solar Management requirements can be found on the WA Government website here: https://www.wa.gov.au/organisation/energy-policy-wa/information-industry-emergency-solar-management. Exemptions apply for OEMs with less than 300 sites in the SWIS.
H. Synergy is the retailer for all residential (non-contestable) customers in the WEM.
I. Standard is at https://www.energex.com.au/__data/assets/pdf_file/0020/1072550/Standard-for-High-Voltage-EG-Connections-2946177.pdf.
J. Queensland Government, Department of Energy and Climate, Emergency Backstop Mechanism, https://www.energyandclimate.qld.gov.au/about/initiatives/emergency-backstop-mechanism#:~:text=The%20emergency%20backstop%20mechanism%20will%20apply%20only%20to%20new%20and,residential%20and%20commercial%2Findustrial%20customers.
K. Further information for New South Wales can be found in the New South Wales Department of Climate Change, Energy, the Environment and Water (DCCEEW) consultation paper: Emergency Backstop Mechanism and CER Installer Portal (https://www.energy.nsw.gov.au/sites/default/files/2025-02/NSW%20Emergency%20Backstop%20Mechanism%20and%20Consumer%20Energy%20Resources%20Installer%20Portal%20consultation%20paper.pdf) and further information for the Australian Capital Territory can be found in the Australian Capital Territory Government consultation paper: Emergency Backstop (https://hdp-au-prod-app-act-yoursay-files.s3.ap-southeast-2.amazonaws.com/5317/4216/9923/2025_Emergency_Backstop_Capability_Consultation_Paper_FA_access.pdf).

1.4 Scope of this report

1.4.1 Regulatory changes

This report aims to collect lessons learnt in implementation of emergency backstop mechanisms, and reflects a broad range of areas where further work is required, including addressing governance gaps (Section 2.7 and Section 3.3).

A range of ongoing workstreams are underway which seek to develop and improve on governance frameworks for CER and DER. Emergency backstop mechanisms involve a wide range of stakeholders (such as jurisdictions, DNSPs, solar retailers and installers, OEMs and technology providers, and customers), and a key learning from this work has been the importance of consulting and engaging with these stakeholders. Hence, this report aims to articulate observed governance gaps as a basis for consultation with stakeholders through the appropriate channels on how to address these gaps, including the governance or regulatory framework under which these gaps should be considered. Much further work will be required to address these complex and interlinked challenges.

1.4.2 CER and DER technologies

Operationally effective emergency backstop mechanisms are an important component to support secure operation of a grid with large amounts of DER which are not dispatched through the centralised market. DER encompasses CER (consumer resources that generate, store or consume electricity such as rooftop solar, batteries and loads), and also includes other larger installations within the distribution system. This report hence refers to DER except where the term 'CER' is used in governance or other frameworks, or where the specific reference is only to resources owned by consumers[43]. Some jurisdictional instruments through which backstop requirements are applied have exemptions for certain categories of DER, which are defined under the relevant instrument. The general use of 'DER' in this report does not affect these exemptions or the way DER is defined in those instruments.

Where this report provides a present point in time view of lessons learned on implementation of emergency backstop mechanisms, primary focus has been on observations for distributed PV, as the most common type of DER in Australia at present. Technologies are rapidly evolving, with EVs, distributed battery energy storage systems, and smart home energy management systems growing in popularity. These and other diverse types of DER will also need to be considered carefully in future design of emergency backstop mechanisms.

[43] For more details on the differences between CER and DER, see https://www.energy.gov.au/energy-and-climate-change-ministerial-council/working-groups/consumer-energy-resources-working-group.

2 Key learnings for all emergency backstop mechanisms

This section summarises a range of key learnings that have emerged in common across multiple DNSPs, jurisdictions, and emergency backstop technologies.

2.1 Significant resources are required for active and ongoing industry engagement and support

Observations to date indicate that significant resources are required to support effective engagement with industry in the months leading up to, and the years following, emergency backstop implementation, particularly in the following areas:

- **Frameworks for change management, collaboration and engagement** – particularly within regions and organisations, to:
  - ensure consistent engagement and trust-building with all relevant stakeholders, including industry and installers,
  - build clear change management processes with responsible parties, and
  - build a consistent picture on the need for emergency backstop with industry.

  For example, Victoria's Emergency Backstop Reference Group organised by DEECA with Victorian DNSPs and installers and OEM representatives appears to have supported engagement and resolution of early stage implementation challenges to support successful rollout of the VBM. New South Wales DNSPs noted they have been providing joint briefings to industry to align on technical and policy approaches. National change management frameworks can further support consistency, noting different jurisdictions are at different stages of emergency backstop implementation.
- **Installer education and training on the need for emergency backstop mechanisms and changes to installation processes** – to date, all active PV management emergency backstop mechanisms implemented in Australia entail changes or added steps in the installation process, and utilities and DNSPs have noted the importance of installer engagement as a pathway to achieving installation compliance. This may include bringing in Registered Training Organisations into emergency backstop, and increasing access to installation compliance training for apprentices and new entrants in the market.
- **Well-resourced and appropriately technically trained support** – for installers, from DNSPs, OEMs and other technology providers of active DER management, as well as support for OEMs and technology providers in onboarding and server integration. SAPN used a dedicated call centre and noted it was most needed in the first six months following the rollout of its emergency backstop mechanism.
- **Progressive incentives for OEMs/technology providers and installers** – supporting industry to progressively improve installation compliance to emergency backstop mechanisms. For example, SAPN noted it had been able to successfully use its installation portal 'traffic light' system by defining compliance thresholds

that solar retailers must meet to keep installing sites in SAPN's network, and progressively increasing these thresholds over time[44]. In another example, Synergy conducts monthly platform testing of selected OEMs/technology providers on its proprietary API platform for emergency backstop mechanisms, and works with these organisations to resolve performance issues identified in these monthly tests.

- **Industry and public understanding of value** – raising awareness and building a consistent picture on the need for emergency backstop, with a united approach from industry and government bodies, to build social awareness of the need for emergency backstop. In regions where backstop is well established, there were no reports of strong customer concerns raised, noting appropriate consumer protections remain important. Some emergency backstop mechanism implementation pathways also have potential to unlock future capabilities for DER by facilitating CER orchestration or flexible solar exports. Engaging with industry and the public about this broader value can help smooth the pathway for emergency backstop mechanisms.

2.1.1 Case study: Victorian Backstop Mechanism

The VBM is implemented under Ministerial Orders[45], and for distributed PV sites ≤ 200kVA requires that all newly established or altered connections from 1 October 2024 are enabled for emergency backstop capabilities, with CSIP-AUS used for most systems[46]. Alongside the Ministerial Orders, the Victorian Government also maintains an emergency backstop industry guide[47] intended to support rooftop solar system manufacturers, installers, and retailers to understand and meet the requirements of the emergency backstop[48]. Under the Ministerial Order, DNSPs must develop processes they will follow where the DNSP is not satisfied that a relevant solar installation is emergency backstop enabled.

Emergency backstop rollout and implementation of Ministerial Orders was undertaken in an accelerated timeframe in response to urgent operational power system security risks identified by AEMO. Victorian DNSPs sought approval through a cost passthrough, and the Australian Energy Regulator (AER) approved revenue allowance that included forecast expenditure of $43.45 million in total for Victorian DNSPs for implementation of the VBM[49].

Teething issues were experienced in the first 3-4 months following implementation, with technology challenges and industry confusion and frustration. Solar industry representatives also noted challenges in implementation due to differences in technology setups across DNSPs, while some DNSPs noted consistency had to be balanced against costs of resourcing and longer lead times for implementation. As installers and industry became more familiar with the requirements, VBM implementation has improved considerably, supported by:

[44] SAPN noted that a key component of the 'traffic light' framework relies on the incentive of Small-scale Technology Certificates (STCs), which have a finite life. More information on STCs is at https://cer.gov.au/schemes/renewable-energy-target/small-scale-renewable-energy-scheme/small-scale-technology-certificates.

[45] For example, the latest Ministerial Order is at State of Victoria 2024, *Ministerial Order specifying licence condition 2024*, No. S 31 Wednesday 31 January 2024, https://www.gazette.vic.gov.au/gazette/Gazettes2024/GG2024S031.pdf.

[46] Some exceptions apply, for example, for solar microgeneration units between 30 and 200 kVA which can be remotely interrupted or curtailed without CSIP-AUS. More detail can be found in section 5(2)(b) of the Ministerial Order.

[47] At https://www.energy.vic.gov.au/households/victorias-emergency-backstop-mechanism-for-solar/industry-guidance.

[48] More information, including the industry guide, is on DEECA's webpage, https://www.energy.vic.gov.au/households/victorias-emergency-backstop-mechanism-for-solar/industry-guidance.

[49] This total is based on publicly released AER determinations on DNSP cost passthrough submissions. Jemena was approved for $8.3 million, AusNet Services for $17.2 million, and CPUE for $17.95 million (for Powercor and United Energy).

- ongoing active engagement by DNSPs with installers and OEMs, including dedicated and technically trained support teams for installers experiencing setup and capability testing challenges,
- a reference group hosted by DEECA which brings together DNSPs and installer and OEM representatives, and
- weekly data reporting by DNSPs that assists in transparently tracking issues and improvement over time.

These engagements, alongside progressive resolution of teething issues, have been successful at improving VBM rollout, with progressive improvements in installation compliance observed. As at June 2025, DNSPs report that ~70-80% of installed sites are now on the VBM[50]. This reflects considerable resources and effort from Victorian DNSPs, industry and DEECA, as well as successful building on learnings from other jurisdictions, for example through SAPN's knowledge-sharing sessions and one-on-one workshops with other DNSPs. Victorian DNSPs noted that the VBM is the first time external vendors of utility servers have used these types of systems for this purpose at scale internationally, and they expect increased maturity, scalability and reliability over time.

Multiple Victorian DNSPs noted challenges with the VBM rollout were exacerbated by national governance gaps in emergency backstop management and coordination, and they had no clear regulatory 'levers' to support or implement compliance and enforcement frameworks. In one example, a Victorian DNSP attempted to draft an agreement for OEMs to provide an agreed level of service and reliability, but found there was no regulatory mechanism to implement this in its network. DNSPs noted this governance gap is pressing and should be resolved in the near to medium term (12 months). AEMO and DNSPs are providing input and advice into a range of ongoing workstreams to address governance gaps related to emergency backstop, discussed in Section 2.7.

All Victorian DNSPs have published documentation to support industry and public understanding of the value of VBM as a foundational piece for transition to improved CER integration (such as flexible exports). AusNet Services' 2026-31 Electricity Distribution Price Review (EDPR) submission on CER strategy[51] notes that capabilities developed to meet the new VBM requirements mean transition to Flexible Exports for all AusNet Services customers from 1 July 2026 comes at a lower incremental cost. Jemena's Grid Stability and Flexible Services Program[52] also notes that DER emergency backstop capability is foundational for the support of flexible exports. Flexible export is also raised in CPUE's 2026-31 EDPR[53] which notes that customers believe in the benefits of flexible exports as a means to maximise solar energy output and support future sustainability.

2.1.2 Case study: South Australian Relevant Agents (RA) and Flexible Export Limits (FELs) mechanism

Active management of new electricity generating plants has been a requirement under the South Australian Government's Smarter Homes regulations[54] from 28 September 2020. SAPN initially implemented these requirements under the RA mechanism, which like the VBM was rolled out under urgent timeframes. Within six

---

[50] Based on data provided by DNSPs to DEECA on the capacity of sites connected to their VBM servers, and AEMO's analysis of Clean Energy Regulator Register (CERR) data on the installed capacity of sites installed in Victoria.

[51] At https://www.aer.gov.au/system/files/2025-02/ASD%20-%20AusNet%20-%20CER%20Integration%20Strategy%20-%2031%20Jan%2025%20-%20PUBLIC.pdf.

[52] At https://www.aer.gov.au/system/files/2025-02/JEN%20%E2%80%93%20RIN%20%E2%80%93%20Support%20%E2%80%93%20Grid%20Stability%20and%20Flexible%20Services%20Program%20%E2%80%93%20Investment%20Brief%20%E2%80%93%2020250131.pdf.

[53] At https://media.powercor.com.au/wp-content/uploads/2024/09/09130856/Draft-proposal-2024-part-B-CitiPower.pdf.

[54] Under the regulations, customers installing or upgrading solar systems in South Australia were required to appoint an RA, who is responsible for enacting active DER management when instructed to do so by SAPN during extreme conditions, as per the Government Gazette published 24 September 2020, https://governmentgazette.sa.gov.au/2020/September/2020_076.pdf.

months, RA capabilities were used to maintain power system security in South Australia on 14 March 2021[55], and RA is still in use for legacy systems. RA use a variety of technology pathways (most of which are internet-based mechanisms) to conduct curtailment.

In part to address installation compliance and visibility challenges in the RA mechanism, new DER installed from 1 July 2023 have been progressively managed using FELs. For sites using FELs, the Flexible Exports mechanism fulfils the role previously served by the RA, enabling active management of DER exports. SAPN anticipates that from 17 July 2025, FELs will be available to all new DER sites connecting across the state.

FELs uses CSIP-AUS and leverages capabilities SAPN had sought and obtained revenue allowance for in its 2020-25 reset period under its low voltage (LV) management program. The AER approved a revenue allowance that included forecast expenditure of $30.3 million for the program[56], which included FELs as a means to increase DER hosting capacity and avoid costs of other network augmentation[57].

Since 1 December 2017, all sites with new DER in South Australia have a 5 kilowatts (kW)/phase static export limit. However, customers installing new DER in an area eligible for FELs could choose:

- a 1.5 kW/phase 'fixed export' limit[58], or
- FELs, which allowed export to a higher level of 10 kW/phase, with export reducing to 1.5 kW when needed for local network stability, or 0 kW when needed for system security.

Customers hence saw value in FELs in the form of higher exports, and SAPN data shows ~85-90% of eligible customers choose FELs[59].

Even with network conditions which incentivised customers towards FELs uptake (through higher export limits), SAPN records show it took over 20 months of rollout (1 July 2023 to 1 May 2025), alongside considerable resourcing efforts from SAPN and engagement with OEMs and installers, for installation compliance[60] to increase to more than 80%. Observed improvements in emergency backstop performance under FELs represent 4-5 years of ongoing development and refinement by SAPN in implementation of active DER management.

[55] AEMO (November 2021), Maintaining operational demand in South Australia on 14 March 2021, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/maintaining-operational-demand-in-south-australia.pdf?la=en.

[56] Based on SAPN's revised proposal supporting document 5.14 DER management expenditure (https://www.aer.gov.au/system/files/SAPN%20-%20Revised%20Proposal%20-%205.14%20-%20DER%20Management%20Expenditure%20Overview%20-%20December%202019.pdf) and the final AER decision on SAPN's 2020-2025 revenue reset (https://www.aer.gov.au/system/files/Final%20decision%20-%20SA%20Power%20Networks%20distribution%20determination%202020-25%20-%20Overview%20-%20June%202020_2.pdf). All other documents on the reset are at https://www.aer.gov.au/industry/registers/determinations/sa-power-networks-determination-2020-25.

[57] As noted in pg. 7 of SAPN's revised proposal supporting document, 5.14 DER management expenditure (https://www.aer.gov.au/system/files/SAPN%20-%20Revised%20Proposal%20-%205.14%20-%20DER%20Management%20Expenditure%20Overview%20-%20December%202019.pdf).

[58] SAPN documentation and websites use the term 'fixed export' for sites which choose a constant 1.5 kW/phase limit at all times. Other regions have used other terms; for clarity, the term 'static export' is used throughout this report to refer to sites which have a limit on the amount of DER generation they can export into the grid at all times.

[59] More information is at SAPN's website, https://www.sapowernetworks.com.au/your-power/smarter-energy/flexible-exports/fixed-v-flexible/.

[60] In this context, installation compliance means the site has chosen FELs and passed capability tests, which confirms correct setup with the CSIP-AUS server.

2.2 Balance gradual rollout pathways against urgent operational needs

Delivery of rapid emergency response across hundreds of thousands (and growing to tens of millions in some networks) of DER sites is inherently complex, and rollouts conducted in compressed timeframe to meet urgent operational needs may result in industry frustration. The benefits of allowing time for a progressive and gradual ramp-up need to be balanced against the requirement for operationally effective emergency backstop measures to be implemented in all NEM mainland regions as quickly as possible[61]. Complementary measures which can be implemented in a shorter timeframe and deliver a significant amount of emergency response may help fill the gap.

2.2.1 Options for staged roll-out emergency backstop mechanisms

To allow time for DNSPs, installers, OEMs and other technology providers of active DER management to learn-by-doing, staged ramp-up of the mechanism alongside clear expectations and reasonable targets that escalate in a predictable manner over time appear to aid in supporting effective emergency backstop rollout. There are a range of options for staged ramp up, which could be used separately or in combination, as summarised in Table 4.

Table 4 Options for staged ramp-up of emergency backstop mechanisms

Area	Description	Examples
Proportion of DER sites covered by the mechanism	The emergency backstop mechanism could apply to a small proportion of sites initially, growing progressively over time towards full inclusion of all customers. The ramp up could be via: • **Opt-in initially** - Initially allowing customers to opt-in to the mechanism (growing to mandatory full coverage of all customers over time). This may need to be partnered with incentives (eg. through programs) for participation in the initial opt-in phase. • **Exemptions** – Some complex sites could be considered exempt, alongside clear indication of how much they should export (eg. low static export limits).	In Victoria, there was an opt-in phase for solar systems with CSIP-AUS inverters through voluntary participation in the Solar Homes rebate program, which preceded the requirements in the Ministerial Order by several months. In addition, sites without internet are exempt from the VBM, but required to have a low static export limit under the Ministerial Order.
Installation compliance thresholds	The mechanism or guidance to support the mechanism can define metrics, targets and systems for installers and OEMs regarding: • The minimum proportion of their fleet which are required to be confirmed as properly set up and responding correctly to a curtailment signal (passed capability tests), in order for installations to continue. • The targets can be set low initially (allowing for teething issues), and grow progressively over time as installers and OEMs gain experience and have time to uplift their systems and processes. Some DNSPs note this is best supported by clear governance frameworks on which parties are responsible for measuring, ensuring, reporting on, and rectifying compliance.	This approach is being applied in South Australia under the installation portal traffic light system.

2.2.2 Complementary measures to deliver emergency backstop capabilities

Mindful of the extensive timeframes involved in setting up an operationally effective emergency backstop mechanism, jurisdictions and DNSPs may need to progress in parallel with exploring other complementary activities to deliver the necessary levels of emergency backstop capability in the timeframes required. This could include **load shifting** – exploring options for increasing load in low demand periods by moving load into the

[61] AEMO (Q4 2024) *Supporting secure operation with high levels of distributed resources*, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en.

middle of the day. Some DNSPs have identified opportunities to increase this capability by using hot water load shifting. There may also be potential to utilise distributed battery energy storage systems (BESS) or other controlled loads for load shifting, or to retrofit controls on some larger existing DER systems (this would likely require incentive frameworks for these customers).

Depending on timeframes and operational risks, this could also include further options that have higher impacts on consumers, such as:

- **EVM** – investigating the possibility for expanded use of EVM to curtail distributed PV generation under extreme conditions. This mechanism may have potential to provide a large bulk response, delivered in a short timeframe, and has been a crucial mechanism for maintaining system security in South Australia on two occasions. The large EVM response available in South Australia has allowed time for learning-by-doing in the staged rollout of active DER management. DNSPs need to assess risks and conduct testing and trials as necessary to confirm this option is suitable for their network and maximise capabilities, while ensuring safety and low risk to customer equipment. This is discussed further in Section 7.1.
- **Reverse flow feeder shedding** – all DNSPs should prepare schedules, processes and tools for efficiently managing shedding of reverse flowing feeders. To minimise customer impact, this is best performed at the most granular level possible, which requires DNSP preparation. This is discussed further in Section 7.2.

These mechanisms are higher impact to customers, and are intended to “buy time”, ensuring adequate tools remain available to maintain system security while the complex and challenging task of implementing operationally effective active DER management is progressed.

2.3 Installation compliance frameworks are a key component for operational effectiveness

All active DER management mechanisms implemented in Australia to date require a change to the installation and/or commissioning process. Ensuring high compliance at the time of installation is important, since it increases visibility of expected emergency backstop response and avoids the costly need for an installer to return to a customer’s site for rectification.

Key observations on installation compliance to date across Australia:

- **South Australia – RA mechanism** – SAPN noted that this mechanism was rolled out under tight timeframes and did not involve a capability test, so data on installation compliance is not available. However, during at-scale RA activations in November 2022 and August 2024, AEMO analysis finds approximately 30-50% of the RA fleet responded successfully to a curtailment signal, suggesting challenges with installation compliance.
- **South Australia – FELs mechanism** – since 1 July 2023, FELs (which uses CSIP-AUS) has progressively replaced RA as the active management mechanism for new DER sites in South Australia. Based on SAPN’s records, it took over 20 months of rollout (1 July 2023 to 1 May 2025), alongside considerable resourcing efforts, for more than 80% of installed sites which choose FELs to pass capability tests (which confirms correct installation setup).

- **Western Australian SWIS – Proprietary API platform** – as of 2 July 2025, Synergy reports approximately 75%-82% of sites have been installed such that they can receive curtailment signals from Synergy's curtailment platform.
- **Queensland – Generation Signalling Devices (GSD)** – as of May 2025, Energex and Ergon Energy Networks note approximately 71% of sites had the GSD installed, of which 26% were assessed as compliant on first inspection, with non-compliance appearing to be associated with incorrect configuration of the inverter. Compliance of audited sites increased to 59% following notification to the installers and resulting rectification. Energex and Ergon Energy Networks have increased audit rates and tightened guidelines around which sites should be audited, alongside installer engagement and rectification efforts, and note that improvement is beginning to be observed in audits.
- **Victoria – VBM** – from October 2024, the VBM applies to sites ≤200 kVA, and uses CSIP-AUS for the majority of sites. The VBM was implemented on urgent timeframes due to forecasts of Victoria reaching very low levels of demand[62]. DEECA implemented requirements on DNSPs via licence conditions in Ministerial Orders, with sites that claimed exemptions to VBM due to lack of internet required to be on low static exports[63,64]. In recent months, improvements in installation compliance to the VBM have been observed as teething issues are progressively resolved, and as at June 2025 (nine months from implementation) DNSPs report installation compliance rates of ~70-80%[65], an installation compliance rate typically observed in later-stage emergency backstop rollouts (~2-3 years since implementation) in other regions. The speed at which installation compliance rates have improved reflects considerable resources and effort from Victorian industry, DNSPs and DEECA (for example through Victoria's Emergency Backstop Reference Group), as well as successful building on learnings from other jurisdictions, including through knowledge-sharing sessions by SAPN.
- **South Australia – Smart meter guidelines** – the South Australian *Technical Regulator Guideline Smart Meter Minimum Technical Standard and Associated Deemed to Comply Wiring Arrangements*[66] ('the Guideline'[67]) was intended to enable capability for smart meters to separately control and measure solar generation and controlled loads[68]. Analysis of smart meters for FELs sites finds less than 20% of these meters are configured to separately measure solar generation. It is likely that a similar portion (<20%) of smart meters are configured with capability to separately control solar generation. In the absence of significant engagement and rectification measures, this is likely to continue being observed going forward; FELs is now the primary active management mechanism for the large majority of new DER in South Australia, and therefore the main focus for rectification efforts.

[62] AEMO (August 2024), *2024 Electricity Statement of Opportunities*, Section A5, https://aemo.com.au/-/media/files/electricity/nem/planning_and_forecasting/nem_esoo/2024/2024-electricity-statement-of-opportunities.pdf?la=en&hash=2B6B6AB803D0C5F626A90CF0D60F6374.

[63] Data was not available to confirm if sites which claimed exemptions due to lack of internet were compliant to their static export limits.

[64] Sites which applied to connect prior to 1 October 2024 (but were installed after that date) have a valid exemption from VBM requirements.

[65] Based on data provided by DNSPs to DEECA on the capacity of sites connected to their VBM servers, and AEMO's analysis of CERR data on the installed capacity of sites installed in Victoria.

[66] Latest version, Government of South Australia 2020 (June 2022 update), https://www.energymining.sa.gov.au/__data/assets/pdf_file/0005/671972/Technical-Regulator-Guideline-Smart-Meter-Minimum-Technical-Standard.pdf.

[67] The roles and responsibilities of Metering Coordinators, Metering Providers and Electrical Contractors is to ensure compliance with this guideline, so owners or operators of electrical installations comply with the *Electricity (General) Regulations 2012*. At time of writing, the current version of these regulations is 14.3.2024, and is at https://www.legislation.sa.gov.au/__legislation/lz/c/r/electricity%20(general)%20regulations%202012/current/2012.199.auth.pdf.

[68] As noted in Section 5 of the Guideline, https://www.energymining.sa.gov.au/__data/assets/pdf_file/0005/671972/Technical-Regulator-Guideline-Smart-Meter-Minimum-Technical-Standard.pdf.

- **New South Wales – EBM and Australian Capital Territory – Proposed emergency backstop mechanism** – governments in both regions have proposed the implementation of emergency backstop via CSIP-AUS. New South Wales DCCEEW is proposing a unified CER installer portal to act as a framework through which installation compliance with EBM is managed, developed in collaboration with DNSPs and a CER Installer Reference Group[69], and DNSPs note this portal is intended to harmonise installer requirements into one platform. The New South Wales EBM is planned for rollout in 2026. The Australian Capital Territory emergency backstop mechanism is expected to follow a similar implementation pathway to New South Wales, including nationally consistent frameworks[70].

Jurisdictions implementing emergency backstop mechanisms should plan to dedicate considerable resources and mechanisms to support improving installation compliance, including the following:

- **Frameworks for compliance monitoring and management** – for example, SAPN noted its installation portal ‘traffic light’ system, which implemented gradually increasing compliance thresholds for installers and solar retailers, was successful at increasing installation compliance. New South Wales DCCEEW noted that the CER Installer Portal it is developing is intended to be designed in a manner consistent with SAPN’s approach[71].
  - **Incentives** – SAPN noted the STC incentive[72] is a key component of the ‘traffic light’ framework, and STC life is finite. Multiple DNSPs noted gaps in governance arrangements regarding emergency backstop mechanisms must be addressed to enact strong and nationally consistent frameworks for installation compliance monitoring and management, potentially through clear resourcing pathways to support installation compliance monitoring and incentivise high compliance. Energex and Ergon Energy Networks noted that there may be pathways to develop incentives alongside industry accreditation bodies.
- **High visibility of correct commissioning** – some internet-based mechanisms have capabilities to confirm correct commissioning at time of install (for example, via capability testing in CSIP-AUS, or registration processes in Synergy’s proprietary API platform). SAPN observed that the use of CSIP-AUS capability testing in FELs has significantly supported improved installation compliance as compared to RA, which did not have a mechanism to confirm correct setup. For other emergency backstop mechanisms, visibility might be provided post-install through regular and systematic audits. For analog devices such as GSDs this may require a physical site visit. Energex and Ergon Energy Networks noted a requirement for installations >30 kVA that a Registered Professional Engineers of Queensland (RPEQ)-signed off Compliance Report is submitted undertaking that a GSD has been installed and commissioned correctly.
- **Confirm compliance with static export limits** – the need for high visibility extends to sites with static export limits. SAPN noted that prior to integration of static limit compliance into its installation portal ‘traffic light’

[69] New South Wales DCCEEW 2025, *NSW Emergency Backstop Mechanism and CER Installer Portal – Consultation Summary*, Section 2.9, https://www.energy.nsw.gov.au/sites/default/files/2025-05/NSW-Emergency-Backstop-Mechanism-and-CER-Installer-Portal-Consultation-Report.pdf.

[70] Australian Capital Territory Government 2025, *ACT Emergency Backstop Capability Consultation Paper*, page 21, https://hdp-au-prod-app-act-yoursay-files.s3.ap-southeast-2.amazonaws.com/5317/4216/9923/2025_Emergency_Backstop_Capability_Consultation_Paper_FA_access.pdf.

[71] New South Wales DCCEEW 2025, *NSW Emergency Backstop Mechanism and CER Installer Portal – Consultation Summary*, Section 2.9, https://www.energy.nsw.gov.au/sites/default/files/2025-05/NSW-Emergency-Backstop-Mechanism-and-CER-Installer-Portal-Consultation-Report.pdf.

[72] STCs were established under the Small-scale Renewable Energy Scheme (SRES); see https://www.energy.gov.au/rebates/renewable-power-incentives.

system, compliance to the static limit was at 40%; following implementation in June 2024, static limit compliance increased to 86% by December 2024.

2.3.1 Case study: Visibility of installation compliance in SAPN Relevant Agents versus FELs

As noted in section 2.1.2, non-CSIP RA technologies were implemented under urgent operational timeframes, which resulted in an approach which did not facilitate confirmation of correct setup at the time of installation (for example, through capability testing). Occasions in which active DER management has been enacted at scale via non-CSIP RA are summarised below.

Table 5 Occasions when RAs were activated

Date	Circumstances	Observations
14 March 2021[A]	Management of power system security	Curtailment observations: • 17 MW via SCADA control • 14 MW via Smarter Homes (RA) • 40 MW via EVM
13-17 and 19 November 2022[B]	Management of power system security	Approximately 30-40% of the RA fleet were observed to respond correctly to the curtailment instruction[C].
22 August 2024	At-scale 'fire drill' test by SAPN	Approximately 49% of the RA fleet was observed to respond correctly to curtailment instruction.

A. AEMO (November 2021) *Maintaining operational demand in South Australia on 14 March 2021*, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/maintaining-operational-demand-in-south-australia.pdf?la=en.
B. Following the initial incident on 12 November 2022. More information on RA performance is in Section 4.2.2 of AEMO's incident report on the event, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en.
C. Noting these responses likely include sites which responded to emergency voltage management (EVM). EVM is estimated to have provided at least two thirds of the required DER curtailment in November 2022, as noted in Section 4.2.4 of the 12 November 2022 incident report, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en&hash=A89F330CF6C979E52EF15EB86E5CF058.

Figure 2 shows AEMO's observations of response rates of the various RA technology providers on three occasions[73]. Different RA technology providers achieve very different response rates, with some achieving total response rates of 80-90% while others demonstrated response rates of only 10-30%. Technology providers used various technologies to manage their sites, and technology provider performance appears broadly consistent across events.

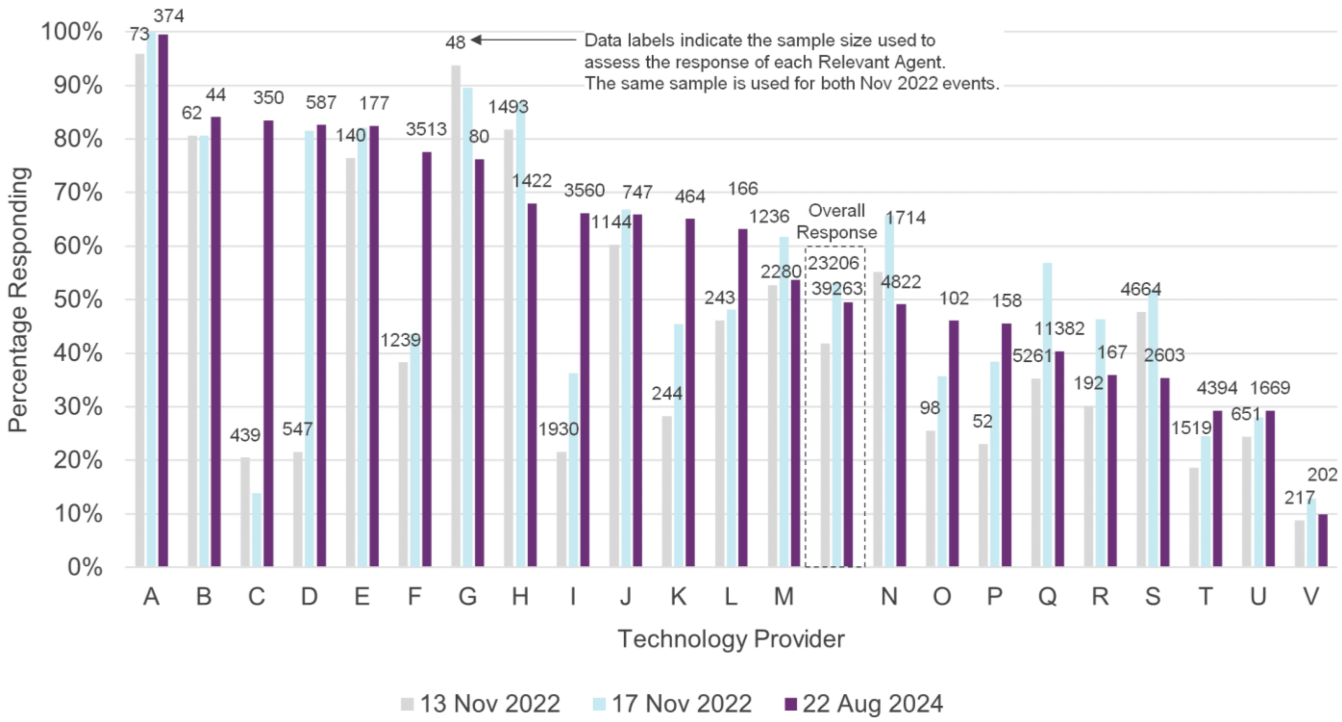
Based on SAPN's investigations, low response rates in the bulk of the RA fleet are attributed to the following:

- **Lack of visibility of installation compliance** – capability testing (confirming compliance at the time of installation) was not conducted to check for correct site setup, so installation compliance could not be confirmed.
- **Scalability challenges** – the RA mechanism used OEM and/or technology provider platforms which do not usually handle large amounts of data. Some of these platforms experienced scalability issues when they received large volumes of curtailment signals during an event, discussed further in Section 2.9.
- **Lack of visibility of site response** – under the RA mechanism, curtailment and reconnection signals were issued once each. Sites which missed the curtailment signal (due to scalability challenges on the

[73] Based on AEMO's independent assessment, in collaboration with SAPN.

OEM/technology provider platform, or customer internet issues) did not curtail. Once the emergency backstop activation period had ended, a small portion of sites also appeared to have delayed return to service, discussed further in Section 2.6. Lack of visibility of response also led to challenges in assessing response to the curtailment signal.

Figure 2 RA response rates to curtailment signal (22 Aug 2024 at-scale test, versus 13 and 17 Nov 2022 events)



Percentage responding was calculated based on:

- For the November 2022 curtailment events: the percentage of systems observed to not export >0.1 kW during the period where RA reported responses on the relevant day. Response rates may be lower than indicated as EVM was also activated in these periods, and some systems may not have been exporting significantly at the time regardless of Relevant Agent signals.
- For the August 2024 'fire drill' test: the percentage of systems observed to curtail export to <0.48 kW/phase within 50 minutes of the curtailment signal.

The observed challenges with RA are contributing factors to why SAPN has progressively rolled out FELs across their network from 1 July 2023. FELs uses CSIP-AUS protocol and features:

- **Improved visibility of installation compliance** – when a new DER site is commissioned, a capability test is conducted while the installer is on the customer site to check for installation compliance. SAPN has visibility of which individual sites pass capability testing.
- **Increased communications** – as part of the FELs mechanism, communications occur every hour between the DER site and SAPN's CSIP-AUS utility server.
- **Visibility of site response** – CSIP-based site telemetry allows monitoring of site responses.
- **Fallback mechanisms** – the CSIP-AUS protocol enables communications loss fallback behaviour, with the site reverting to a static export limit if communication is lost for a period of time[74]. In the event of lost communications, sites behave in expected ways which have been pre-programmed at time of installation, which reduces the impact of lost communications on system security outcomes. As a range of factors may

[74] Loss of communications can occur due to outages on OEM or CSIP-AUS utility servers, changes to customer WiFi or internet.

cause communications loss, consideration of bulk fallback behaviour in the event of large communications outages (for example the unplanned outage of a DNSP utility server) should be considered as part of the fallback mechanism design. During extreme conditions, fallback mechanisms have been demonstrated to support system security, as outlined in the following section.

2.3.2 Case study: FELs enacted on 15 February 2024

On 15 February 2024[75], as part of a range of actions to maintain power system security, SAPN curtailed its entire FELs-eligible[76] fleet. This provides an opportunity to analyse the actual responses of the FELs fleet in a real event. Figure 3 illustrates the breakdown in observed responses from FELs-eligible DER systems during the period when curtailment was enacted[77].

As at February 2024, sites installed in SAPN's network which were eligible for FELs were generating an estimated total of 11.1 megawatts (MW). Of this generation, 4.9 MW of successful curtailment was successfully delivered, with:

- 4.1 MW **successfully curtailed** to close to zero exports (the dotted green box in Figure 3), and
- a further 0.8 MW delivered by systems which **correctly delivered comms loss fallback behaviour** (the dotted teal box). 10% of correctly commissioned FELs sites delivered the "loss of communications" 1.5 kW fallback export limit and minimised the impact of these sites on system security.

These response rates represent the total at-scale response to a curtailment signal via CSIP-AUS. Testing of at-scale response is important to understand the expected operational capability of the emergency backstop mechanism, discussed further in Section 2.5).

Of the remaining 6.2 MW of FELs-eligible DER generation:

- 2.2 MW was related to **self-consumption** (the dotted purple box) – when activated, FELs sites reduced to zero exports, not zero generation. Zero export is an intended design decision in the FELs mechanism.
- 2.0 MW was related to sites which had **not yet passed capability tests** (the yellow bar). This demonstrates the importance of installation compliance in supporting effective operational emergency backstop response.
- 0.8 MW was related to sites which ***passed* capability tests, but did not respond** on the day (the brown bar). This appears associated with scalability challenges, changes to individual site setup, or extended delays in site response. This observation is discussed further in Section 2.5.
- 1.0 MW was related to sites which **chose the static export limit but were non-compliant** to the limit and exported beyond 1.5kW/phase (the red bar).
- In contrast, 0.1 MW was related to exports from sites which **chose the static export limit and were compliant** to this limit. This demonstrates the importance of actively confirming compliance of sites that choose static export limits.

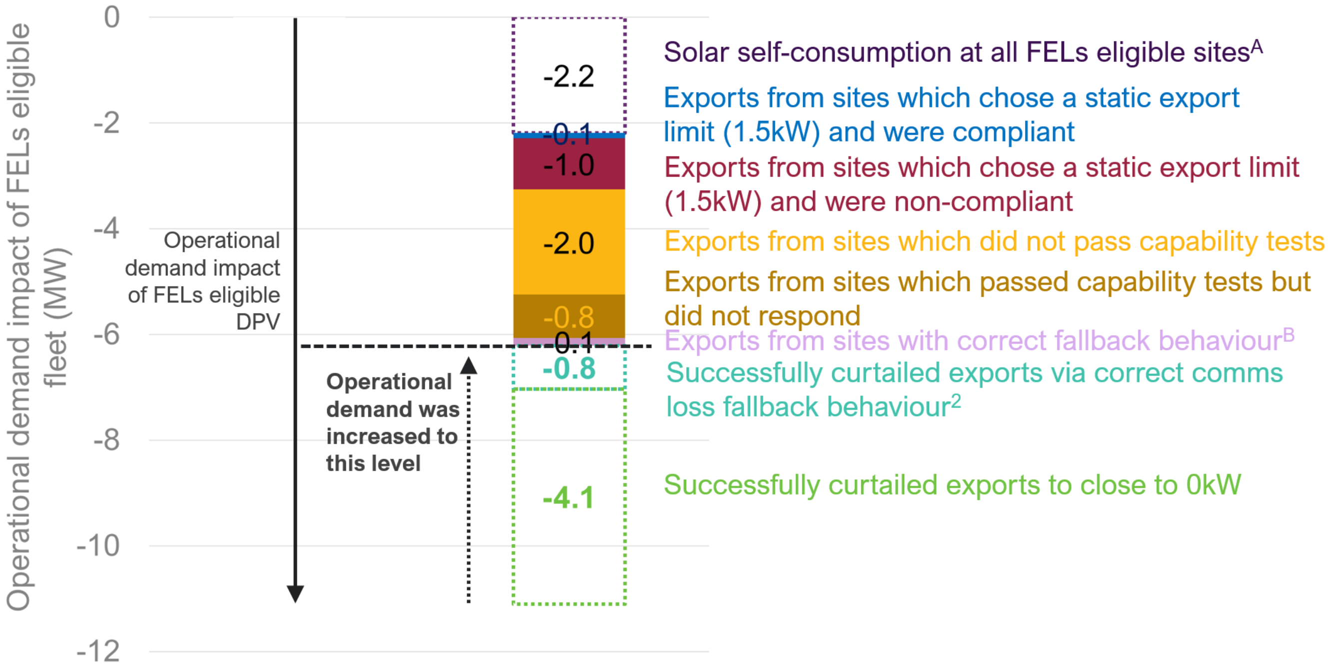
[75] The condition arose two days after a power system incident on 13 February 2024 in Victoria. The final published report on this incident is at https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2024/final-report---loss-of-moorabool---sydenham-500-kv-lines-on-13-feb-2024.pdf?la=en.

[76] The term 'FELs-eligible' is used to refer to sites where the customer was offered the option of FELs (as an alternative to static export limits). The proportion of customers offered this option was progressively increased over time.

[77] Based on records from SAPN and AEMO's independent analysis of smart meter data used for settlement.

SAPN noted that installation compliance has improved since February 2024, and that future enactments of FELs are expected to show progressively higher levels of performance.

Figure 3 Observed responses in SAPN's FELs-eligible fleet on 15 February 2024



Source: AEMO (July 2025), Final Report – Trip of Moorabool – Sydenham 500 kV No. 1 and No. 2 lines on 13 February 2024, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2024/final-report---loss-of-moorabool---sydenham-500-kv-lines-on-13-feb-2024.pdf?la=en.

A. Solar self-consumption continued across all FELs-eligible sites. The FELs mechanism is designed to curtail DER exports only, and when used as designed does not impact DER self-consumption at the site.

B. The FELs comms loss fallback export limit is 1.5 kW at present.

Some key elements presented in Figure 3 are discussed further below, and more detail on the FELs performance analysis is provided in Appendix A1.3.

Testing for installation compliance

For emergency backstop pathways using CSIP-AUS protocol, capability testing is used to provide visibility of whether a site has been correctly set up to receive and act on curtailment signals from the utility server (termed installation compliance in this context). For GSDs, installation compliance testing is carried out by conducting physical audits.

In South Australia, SAPN is focusing efforts on working with OEMs and installers to improve the proportion of sites passing capability tests. SAPN notes from the first implementation of FELs in 1 July 2023, it took ~20 months and concerted effort to improve installation compliance, including through the installation portal traffic light system discussed in Section 2.2.1, for installation compliance to reach 83% in Q2 2025 (that is, 83% of all installed DER sites which chose FELs passed capability tests, indicating the installation was set up correctly to receive curtailment signals).

Assessing compliance to static export limits

In South Australia, customers in areas eligible for FELs choose between a FELs connection or a static export limit of 1.5 kW/phase. Sites on static limits which were non-compliant contributed an order of magnitude more to minimum demand challenges than sites which were compliant to static limits (1 MW of export, shown in the red slice in Figure 3 above, vs 0.1 MW of export for compliant sites).

Compliance to the static export limit in South Australia was low until SAPN undertook a program to include static export limit compliance into the installation portal traffic light system. SAPN noted that following this inclusion, the proportion of sites compliant to their 1.5 kW static export limit increased from 40% in February 2024 to 97% in June 2025.

In Victoria, sites without internet are required under Ministerial Order to have a static export limit applied. Challenges with compliance with static export limits have also been observed in Victoria, with DNSPs observing that some sites appear to be exporting beyond their static export limits. These experiences suggest it is important that there are processes for checking and confirming compliance with static export limits.

Sites compliant to their static limits keep a lower level of export in all periods, not just during extreme conditions, and are an important part of management of low demand conditions because the static export limit reduces downward pressure on operational demand, hence limiting their impact on system security.

If zero export is typically used, capability to reduce solar self-consumption if necessary

Some emergency backstop mechanisms curtail PV sites to zero export, prioritising customer ability to self-consume and reducing customer impact. Zero export delivers a smaller amount of demand increase because solar self-consumption at the site continues. For regions where zero export is typically used and where existing levels of emergency backstop capability are insufficient, including the capability to reduce DER generation from zero export to zero generation in extreme conditions supports system security and avoids the need to undertake actions with higher customer impact, such as EVM or shedding of entire feeders in reverse flow[78].

FELs is designed to curtail sites to zero export, meaning self-consumption continues to occur at the site. As shown in Figure 3, solar self-consumption contributed 2.2 MW of downward pressure on operational demand on 15 February 2024. CSIP-AUS protocols are technically capable of reducing DER to zero generation (for example using 'generation off' commands), but at present this capability has not yet been tested at-scale.

2.4 Apply transparent and consistent reporting and performance definitions

Many different metrics are used to measure emergency backstop implementation progress, and different organisations use different metrics, often because of differences in emergency backstop technology or setup. Lack of clarity in metrics has led to confusion when comparing outcomes between organisations. As challenges

[78] If the site is active in the spot market, reducing self-consumption by curtailing total PV generation at the site to zero may be of benefit to the financially responsible market participant (FRMP) and the customer.

emerge across the NEM and WEM, it becomes increasingly important that consistent and clear definitions are used to discuss emergency backstop.

Consumers continue to install DER across Australia and minimum demand decreases year-on-year. To stay ahead of MSL challenges, during MSL conditions it is important to have capability to manage new DER to the greatest extent practically possible. Operationally effective emergency backstop mechanisms need to provide reliable DER curtailment to a level necessary to keep operational demand above the minimum secure level.

To arrive at a consistent approach to anticipate expected levels of emergency backstop performance across the NEM, one metric that AEMO is suggesting as an initial starting point is shown below:

$$X\% = \frac{\text{MW of generation: Curtailed in 60 minutes} + \text{Foregone due to fallback response} + \text{ Forgone due to static export limits}}{\text{MW of generation: From all sites required to be on emergency backstop mechanisms}}$$

This represents the MW of generation successfully curtailed (including active DER management, fallback response, and static export limits), as a proportion of all generation required to have emergency backstop**,** noting the calculation may require new methods or estimations to provide the required information. AEMO intends to work with DNSPs over the coming months to arrive at a metric that is suitable for across NEM regions.

2.4.1 Assessing performance of emergency backstop delivery

Table 6 outlines various different performance ‘tiers’ of a DER system on emergency backstop and provides an illustrative example. In discussions with NSPs, AEMO has found that many different combinations of these tiers can be used to create different performance metrics of the form below:

$$Z\% = \frac{\text{Tier X}}{\text{Tier Y}}$$

Reporting on emergency backstop installation compliance as a percentage can lead to misinterpretation unless it is defined carefully, since different organisations report on different ratios of tiers. For example, within the same illustrative example outlined in Table 6, the proportion of tier 4 as a ratio of tier 2 (68%) is very different to the ratio of tier 5 over tier 1 (49%). Both percentages reflect the *same* emergency backstop mechanism and ultimately deliver the same level of emergency backstop operational response. However, in the absence of clear definitions, incorrect application of the 68% ‘tier 4 over tier 2’ rate may result in a lower than anticipated response. It is also important to clarify whether response rates are defined on a percentage of numbers of systems, or a percentage of MW. This can also lead to differences when grouping systems of various sizes and with different properties.

Table 6 Tiers of emergency backstop capability: An illustrative example

Commissioning tiers	Description	Illustrative example	
		Sites which curtail during an emergency event	Sites on static exports
Tier 1: All new DER installations which are required to be on backstop	All new DER installed in the network subject to the emergency backstop mechanism. This excludes sites and/or types of DER that have valid exemptions from emergency backstop requirements. For example in Queensland at present, all new installations ≥10 kVA must be installed with a GSD, which means systems <10 kVA would be excluded from this tier.	For every 133 MW of installed capacity of DER required to be on an emergency backstop mechanism: Typical capacity factor during MSL conditions: 75% As distributed PV constitutes the majority of DER at present: assume most DER required to be on backstop is distributed PV ➔ **100 MW of generation** during typical MSL conditions	

Commissioning tiers	Description	Illustrative example	
		Sites which curtail during an emergency event	Sites on static exports
Tier 2: Sites which register to connect to the DNSP network	Sites connecting to the distribution network are required to register with the DNSP. For example, in South Australia, sites connecting to SAPN's network must register on the online registration installation portal. SAPN comparison against a state government register finds ~90-95% of sites register as required.	Assuming 92.5% of sites apply to connect to the DNSP network: **93 MW of generation** during typical MSL conditions	
Tier 3: Sites with active curtailment mechanism applied	In South Australia and Victoria, sites with new DER required to have emergency backstop are either on static export limits, or an active management mechanism. Data suggests ~85% of customers in South Australia are on FELs, and ~90% of customers in Victoria on VBM, with the remaining 10-15% of customers on static limits[A]. Compliance to static limits should be verified, as sites compliant to static limits support system security. In Queensland, Energex and Ergon Energy Networks notes their audits find 70-75% of installations ≥10 kVA are installed with a GSD.	Assuming 85% of sites are on an active curtailment mechanism (T2/T3): **79 MW of generation** during typical MSL conditions	Assuming 15% of sites are on a static 0 kW export limit, and; 80% of these sites are compliant, and; Typical self-consumption during MSL conditions is 10-15% of DER generation: Approximately **10 MW of curtailment** is delivered by static exports in all periods with high distributed PV generation
Tier 4: Sites which are correctly set up to receive curtailment signals	For regions using CSIP-AUS, sites are required to pass capability tests, which are indicative of correct installation setup. As at Q2 2025, SAPN notes that ~80% of sites which choose FELs in their network pass capability tests. In Queensland, Energex and Ergon Energy Networks note that as at June 2025, for 10kVA-30kVA sites, 12% of sites responded on first inspection, increasing to 59% following rectification. For >30kVA sites, Energex and Ergon Energy Networks estimates conservatively that 60% respond[B]. One Victorian DNSP notes that as at mid-2025, ~80% of their sites are passing capability tests and connecting on VBM. In the SWIS, Synergy notes that 73-82% of sites have been installed such that they can receive curtailment signals from their curtailment platform.	Assuming 80% of sites are correctly set up to receive curtailment signals (T3/T4): **63 MW of generation** during typical MSL conditions	
Tier 5: Sites which respond to a curtailment signal	During an at-scale test or extreme condition, these sites respond correctly to a curtailment signal. In two events in South Australia, AEMO has independently confirmed that of FELs sites that are correctly set up: • **70-75%** respond to an at-scale activation, and; • **10-15%** exhibit correct fallback behaviour. Synergy has also observed that approximately **70-75%** of sites correctly set up on their curtailment platform respond to regular at-scale testing (discussed further in section 2.5). As at June 2025, at-scale activations for emergency or test purposes have not been conducted outside of these two regions.	Assume 75% of sites which are correctly set up will respond to an at-scale activation (T5/T4), and; 10% have correct fall back behaviour (to 0kW export), and; Typical self-consumption during MSL conditions: 10% of DER generation **43 MW of active curtailment** Approximately **6 MW of foregone export from fallback**	

Commissioning tiers	Description	Illustrative example	
		Sites which curtail during an emergency event	Sites on static exports
[Tier 6: Depending on mechanism, additional emergency backstop may be delivered by further curtailment to zero generation]	This tier is optional as some emergency backstop mechanisms (eg. GSD, Synergy's proprietary API platform, and mechanisms using 'generation off' commands in CSIP-AUS), already curtail to zero generation in Tier 5. However, for regions where: • active DER management mechanisms are typically set up for curtailment to zero export, and • existing levels of emergency backstop capability are insufficient, Capability to further reduce DER generation from zero export to zero generation may avoid the need to undertake actions with higher customer impact, such as EVM or shedding of entire feeders in reverse flow.	Assuming typical self-consumption during MSL conditions (as in Tier 5) **5 MW of additional curtailment delivered**	
For every 100 MW of DER generation:		**43-48 MW of curtailment delivered in extreme conditions** **Approximately 6 MW of export foregone due to fallback**	**Approximately 10 MW of curtailment delivered from static exports in all high PV generation periods**

A. In South Australia, customers choose between a static limit (of 1.5kW/phase), or active management (via FELs). In Victoria, customers with internet connection are required to be managed via CSIP-AUS, and sites without internet are exempt but must be placed on static export limits. Aggregated data from Victorian DNSPs suggests ~10% of customers are on exemptions, with the remaining ~90% on CSIP-AUS.
B. Audit data for >30 kVA sites will be available towards the end of the year. Energex and Ergon Energy Networks note that response rates are expected to be higher than 60% due to more stringent requirements on >30 kVA sites.

For this example, the initial suggested metric from AEMO needs to understand to anticipate expected levels of emergency backstop operational performance across the NEM as calculated below:

$$X\% = \frac{\text{MW of generation: Curtailed in 60 minutes} + \text{Foregone due to fallback response} + \text{ Forgone due to static export limits}}{\text{MW of generation: From all sites required to be on emergency backstop mechanisms}}$$

$$= \frac{\text{T5 including active curtailment and fallback } (+\text{ T6}) \ + \text{ curtailment from compliant static export sites}}{T1}$$

$$= \frac{43 + 6\ (+5) + 10}{100} = \mathbf{59 - 64}\%$$

AEMO recommends the precise metric be made transparent when reporting emergency backstop performance.

2.4.2 Operational response rates

In the absence of at-scale testing, or an extreme condition where the emergency backstop mechanism is activated, visibility of expected backstop response does not go beyond tier 4 (outlined in Table 6). However, evidence across a range of at-scale emergency backstop activations finds operational delivery of emergency backstop is consistently lower than tier 4 capability.

In regions where at-scale emergency backstop activations have taken place (South Australia and the SWIS), a subset of sites which have been *correctly* set up on the curtailment platform are observed to continue generating at high levels:

- In South Australia, AEMO analysis of smart meter data for 15 February 2024 and the 22 August 2024 'fire drill' test finds that of the FELs sites which were correctly set up (passing capability tests), 70%-75% respond during at-scale activations[79], and 10-15% exhibit fallback behaviour. For more detail see appendix A1.3.
- In the SWIS, Synergy observed that 70-75% of sites correctly set up on their proprietary emergency backstop platform respond to their regular at-scale tests[80].

This indicates that 15-30% of sites correctly set up for emergency backstop continue to generate at high levels across a range of tests and events. This observation underscores the need to conduct regular at-scale tests of emergency backstop mechanisms, discussed further in Section 2.5. The proportion which responds for other emergency backstop mechanisms is not known, as at-scale activations have only been enacted for internet-based mechanisms as at Q2 2025.

2.5 Regular at-scale testing

Regular at-scale testing of emergency backstop mechanisms allows early identification of challenges in emergency backstop operation, prior to needing the mechanism to manage extreme conditions.

At-scale tests provide a best-estimate measure of effective operational response, and mitigate risks of over-estimating emergency backstop capability during an emergency activation. Analysis of at-scale tests finds 15-30% of sites correctly set up for emergency backstop appear not to respond to a curtailment signal across a range of tests and emergency events (Section 2.4.2). This allows development of appropriate actions and decisions to ensure power system security during extreme conditions, which may include complementary measures (Section 2.2.2) if emergency backstop capability is found to be insufficient.

The need for at-scale testing increases for interconnected regions where multi-region activations of emergency backstop mechanisms may be required. For example, a joint MSL condition in Victoria and South Australia may necessitate multi-region emergency backstop mechanism activation across both regions. Since both regions use internet-based mechanisms, interacting with the same OEMs and other technology providers of active DER management, at-scale testing is likely necessary to identify scalability challenges and quantify the extent to which they may impact emergency backstop mechanism performance under extreme conditions.

AEMO's analysis to date indicates that MSL conditions could arise in all NEM mainland regions simultaneously (Queensland, New South Wales, Victoria and South Australia), which could require simultaneous use of emergency backstop capabilities in all these regions. Market-responsive and coordinated CER will reduce the incidence of scenarios where simultaneous emergency backstop activation is required, but do not remove the need for a suitable mechanism to manage extreme scenarios such as outages and extreme coincident low demands across multiple regions. Based on present setups, widespread scalability challenges for such an activation may exist, and co-incident testing of internet-based emergency backstop mechanisms across all NEM mainland regions would support identification and rectification of these issues.

[79] This means that of the 75-80% of correctly commissioned FELs sites, it is expected that 70-75% of those will respond fully to the curtailment signal and reduce export to close to 0 kW at each site.

[80] Independent assessment and verification for the SWIS could not be conducted as AEMO does not have access to non-contestable residential customer meter data in this region.

Implementation of at-scale testing of emergency backstop mechanisms will require significant new processes to introduce routine tests coordinated across all NEM mainland regions, involving AEMO, DNSPs and TNSPs, and consideration of potential regulatory barriers to testing.

To properly identify scalability challenges, tests may need to be performed at scale:

- for each DNSP, and
- for each region (for Victoria and New South Wales, where there are multiple DNSPs in a region), and
- across multiple regions, particularly if there are high risks of needing emergency backstop simultaneously across those regions. This includes conditions where multiple regions are simultaneously involved in a MSL event, and may include extreme conditions where emergency backstop is simultaneously required across all mainland NEM regions (South Australia, Victoria, Queensland and New South Wales).

At-scale tests also support improved coordination between organisations involved in emergency backstop activations (for example, AEMO, TNSPs and DNSPs, particularly for multiple region tests) and facilitates a smooth experience for customers and installers during extreme conditions.

SAPN conducted its first at-scale test of its emergency backstop fleet in August 2024, and the SWIS has a mature testing regime in place for region-wide at-scale tests, discussed further in the following case study.

2.5.1 Case study: Synergy's at-scale end-to-end testing

From 14 February 2022, new DER sites ≤5 kVA in the SWIS which receive buyback payments through the Distributed Energy Buyback Scheme (DEBS) must be able to be actively managed. SWIS retailer Synergy[81] implements this via the Emergency Solar Management scheme.

More than 97% of Synergy's Emergency Solar Management capability is delivered via a proprietary API cloud control platform, with the remainder managed by automated metering infrastructure (AMI). Synergy's testing regime utilises a rigorous testing framework, outlined in Table 7. Synergy's test regimes include:

- **end-to-end at-scale testing conducted twice a year** – prior to the low load (shoulder) seasons, and including coordination across Synergy, Western Power (SWIS DNSP and TNSP), and AEMO. End-to-end testing supports coordination across organisations during extreme conditions, as coordination can be time consuming and non-trivial, and speed of response is a key component of an effective emergency backstop mechanism, and
- **monthly testing for selected OEMs** and other technology providers of active DER management on the API platform.

[81] Synergy is the retailer for all residential (non-contestable) customers in the WEM.

Table 7 Types of tests conducted in Synergy's regular Emergency Solar Management testing regime

Type of test	Details	Sites tested	Period	Test duration
End-to-end at-scale testing	'Fire drill' testing, including coordination with Western Power and AEMO to ensure the entire system operates as designed	Full fleet[A]	Twice a year, prior to low load season (one in Feb/March, one in August)	120-180 minutes
Platform test	Ensure that connected assets can be curtailed and reconnected, with a post-event report being generated by the API platform	Selected OEMs/technology providers	Monthly	60 minutes
OEM/technology provider onboarding	Test successful integration onto platform/server	Onboarded OEM/technology provider	Once-off	As needed
Significant system upgrades or changes	Testing systems impacted by the upgrade	Small-scale testing	As advised by the technology teams responsible at Synergy or Western Power	

A. Including the ~97% of sites in the Emergency Solar Management fleet on the API platform, as well as the ~3% on AMI.

Synergy's last at-scale end-to-end test was conducted 13 March 2025 between 10:30 to 13:30 (WA time). In this test, Synergy estimates 208 MW of installed DER capacity responded. As at June 2025, the latest platform test occurred on 20 May from 09:00 (WA time) and Synergy estimates approximately 247 MW of response across the tested fleet.

Following the platform tests and at-scale end-to-end tests, the API platform generates a post-event report which summarises performance by OEM or other technology providers of active DER management, and Synergy also requests 30-minute interval meter data from Western Power to cross-check site performance in the test[82].

The end-to-end test also ensures the active PV management mechanism is performing as designed, and supports identification of technical issues with activation. If issues are identified that lead to a reduction in the Emergency Solar Management response, Synergy shares with AEMO its progress on investigating and rectifying the cause, or if ongoing issues are observed the capacity of sites experiencing these issues is excluded from expected emergency backstop capability. Synergy also conducts its own internal monthly testing for selected OEMs/technology providers to identify and work with them to fix performance issues with their platforms.

Synergy's tests are important in:

- **Diagnosing and rectifying challenges in delivery of Emergency Solar Management response** – where testing identifies material performance issues, Synergy works closely with the API platform provider and OEM/technology provider to rectify the issue. Until the issue is rectified, Synergy removes the entire OEM/technology provider fleet capacity from the expected response capability. Once the root cause of an issue is identified, small scale testing of systems (typically 2-3 tests) is conducted to ensure the issue is resolved, before reintegration into the main Emergency Solar Management fleet. Regular platform testing is one way to identify and mitigate challenges which impact emergency backstop effectiveness (such as OEM platform response, or system changes and upgrades).

[82] Not all sites can be cross-checked as some sites are still on accumulation meters.

- **Quantifying actual response to curtailment signals** – it is important the quantity of response that will be delivered is well understood (accounting for installation compliance, delays, or scalability challenges), so effective operating procedures can be developed on this basis. Based on responses in at-scale and platform tests, Synergy estimates that 75% of all correctly connected Emergency Solar Management sites typically respond to a curtailment signal. In the March 2025 'fire drill' test, an operational issue was observed for the AMI fleet and 67% of installed capacity on their controllable Emergency Solar Management fleet was observed to respond[83].
- **Establishing coordination pathways between organisations during extreme conditions** – emergency backstop is typically required following a power system incident and/or complex network conditions where control room operators may be managing multiple complex factors. Ensuring well-established coordination pathways between organisations supports the prompt delivery of emergency backstop curtailment signals. The 'fire drill' testing includes coordination between AEMO, SWIS DNSP Western Power, and Synergy and serves the purpose of training for controllers, as well as identifying opportunities to streamline procedures and processes for interactions between organisations.
- **Identifying and fixing sites with delayed return to service** – after testing, the API platform produces a report on sites which failed to reconnect immediately following the test, and Synergy also uses meter data to identify sites with reconnection challenges. Synergy then requests that OEMs/technology providers reconnect these sites. Testing and checking for reconnection behaviour supports identification of characteristics which may make sites vulnerable to delayed return to service, and development of automated methods to reduce the incidence of delayed return to service.

Information regarding tests is made available to customers through their online account and on Synergy's public Emergency Solar Management portal[84]. If customer sites experience issues with return to service following a test, Synergy conducts a structured process to return them to service (discussed in Section 2.6.1). If there are issues still ongoing in the 1-2 weeks following the test, Synergy notifies the impacted customer.

2.5.2 Best practice testing approaches

Based on experiences to date, it is suggested that best practice testing regimes in the NEM would involve the following characteristics:

- Full at-scale system-wide testing performed at least annually. This should be coordinated within the DNSP, and ideally across all regions and DNSPs where emergency backstop mechanisms may need to be activated simultaneously, with appropriate measures in place to limit or manage any operational system impacts from testing.
  - For the NEM, in the near term at-scale testing should be coordinated between Victoria and South Australia simultaneously, with systems in place to expand at-scale testing to Queensland and New South Wales when feasible. This would ideally occur ahead of the lowest demand periods (typically in autumn and spring shoulder seasons) to give an accurate indication of the expected response for that upcoming period.

[83] As an example of the wide range of metrics used to discuss emergency backstop, these metrics are based on installed capacity and are hence different to the values outlined in section 2.4.1, which use DER generation as the base.

[84] Synergy 2025, *Your guide to emergency solar management: ESM low load events and testing,* https://www.synergy.net.au/Your-home/Solar-battery-and-EV/Emergency-Solar-Management/ESM-low-load-events-and-testing.

- Testing performed on a "clear sky" day[85], at a time of day when DER systems are operating moderately, will support clear identification of system responses while minimising step change impacts on the power system. Ideally, the test would end while DER generation levels are high enough to identify systems that do not immediately return to service so these can be rectified promptly.
- The test duration (the period over which the emergency backstop mechanism is activated) needs to extend for a sufficient duration to allow a response to be observed from most systems, accounting for anticipated possible delays in responses. This helps with accurately diagnosing behaviours and operational challenges. For internet-based mechanisms at present, analysis suggests a test duration of at least 60-90 minutes is required.
- Notification requirements which allow flexibility to choose optimal test times and platforms/sites which are of high priority to test, balanced with consideration of consumer protection needs and minimising impacts on customers during testing. Multiple DNSPs have provided feedback that tests which require advance notification to customers may reduce flexibility of emergency backstop testing and impact the ability to choose optimal periods for testing. Some DNSPs noted that notifying installers of at-scale testing supported their ability to support customers that reached out with concerns. AEMO considers that in conducting testing it may be important to be flexible around the test timing aligning with optimal power system conditions and solar insolation levels on the day, and advance notification may mean reduced flexibility.

Test data needed for due diligence verification of emergency backstop capability

There are ongoing processes in progress to review and clarify roles and responsibilities for emergency backstop delivery. For the purposes of this report, given that emergency backstop is a service critical for power system security, it is assumed a responsible party will need to perform an ongoing independent due diligence verification of conformance to expected operational emergency backstop capability. This assessment would need to be nationally standardised, and targeted at confirming sufficient operational response to support secure management of NEM-wide MSL conditions. Whichever party is performing this function will need access to certain datasets. Assessments could be conducted following at-scale testing processes, as well as following operational use of emergency backstop mechanisms (aligning with AEMO's role around investigation and review of major power system operational incidents[86]).

If AEMO is performing this function, the data that would ideally be collected and supplied in the NEM to facilitate an efficient and accurate due diligence assessment would include:

- Lists of National Metering Identifiers (NMIs) on the emergency backstop mechanism, including sites on the active management mechanism and those with static export limits. In the NEM, AEMO has access to NMI-level meter data and details to carry out market settlement, so the only information needed in the near term to conduct consistent and independent verification of expected operational emergency backstop capability is which NMIs are on emergency backstop and/or have export limits applied[87]. In the longer term, with more sites becoming more complex (for example with distributed storage and controlled loads), more granular monitoring capabilities may become required in some cases.

[85] Emergency backstop mechanisms may also be required to manage conditions following equipment damage due to severe weather, which may also impact communications systems. Possible impacts on communications infrastructure under such conditions will need to be accounted for in estimates of available emergency backstop response.

[86] NER 4.3.1(v)

[87] Different functions, governance and regulation apply in the SWIS.

- Accurate standing data for all systems involved in the emergency backstop mechanism, including:
  - installed capacity of the system (kW), and export limit if present, and
  - number of phases.

In the long term, it may be possible to extract some of this data from the DER Register. However, in the near term, there are concerns with data quality and potential gaps in the DER Register which mean independent collection of this data is needed to ensure accuracy. Work is ongoing to address these gaps.

Other data that may be helpful for DNSPs or other organisations implementing emergency backstop to collect:

- Meter data collected via the CSIP-AUS central servers.
- OEM(s) or other technology provider(s) of active DER management at the site.

AEMO recommends that DNSPs aim to design their systems to be able to efficiently extract these datasets in the medium term, acknowledging that setup of data reporting structures and data collection, alongside implementation and design of the emergency backstop mechanism, can be resource-intensive.

Clear data reporting is important to provide assurance of consistent assessment, as many parameters make up a successful emergency backstop response and algorithms which define operational response are complex (for example, thresholds applied for measurement errors, and tests for consistency of curtailment response). As emergency backstop becomes important across the NEM, using one consistent performance assessment algorithm will support equity.

2.6 Confirming return to service

The available evidence suggests that following the use of emergency backstop mechanisms, the vast majority of customer sites return to service without issues. In implementing and applying emergency backstop mechanisms, it is important that systems are established with visibility and monitoring of the return to service status of customer DER, to enable identification of sites experiencing return to service challenges.

Two types of issues have been observed in return to service:

- **Pathway issue** – return to service is impacted by an issue with the emergency backstop technology pathway (for example, if a central platform does not communicate often with the customer DER site, reconnection signals may be missed). These types of challenges typically can be resolved via the DNSP or utility working with the OEM (or other technology provider of active DER management) to reconnect the sites. Technology pathways in which the customer DER site communicates often with the utility server (such as in CSIP-AUS) further reduce the incidence of these types of return to service issues.
- **Complex pre-existing issues** – return to service is impacted by complications at the site, such as a pre-existing issue, hardware failure or a change to the site (for example, the installation of a new device at the customer site which has unexpected impacts on the rest of the site). These types of issues may exist across different types of consumer sites, including those which are not emergency backstop enabled. While these pre-existing issues are unrelated to the emergency backstop pathway, they may become more apparent following an at-scale test of emergency backstop. Resolving these types of issues often requires extensive and resource-intensive troubleshooting.

If sites are not properly and promptly returning to service following use or test of an emergency backstop mechanism, this undermines trust with customers and installers. OEMs and DNSPs have raised concerns that roles and responsibilities around ensuring return to service need to be more clearly defined and developed, with appropriate mechanisms to protect consumer interests.

2.6.1 Case study: Return to service in Synergy's Emergency Solar Management

Synergy conducts regular at-scale testing of its Emergency Solar Management platform (Section 2.5), and estimates ~1-2% of sites curtailed by its proprietary API platform show delayed return to service, due to a range of reasons including gaps in site telemetry and technical issues with third-party and OEM/technology provider platforms. To address this, Synergy has developed a systematic method to identify and reconnect sites with delayed return to service. This operates as follows:

- The proprietary API platform sends an automated email to Synergy with a list of devices (including details of NMIs and the OEM/technology provider) which have failed to immediately reconnect following the test, and Synergy requests that OEMs/technology providers reconnect the devices.
- 30-minute meter data from Western Power is also used to identify sites with delayed return to service which were not diagnosed by the API platform. It takes 2-3 days for Synergy to receive the meter data, and they then cross-validate the data against the API platform. If additional sites with delayed return to service are identified in this stage, Synergy initiates further reconnection requests with the OEM/technology provider.

In both stages, OEMs/technology providers typically reconnect sites within 24 hours. Customers for sites which cannot be reconnected within 1-2 weeks are informed by Synergy that their systems may not be exporting. Synergy has found that some sites which cannot be reconnected have hardware faults, and notes that regular testing supports them in identification of these sites. Synergy's regular processes to identify and return sites to service supports smooth operation of emergency backstop when required in extreme conditions. Synergy is progressively rolling out CSIP-AUS and noted that this technology pathway is likely to reduce the incidence of return to service challenges.

2.6.2 Case study: Benefits of increased visibility to support return to service – RA versus FELs

During previous emergency backstop activations, a small number of (non-CSIP) RA sites have been observed to exhibit delayed return to service. SAPN indicated that this may be due to the structure of some legacy RA technologies, which use a once-off curtailment and reconnection signal. If a site loses communications during the curtailment period, its return to service may be delayed.

Adequate visibility of site behaviour is important to support confirmation of return to service. Introduction of CSIP-AUS capability via the FELs mechanism (discussed in Section 2.1.2) improves visibility through the increased number of communications between the site and the server, and reduces risks of delayed return to service through the loss of communications fallback mechanisms pre-deployed at the site.

On 22 August 2024, SAPN conducted an at-scale 'fire drill' test of its FELs (which uses CSIP-AUS) and RA mechanisms. Following the test, SAPN conducted detection of sites which did not return to service and worked to rectify this with OEMs. Table 8 shows that, of the FELs and RA sites which successfully curtailed during the 'fire drill' test, more than 99.7% returned to export in the week following the test. FELs sites returned slightly faster (99.9% returned to export within one day of the test).

Of the ~28,000 sites which were successfully curtailed across both FELs and RA mechanisms, 26 sites took more than a month to return to export (all 26 sites were RA sites, representing 0.1% of the fleet). Further investigation and rectification for these sites likely requires a site visit and extensive troubleshooting, and at present there is no clear pathway or role to do so. This should be considered under the relevant National CER Roadmap workstreams, including the Consumers workstream.

Table 8 Proportion of sites returning to export following SAPN's 'fire drill' test on 22 August 2024

<table>
<tr><th>Return to full export</th><th>% of FELs (CSIP-AUS) sites</th><th>% of RA sites</th></tr>
<tr><td>Within 1 hour</td><td>95.49%</td><td>84.78%</td></tr>
<tr><td>By the next day</td><td>99.94%</td><td>98.76%</td></tr>
<tr><td>In the week following curtailment</td><td rowspan="2">100.00%</td><td>99.71%</td></tr>
<tr><td>Within the month following curtailment</td><td>99.87%[A]</td></tr>
</table>

A. The remaining 0.13% is from 26 RA sites which took more than one month to return to full export. Of these, 11 returned within three months, nine returned within 6.5 months, and six appear to not have returned to export as at May 2025.

2.7 Address urgent governance gaps in emergency backstop mechanism performance requirements

In building this report, many stakeholders raised a range of governance gaps which have reduced their ability to resource for, support and enforce high compliance in emergency backstop mechanisms. This report intends to note key areas where governance gaps have been observed in emergency backstop operations and implementation.

AEMO has identified areas where clearly defined and monitored operational performance parameters for emergency backstop mechanisms are required. AEMO suggests these parameters are important for an operationally effective emergency backstop mechanism: forecast and actual MW of emergency backstop mechanism response delivered, speed of response delivery, visibility of response, and confirmation of return to service.

Multiple DNSPs have also articulated challenges with emergency backstop mechanism implementation due to governance gaps, including the following:

- A lack of formally assigned roles and processes for emergency backstop mechanism installation compliance monitoring, assessment and enforcement. Addressing this, potentially through inclusion of clear regulatory pathways to provide information on emergency backstop capability and performance, would provide clear 'levers' to support high compliance and address non-compliance (for example, through rectification of installations which do not meet emergency backstop mechanism requirements).
- For internet-based mechanisms using national standards (such as CSIP-AUS), a need for national consistency in areas including:
  - Testing and certification pathways for OEMs (and other technology providers of active DER management) and utility servers to streamline integration and ensure interoperability.

- End-to-end cybersecurity and certificate management mechanisms across technology areas which impact emergency backstop (such as firmware and private key infrastructure).

Clearly defined roles and responsibilities are particularly important because of the number of parties involved (including AEMO, jurisdictions, DNSPs, installers and OEMs) at different stages of emergency backstop mechanism implementation and delivery.

Potential governance gaps raised by various stakeholders as being of immediate concern are summarised in Table 9. Section 3.3 also articulates further governance gaps specific to the role of OEMs and other technology providers of active DER management in delivery of internet-based emergency backstop mechanisms.

Some of these gaps are being addressed through a range of ongoing workstreams, which include:

- national CER Roadmap, including the workstream on Redefining Roles for Market and Power System Operations[88] as well as the National Technical Regulatory Framework workstream, led by the Commonwealth DCCEEW and including extensive industry workshops,
- development of nationally consistent testing and accreditation pathways for CSIP-AUS, including the updated CSIP-AUS[89], the Distributed Energy Integration Program Interoperability Steering Committee leading establishment of a nationally consistent testing and certification service, intended to come later in 2025 in support of the New South Wales and Australian Capital Territory rollouts[90], SmartConnect, and the DER API Technical Working Group,
- ongoing harmonisation efforts on EBM implementation in New South Wales and the proposed emergency backstop mechanism in the Australian Capital Territory, also intended to support and enable consistency across other CSIP-AUS implementations: including with the ENA, New South Wales DCCEEW and the Australian Capital Territory Government, to use consistent commissioning and onboarding[91] – the ENA has engaged a consultant to work with DNSPs on harmonisation efforts,
- a collaborative forum established by AEMO with NEM DNSPs on functional requirements for operating a high CER power system, including requirements for effective emergency backstop and learnings across implementations, and
- ongoing work to develop a National Energy Public Key Infrastructure (NEPKI) company, out of the National CER Roadmap actions[92].

---

[88] Commonwealth DCCEEW, National CER Roadmap – Redefine roles for market and power system operations – M3/P5, https://consult.dcceew.gov.au/national-cer-roadmap-redefine-roles-m3-p5.

[89] Version 1.2, with test procedures for DER clients and devices. For more information refer to Standards Australia (June 2025) Technical Specification SA TS 5573:2025 Common Smart Inverter Profile - Australia with Test Procedures, https://store.standards.org.au/product/sa-ts-5573-2025.

[90] The Committee is leading establishment of a nationally consistent testing and certification service. For more information see https://www.csipaus.org/certification.

[91] New South Wales DCCEEW 2025, NSW Emergency Backstop Mechanism and CER Installer Portal Consultation Summary, Section 2.1, https://www.energy.nsw.gov.au/sites/default/files/2025-05/NSW-Emergency-Backstop-Mechanism-and-CER-Installer-Portal-Consultation-Report.pdf.

[92] Authorisation to form NEPKI with conditions was granted by the Australian Competition and Consumer Commission on 11 July 2025: https://www.accc.gov.au/public-registers/authorisations-and-notifications-registers/authorisations-register/energy-networks-association-limited-and-ors.

AEMO will continue to provide advice to these workstreams, and advocate for national consistency in emergency backstop mechanism performance. Some DNSPs have noted that opportunities to improve national consistency in implementation may need to be considered in the context of the costs and time to achieve that consistency.

Table 9 Potential governance gaps identified

Potential gap	Details
Performance specifications	AEMO identified a gap around the definition of performance parameters for emergency backstop delivery, and pathways for assessment and rectification if these specifications are not met. For example, this likely includes the delivery specifications summarised in Section 2.8: • Sufficient amount of emergency backstop mechanism response (available and delivered). • Speed of response delivery. • Accurate forecasts of available response in real time.
Amount of emergency backstop required	Some DNSPs have raised that existing regulatory mechanisms require amendment to provide certainty for investment purposes. DNSPs support regulatory amendments which provide clarity regarding the amount of operational capacity required to mitigate against the risks of MSL events efficiently, based on minimising customer impacts and providing customer benefits[A].
Emergency backstop installation compliance	Multiple DNSPs and OEMs have articulated challenges with a lack of formally assigned roles and processes for emergency backstop installation compliance monitoring, assessment and enforcement. The SEC also expressed concerns that roles and responsibilities are unclear and can be particularly problematic for installers in cases where a return to site is required. The cost and administrative burdens to installers can be substantial. Addressing these gaps would provide clear 'levers' to support high installation compliance and address non-compliance (e.g. through rectification of installations which do not meet emergency backstop requirements)[A]. As noted above, there are ongoing workstreams to address this, to which AEMO will continue to provide advice.
Due diligence assessment of emergency backstop capability	Given the high importance of emergency backstop mechanisms for managing system security, and the high level of complexity of these mechanisms, there is a role in due diligence confirmation of information provided by DNSPs around the amount of emergency backstop response that will be delivered when required for system security. AEMO has found significant value in co-assessment of performance outcomes of emergency backstop with DNSPs as part of AEMO's functions around assessment of and reporting on power system incidents. Performing due diligence assessments requires various detailed datasets, and the provision of these may lack clarity under present governance arrangements[A,B].
At-scale testing	At-scale testing (discussed further in Section 2.5) will require significant efforts and resourcing across AEMO, TNSPs, DNSPs, OEMs and other technology providers of active DER management. Regulatory frameworks to allow and incorporate formal requirements for at-scale testing do not exist at the moment.
Return to service	OEMs, DNSPs and the SEC representing installers have raised concerns about lack of clarity around responsibilities for ensuring DER systems successfully return to service (and are promptly rectified if necessary) following testing or use of emergency backstop mechanisms to manage system security. This can be particularly unclear and challenging for sites where there are complex pre-existing issues at the site, which become more apparent following an at-scale test. See Section 2.6 for further details.
Continuity of service delivery	Roles and responsibilities for ongoing maintenance of DER site connectivity and continued delivery of emergency backstop capabilities over time should be clarified. Troubleshooting can be complex and resource intensive, and may require visits to sites with complex pre-existing issues. The SEC expressed concerns about installers inability to manage the cost and administrative burden of repeated returns to site[C].
Unregistered sites	Another type of pre-existing issue is in sites which do not register with the DNSP to connect, but connect to the distribution network regardless. DNSPs noted that this issue pre-dates emergency backstop, and are seeking data-sharing alongside appropriate frameworks to identify and rectify these sites[C].
Server testing and certification	For internet-based mechanisms using national standards (such as CSIP-AUS), DNSPs, OEMs and Synergy have noted a need for national consistency around testing, certificate management, and certification pathways for OEMs, technology providers, external vendors and utility servers to streamline integration and ensure interoperability. As noted above, there are ongoing workstreams to address this, including with New South Wales and Australian Capital Territory DNSPs and governments to operate CSIP-AUS using consistent testing and compliance protocols. AEMO will continue to provide advice to ongoing governance workstreams in this area.

Potential gap	Details
Broader regulatory context	Some stakeholders raised concerns that new arrangements for emergency backstop mechanisms were not well supported by a consumer rights policy framework, and that this needs to be considered in the context of current consumer law. International trade law may also need to be considered [C].
Industry engagement	The SEC raised concerns on a lack of clarity around roles and responsibilities for industry engagement about introduction of new arrangements such as emergency backstop mechanisms. Appropriate and accessible engagement with OEMs, solar installers and solar retailers requires significant resourcing, to ensure these highly affected groups are empowered and can appropriately influence these processes.

A. This could potentially be addressed through the National CER Roadmap – Redefining Roles for Market and Power System Operations workstream.
B. This could potentially be addressed through the National CER Roadmap – National Technical Regulatory Framework workstream.
C. This could potentially be addressed through the National CER Roadmap – Consumer protections workstream.

2.8 Emergency backstop mechanism design specifications for management of Minimum System Load conditions

Based on AEMO's experiences integrating emergency backstop mechanisms into MSL operational processes, they should be designed to deliver the following specifications:

- **Rapid response** – there are significant benefits to rapid delivery of emergency backstop mechanisms, ideally targeting significant at-scale response achievable within ~15 minutes, with a response time of 60 minutes as a practical initial target.
- **Certainty of emergency backstop response** – where possible, emergency backstop mechanisms should be designed with systems that facilitate accurate estimation in DNSP control rooms of the amount (MW) of response available as close to real time as feasible.

Additional recommended design specifications include:

- **Include the capability to reduce DER generation from zero export to zero generation** in extreme situations. If reducing generation to zero export remains insufficient to maintain system security, capabilities to reduce to zero generation avoid the need to undertake actions with higher customer impact, such as EVM or shedding of entire feeders in reverse flow. Exceptions may apply to complex sites.
- **Confirmation of return to service** – visibility and monitoring of the return to service status of customer DER sites, linked to failsafes and consumer protections.
- **Expected behaviours in event of lost comms ('fallback')** – pre-programmed behaviours at the DER site so that unexpected interruptions (such as loss of internet or AFLC signals) results in expected behaviours at the site that support power system security.
- **Consider broad need for emergency backstop capability** – emergency backstop capabilities are intended to allow AEMO to manage power system security in a wide range of extreme circumstances. The power system security issues highlighted in this report represent only those issues that are known at this time, but many other potential system security issues could arise and require backstop capabilities, such as:
  - management of cybersecurity threats,
  - CER control system interactions (which could occur even if systems are curtailed to 0 MW but remain connected to the system), and
  - possible use to facilitate a system restart process.

- **Robustness under extreme conditions** – consider the robustness of the technical approach applied, especially under conditions where communications networks may be compromised and there may be widespread power outages (due to flooding, bushfires, storm damage, or other reasons). These types of conditions may coincide with challenging grid conditions where emergency backstop capabilities are more likely to be required.

Rapid response

There are significant benefits to rapid delivery of emergency backstop mechanisms, ideally targeting significant at-scale response achievable within ~15 minutes.

For example, emergency backstop mechanism use may be required to resecure the power system following a contingency event. When the power system falls to MSL2 thresholds (one credible load contingency away from MSL3, which is when forecast demand is insufficient to maintain a secure operating state[93]), AEMO will take actions required to land in a satisfactory state and be able to return to and remain secure within 30 minutes[94] following a credible load contingency[95]. If emergency backstop mechanisms cannot be reliably delivered at scale within ~15 minutes (allowing for control room information collection and decision-making processes within the total 30-minute window), this may require that pre-contingency actions are taken, such as preparing BESS to act as a fast-acting reserve that can return the system to secure as a stop-gap measure until emergency backstop mechanisms can be activated[96]. These actions have impacts on market participants, and may lead to increased costs for consumers. The capability for rapid emergency backstop mechanism activation can therefore minimise the amount and incidence of DER curtailment required, minimise impacts on market participants, and minimise costs for consumers.

AEMO is collaborating with TNSPs and DNSPs to improve operational systems, tools and processes to streamline control room processes, and also recommends design of emergency backstop mechanism delivery methods to minimise delays in the actual curtailment response.

As a practical initial target, AEMO suggests a design criteria that targets an operationally effective emergency backstop mechanism response within 60 minutes of DNSP activation of the mechanism, with an aim to reduce this delay as much as possible in the longer term and ultimately align with the speed of response available via load shedding mechanisms (for example, targeting full emergency backstop mechanism response within ~15 minutes from DNSP signal to confirmation of curtailment).

Certainty of emergency backstop mechanism response

Where possible, emergency backstop mechanisms should be designed with systems that facilitate accurate estimation in DNSP control rooms of the amount (MW) of response available as close to real time as feasible, accounting for factors that may limit response capability (for example, communications challenges that are likely to

[93] AEMO (November 2024) *Victorian Minimum System Load Procedure Overview*, https://aemo.com.au/-/media/files/electricity/nem/security_and_reliability/power_system_ops/2024-11-01-vic-msl-procedure-factsheet_final.pdf?la=en.

[94] Under NER 4.2.6.

[95] Any incident where the power system is not in a secure operating state for more than 30 minutes is considered a reviewable operating incident (NER 4.8.15(a)(1)(iv)).

[96] AEMO, *Victorian Minimum System Load (MSL): Role of BESS*, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/vic-msl-directions-process.pdf?la=en.

impact emergency backstop mechanism response or low levels of generation from PVNSG due to price-responsive self-curtailment). DNSPs should aim to make it possible to relay this information to AEMO's control room as accurately as possible, so it can inform control room decision-making.

Additional design specifications

Additional recommended design specifications include the following:

- If the emergency backstop mechanism is typically set up for curtailment to zero export, **include capability to reduce DER generation from zero export to zero generation** in extreme conditions. If reducing generation to zero export remains insufficient to maintain system security, capabilities to reduce to zero generation avoid the need to undertake actions with higher customer impact, such as EVM or shedding of entire feeders in reverse flow. Special consideration is required for hybrid sites that include storage or controlled loads, which may need more complex arrangements to support optimal behaviour.
- **Visibility of return to service** – systems with visibility and monitoring of the return to service status of customer DER, to enable identification of sites experiencing return to service challenges, discussed further in section 2.6. OEMs and DNSPs have raised concerns that roles and responsibilities around ensuring return to service need to be more clearly defined and developed, with appropriate mechanisms to protect consumer interests.
- **Fallback behaviours** – communications interruptions should be anticipated and planned for, and may be more prevalent under extreme conditions when use of emergency backstop mechanisms is required. Emergency backstop mechanisms should include pre-programmed behaviours at the DER site so that unexpected interruptions (such as loss of internet for internet-based mechanisms) result in expected behaviours at the site that support system security. For example, upon loss of communications or signals for a period of time, the DER system might gradually ramp down over 30-60 minutes to a fallback limit, minimising potentially problematic export levels during extreme conditions. High transparency is needed to mitigate potential reliability impacts if loss of communication were to occur in high demand conditions.

2.9 Consider and design for scalability

Many emergency backstop mechanisms use complex architecture. It is important that scalability is considered, projecting forward to scenarios where these mechanisms may be utilised simultaneously across the NEM to manage power system security in multi-region MSL conditions.

For all emergency backstop mechanisms, pathways need to be designed and resourced to provide high visibility to identify and resolve performance issues that may be encountered for at-scale activations of the emergency backstop mechanism.

For internet-based emergency backstop mechanisms, server scalability challenges have been observed in some form by all organisations implementing emergency backstop mechanisms via this pathway in Australia (SAPN, Victorian DNSPs and Synergy). These organisations have noted scalability challenges may arise in the utility server and/or OEM technology infrastructure, and can have a wide range of impacts. For example, in some cases a small portion of devices for a particular OEM were impacted, while other cases involved large-scale utility server outages, sometimes due to challenges in external vendor utility server infrastructure. DNSPs noted that the VBM is the first time external vendors of utility servers have used these types of systems for this purpose at scale internationally, and they expect increased maturity, scalability and reliability over time.

OEMs and DNSPs noted the importance of consistent application of national standards such as CSIP-AUS, with pathways to support consistent implementation and interpretation, and that this may require longer lead times to align pathways for certification and approval of devices across organisations. New South Wales and Australian Capital Territory DNSPs have also noted the work they are undertaking in coordination with New South Wales DCCEEW, the Australian Capital Territory Government and the ENA, to operate CSIP-AUS using consistent testing and compliance protocols.

Scalability challenges may mean risks of hours-long delays in at-scale emergency backstop mechanism response when required during extreme conditions, or that installers cannot connect new systems to the network due to delays in completing capability testing, which may reduce installation compliance. The following factors appear to be helpful in diagnosing and addressing scalability challenges:

- **Design digital architecture which can handle considerable data flows** from hundreds of thousands of DER devices, and growing in number in the coming years to tens of millions in some networks (for example, during at-scale activation under low demand conditions to manage system security), or handling large quantities of timeseries data when checking for correct setup (for example in capability tests).
- **Ensure high visibility** of server operation challenges to rapidly diagnose challenge areas.
- **Rigorous server load testing prior to large-scale rollout** using tools proven to deliver accurate results. For example, SAPN undertook a resource-intensive testing process prior to FELs rollout, which included end-to-end load testing of communications systems.
- **In-house expertise** – consider the need for development of in-house expertise to support key elements of server performance where feasible.
- **Consistent application of standards** – where national standards such as CSIP-AUS are used, consider pathways to support implementation and interpretation consistent with other regions in Australia (discussed further in sections 2.7 and 3.3). This may require longer lead times to align pathways for certification and approval of devices across organisations.

For non-internet-based mechanisms such as GSDs, scalability needs to be considered in the **design of testing and auditing processes**, ensuring they can be practically scaled up as required. This may involve regular at-scale testing, regular systematic audits (possibly requiring site visits), and significant engagement with installers.

3 Internet-based active DER management

This section discusses insights that are specific to the range of methods for active DER management using the internet. These internet-based methods typically rely on computer servers to communicate curtailment signals in at least one step in its process. In Australia, internet-based methods have been implemented in South Australia, the SWIS in Western Australia, and Victoria, and are planned to be implemented in New South Wales and the Australian Capital Territory (details in Table 3).

In most of these methods, if emergency backstop is required for system security:

1. AEMO instructs the TNSP to maintain demand above a secure threshold.
2. TNSPs then contact DNSPs (or Synergy).
3. DNSPs (or Synergy) then contact OEMs or other technology providers of active DER management to curtail their respective fleets. In pathways using CSIP-AUS, this communication is conducted via a utility server, which in some implementations is provided by an external vendor.
4. Once contacted, OEMs/technology providers send DER devices a curtailment signal.

Some communications pathways also include direct to device controls (utility-to-DER), where DER devices are directly connected to DNSP systems. At present, uptake of these pathways appears to be much lower.

3.1 National harmonisation

Both OEMs and Victorian DNSPs have noted a need for streamlined and nationally consistent onboarding, certification and compliance pathways, particularly for OEMs onboarding onto CSIP-AUS utility servers, potentially through SmartConnect. OEMs have observed the following:

- Present utility-to-OEM integrations, testing and onboarding requirements are different across DNSPs (even with CSIP-AUS, due to different interpretations of the national standard), and building multiple pathways to address each different implementation is resource-intensive.
- It is challenging to make the case for improved resourcing to overseas decision-makers when there are multiple different requirements within Australia. Many OEMs with major market share are headquartered overseas and may not have authority to approve the scope of resourcing within Australia. For example, different CSIP-AUS interpretations and implementations can lead to negative perceptions of the Australian market maturity, and undermine enthusiasm for investment.

In the New South Wales EBM and the proposed Australian Capital Territory emergency backstop mechanism, work is underway with New South Wales DCCEEW, the Australian Capital Territory Government and New South Wales/Australian Capital Territory DNSPs to operate CSIP-AUS using consistent testing and compliance protocols across DNSPs[97]. New South Wales/Australian Capital Territory DNSPs noted they are streamlining integration requirements for utility servers, and aligning with each other on common testing pathways with OEMs.

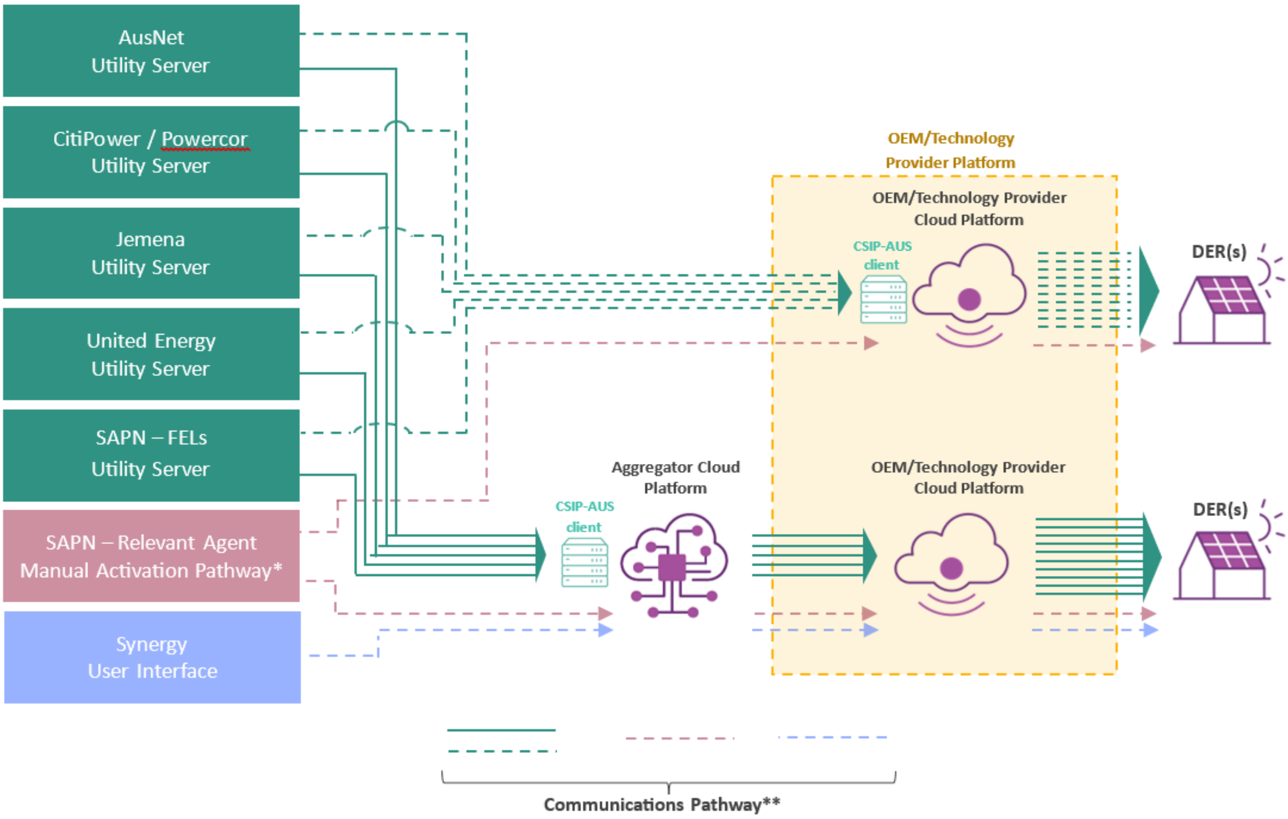
[97] New South Wales DCCEEW 2025, New South Wales Emergency Backstop Mechanism and CER Installer Portal Consultation Summary, Section 2.1, https://www.energy.nsw.gov.au/sites/default/files/2025-05/NSW-Emergency-Backstop-Mechanism-and-CER-Installer-Portal-Consultation-Report.pdf.

3.2 "Bottleneck" issues

In the most common form of delivery of internet-based emergency backstop mechanisms, OEMs and other technology providers of active DER management act as a 'middleman' relaying curtailment signals from the DNSP (or Synergy) to individual DER inverters. The servers and platforms used by OEMs and technology providers therefore impact emergency backstop performance, regardless of the type of technology employed by the DNSP (whether a CSIP-AUS central utility server, proprietary API platforms, or manual activation pathways).

An OEM/technology provider platform will interact with multiple central utility servers, and DNSP visibility of the OEM/technology provider internal digital infrastructure is typically limited. Figure 4 illustrates the typical communications pathways used in the delivery of emergency backstop mechanisms. For example, if the mechanism is activated in Victoria, an OEM platform receives signals from utility servers from each Victorian DNSP. This OEM then has to relay curtailment signals to tens of thousands of connected sites. As more DER sites are added, OEM/technology provider platforms and technology infrastructure may encounter scalability challenges and become a "bottleneck" to emergency backstop performance.

Figure 4 Communications pathways between utility and OEM platforms



* SAPN's RA mechanism is currently activated via phone call from the DNSP to the RA (typically an OEM or aggregator). OEMs then use their platforms to curtail the connected DER devices.
** Some communications pathways also include direct to device controls (utility-to-DER), where the DER devices are directly connected to DNSP systems. As uptake of these pathways appears to be low, direct-to-device pathways have been left off the diagram in the interest of clarity.
Note: Alongside emergency backstop, virtual power plant (VPP) and voluntary scheduled resource (VSR) providers also interact with DER devices.

For example, AEMO analysis of RA data observed that four OEMs appear to exhibit long time delays in responding to a curtailment signal, with 40-55% of their fleet observed to take between 1-3 hours to respond, and a further 10-15% potentially taking more than six hours to respond. AEMO and DNSPs are working with OEMs to better understand factors causing these delays. OEMs noted a lack of clarity in the NEM on which party should bear the costs of addressing these delays, and some OEMs noted that inconsistent integration with DNSPs is a contributing factor to long response times.

While there are methods to reduce server load and increase server scalability performance, OEMs have highlighted that these are resource-intensive and costly to implement, and under present governance frameworks in the NEM there are no clear incentives or support for OEMs to improve performance of their platforms[98]. OEMs have observed that improving platform performance (for example, by including resilience, redundancy requirements and load testing) is high cost and requires specialised resources and expertise.

Some OEMs have elected to adopt communications pathways that utilise direct to device controls by incorporating active DER management in the firmware of the device. In these utility-to-DER pathways, DER devices are directly connected to DNSP systems and the OEM's role is in the design of firmware which implements active DER management. These OEMs noted that while this type of pathway may reduce risks of scalability "bottleneck" challenges during at-scale activation of emergency backstop, and may lower costs of ongoing platform/server maintenance, it has particularly high up-front costs and effort. They echoed sentiments around resourcing challenges in this approach, which have been significantly exacerbated by differences between DNSPs. Designing firmware for scalability, and managing firmware updates, are also important considerations in this pathway (for example, ensuring that firmware updates do not result in unexpected changes DER device behaviour).

Reliable and robust platforms for OEMs (and other technology providers of active DER management) are a crucial step in the function of internet-based emergency backstop, and strong incentives for them to maintain ongoing operational performance of their servers during extreme conditions should be explored.

3.3 Governance gaps

In these types of internet-based emergency backstop mechanisms, OEMs and other technology providers of active DER management are playing a central role in delivery of a function that is essential for power system security. This leads to a number of flow-on risks that need to be carefully managed.

Clear performance expectations – potentially through minimum technical requirements and compliance arrangements, in the context of a broader governance framework which considers cybersecurity, sovereign and operational continuity risks – could support more consistent outcomes and encourage proactive investment by OEMs.

The specific governance gaps identified by stakeholders related to internet-based mechanisms are summarised in Table 10. These are in addition to the more general governance gaps (applying to all types of emergency backstop mechanisms) summarised above in Table 9.

[98] In the SWIS, Synergy noted that it has contract arrangements and service level agreements (SLAs) in place with some OEMs and technology providers, as part of its website listing process.

Table 10 Governance gaps identified for internet-based mechanisms

Governance gap	Details
National harmonisation	OEMs consistently emphasised the high degree of cost and effort involved in managing different requirements in different jurisdictions (including varying implementations of CSIP-AUS), and expressed a strong desire for national harmonisation.
Performance requirements or guidelines	In the NEM, there is no formal process for defining or managing delivery of emergency backstop capabilities, or resourcing to deliver these capabilities, from OEMs and other technology providers of active DER management.
Cybersecurity oversight	There is no established framework to ensure or monitor compliance of OEM and technology provider systems to appropriate cyber security standards (such as the *Cyber Security Act*[A]). Additional requirements may be needed for devices with potential impact on power system operations, particularly as the generation capacity under control increases. This may include consideration of certificate management, password protection, and system resilience.
Sovereign risk	No specific and formal assessment process around foreign owned and operated OEM devices leading to unidentified/unmanaged risks.
Operational continuity	OEMs' business models are primarily based on generating revenue through the sale of devices rather than the continued operation and maintenance of these platforms. The industry faces the potential for significant disruption if: • an OEM or technology provider exits the market or ceases operations, • an OEM or technology provider discontinues support for its platform, or • critical system elements (such as certificates, credentials) are lost or corrupted due to poor maintenance. Continuity requirements may also mean a need for processes to manage updates or changes to firmware, software and/or utility servers, to ensure emergency backstop capability is maintained across the range of technologies used by OEMs, technology providers and external vendors.

A. More information on this Act can be found on this Australian Government Department of Home Affairs webpage, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act.

The ongoing workstream to establish a national CER Technical Regulatory Framework, led by the Commonwealth DCCEEW and including industry workshops, is intended to provide a pathway to implementing frameworks to address some of these issues. This workstream and other ongoing work to address governance gaps are discussed further in section 2.7.

The governance gaps outlined in Table 10 present a high risk to successful emergency backstop mechanism delivery, and need to be urgently addressed.

4 Generation Signalling Devices

A GSD[99] is a device connected at the customer's site that enables the inverter to receive a signal to activate a standardised demand response mode which disconnects the DER inverter.

4.1.1 Case study: GSD implementation in Queensland

From 6 February 2023, all new and some replacement inverter energy systems (including DER inverters) with aggregate capacity ≥10 kVA in the Energex and Ergon Energy Networks were required to be installed with a GSD[100]. The GSD is remotely activated by high-frequency coded signals sent from Energex and Ergon Energy Networks' existing powerline signalling system, known as audio frequency load control (AFLC). When activated, the GSD prevents generation, self-consumption or export for the duration of the curtailment period.

AFLC has been demonstrated to be a robust and reliable physical communications mechanism that has demonstrated capability, and can deliver curtailment to devices under conditions with limited communication network availability[101]. Site audits by Energex and Ergon Energy Networks indicate that:

- 65-75% of new installations ≥10 kVA have a GSD installed, and
- of those with a GSD installed, ~26% are functioning as required to deliver emergency backstop capabilities:
  - for sites <30 kVA – 12% first time installation compliance – audited sites found to be non-compliant were rectified, and compliance subsequently increased to 59%, and
  - for sites ≥30 kVA – assumed 60% compliance rate, likely to be a conservative estimate as there are more stringent requirements on ≥30 kVA sites.

Energex and Ergon Energy Networks have taken steps to increase installation compliance, including:

- an uplift in audits of new installations ≥10 kVA from 2% of sites prior to September 2024 to >5% of sites, with approximately 10% of new sites audited as at Q1 2025,
- tightening guidelines around which sites should be audited, alongside audit tools and data analysis to target audits and inspections on areas or installers identified to have low compliance, and work with installers on education and rectification, and
- investigating causes of non-compliance, which find two types of causes – GSDs not being installed at all or incorrectly installed, and incorrect inverter configuration.

---

[99] The GSD is a type of Demand Response Enabling Device (DRED) conforming the AS4755.1, which has a specified DRED port that connects to inverters compliant to AS4777.2.

[100] The requirements for emergency backstop mechanism are referenced in Energex and Ergon Energy Network standards STNW 1170, 1174, 3510 and 3511 and the Queensland electricity connection manual, which can be found on the Queensland Government website, https://www.energyandclimate.qld.gov.au/about/initiatives/emergency-backstop-mechanism#:~:text=The%20emergency%20backstop%20mechanism%20will%20apply%20only%20to%20new%20and,residential%20and%20commercial%2Findustrial%20customers. More information on which inverter connections must install a GSD device can also be found at https://www.ergon.com.au/network/our-services/connections/residential-and-commercial-connections/solar-connections-and-other-technologies/emergency-backstop-mechanism and https://www.energex.com.au/our-services/connections/residential-and-commercial-connections/solar-connections-and-other-technologies/emergency-backstop-mechanism.

[101] AFLC have been used for more than 70 years to enable load control tariffs.

Energex and Ergon Energy Networks observe that following installer engagement and rectification efforts, improvement is beginning to be observed in audits.

4.1.2 GSD approaches

The use of GSDs to deliver emergency backstop capability has the following benefits:

- Robust and reliable physical communications mechanism with demonstrated capability.
- Fewer parties involved in emergency backstop activation in real time (compared to internet-based mechanisms, where multiple parties have to respond for an operationally effective emergency backstop).
- Unlikely to demonstrate scalability issues.
- Likely able to achieve rapid response in a power system event.
- Cybersecure.

This approach has the following limitations:

- Significant installation compliance challenges need to be addressed. Installers are able to test correct GSD setup at the site, but awareness of this test is low. Energex and Ergon Energy Networks has sought to increase awareness by:
  - developing a new installation and compliance document,
  - auditors sharing information about the correct setup verification test during site inspections, and
  - collaborating with training and accreditation bodies, including a training board developed by the GSD manufacturer.
- At present, verifying and ensuring correct GSD setup requires an in-person site audit, or simultaneous activation of all systems associated with a substation. Auditing a large number of sites can be prohibitively expensive, and might only be practical for a subset of sites (<10%).

5 Smart meters

The ability for smart meters to manage DER has been raised as an additional possibility to deliver active DER management while delivering other capabilities including monitoring. Smart meters have been included in their own category as they sit separately in the regulatory framework and have existing infrastructure and NER obligations related to retail market operation and energy settlement. Smart meters are capable of multiple types of communications pathways, including internet-based approaches and AFLC[102].

5.1.1 Case study: Availability of gross DER data from smart meters in South Australia following the implementation of Smarter Homes

The South Australian Government's Smarter Homes regulations, introduced from 28 September 2020[103], included new requirements for wiring arrangements for smart meters. This was intended to allow for several functionalities, including the capability to separately measure and control distributed PV[104]. It was enabled via the *Technical Regulator Guideline Smart Meter Minimum Technical Standard and Associated Deemed to Comply Wiring Arrangements*[105] ('the Guideline'[106]), which contained a set of 19 Deemed to Comply Wiring Arrangements (DCWA) for smart meters. The Guideline was updated on 27 August 2021 to have four default DCWA, to help streamline compliance[107].

Smart meters have been used by some RA who were Metering Coordinators (MCs) on a limited basis, a capability which forms an additional control functionality beyond what is specified in the Guideline[108]. However, analysis of smart meter data in South Australia provides insights on the potential capability that might be available via the Guideline.

Analysis was undertaken on smart meter data obtained from Meter Data Providers (MDPs) to identify if gross distributed PV measurements were available[109]. Data from three MDPs was analysed across two separate dates. Findings include the following:

- 11-18% of analysed sites appear to have gross distributed PV generation data, separate from load and other measurements on the site.
- 60-73% of sites appear to only have net data. Separate distributed PV data is not available at these sites.

[102] At present, smart meters use meshed networks (within Victoria) or 4G (outside Victoria) to provide meter data for settlement to AEMO.

[103] As per clause 55G of the Government Gazette published 24 September 2020, https://governmentgazette.sa.gov.au/2020/September/2020_076.pdf.

[104] As stated in Section 5 of the Guideline, https://www.energymining.sa.gov.au/__data/assets/pdf_file/0005/671972/Technical-Regulator-Guideline-Smart-Meter-Minimum-Technical-Standard.pdf.

[105] Latest version, Government of South Australia 2020 (June 2022 update), https://www.energymining.sa.gov.au/__data/assets/pdf_file/0005/671972/Technical-Regulator-Guideline-Smart-Meter-Minimum-Technical-Standard.pdf.

[106] The roles and responsibilities of Metering Coordinators, Metering Providers and Electrical Contractors is to ensure compliance with this guideline, so owners or operators of electrical installations comply with the *Electricity (General) Regulations 2012*. At time of writing, the current version these regulations is 14.3.2024, at https://www.legislation.sa.gov.au/__legislation/lz/c/r/electricity%20(general)%20regulations%202012/current/2012.199.auth.pdf.

[107] Other DCWA are not precluded, but must be coordinated between the electrical contractor and metering provider.

[108] The RA regulations were also introduced within the Smarter Homes regulations, under separate clauses (55B to 55D) in the Government Gazette, https://governmentgazette.sa.gov.au/2020/September/2020_076.pdf.

[109] AEMO does not have data on which DCWA has been applied to a particular meter.

- The remainder of sites appear to be exempt from separate control and metering of distributed PV, such as existing sites with single element meters installed prior to the Smarter Home requirements, multiple-phase sites, sites with insufficient space on an existing group meter panel, sites where the solar inverter was connected to a distribution board (such as strata title sites), and sites where the inverter(s) rated current exceeded the auxiliary/second metering element current rating[110], alongside other exemptions[111].

These findings did not vary significantly by MDP. The proportion of smart meters with capability to control distributed PV under the Guideline is likely similar to the proportion with capability to measure distributed PV (<20%)[112].

This suggests that if it were pursued to enable emergency backstop capability via smart meters in South Australia under the Guideline, less than 20% of the systems installed since these arrangements were put in place would be likely to respond successfully.

Discussions with the South Australian Government and MDPs indicate that the low proportion of sites with separate distributed PV data available is potentially attributable to legacy sites, other exemptions, installer confusion around the DCWA requirements, and lack of compliance incentives for correct installation.

The focus on compliance in South Australia has been on the critical task of improving compliance in the implementation of FELs to support emergency backstop capabilities. Future focus on metering guidelines compliance could similarly yield improvements.

5.1.2 Case study: Relevant Agent technology providers using smart meter capabilities

Several non-CSIP RA technology providers in South Australia opted to use smart meter options (DCWA 7 in the Guideline[113]). AEMO analysis of power system incidents found several technology providers using smart meter options achieved high response rates[114]. This provides an example where smart meters have been shown to be capable of successfully delivering emergency backstop responses.

---

[110] Standardised requirements for minimum current rating of auxiliary/second metering elements, as well as the inclusion of auxiliary contacts, were not specified in AEMO advice at time of development of the Guideline.

[111] Exemptions are outlined in Section 6 of the Guideline, https://www.energymining.sa.gov.au/__data/assets/pdf_file/0005/671972/Technical-Regulator-Guideline-Smart-Meter-Minimum-Technical-Standard.pdf.

[112] While all DCWA with separate distributed PV measurements were also capable of separately controlling distributed PV, two arrangements (DCWA 7 and 11) were capable of separately controlling distributed PV without separately measuring PV. However, these two arrangements are unlikely to apply to most sites, as they were intended to be applied under specific conditions. DCWA 7 was permissible for sites where either 1) the solar inverter was connected to the distribution board, or 2) the Metering Provider was the RA. It is not known how many sites analysed have inverters connected to the distribution board, but sites analysed do not meet condition 2) as they are Flexible Exports sites with SAPN as the RA. DCWA 11 was permissible for sites with BESS. Further detail on DCWA 7 and 11 is in Section 7.1.7 and 7.2.4 of the Guideline.

[113] DCWA 7 was permissible for sites where the Metering Provider was the Relevant Agent. Further detail on DCWA 7 is in Section 7.1.7 of the Guideline.

[114] AEMO (May 2023) *Trip of South East – Tailem Bend 275kV lines on 12 November 2022*, Section 4.2.2: Smarter Homes Regulations, Figure 26: Response rates for different relevant agents, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en&hash=A89F330CF6C979E52EF15EB86E5CF058.

5.1.3 Smart meter-based approaches

Smart metering systems have the potential to support monitoring of DER, with secure communication of emergency backstop signals and a potentially lower risk of scalability issues. However, this approach is not without limitations and risks.

Due to the diversity of metering configurations and compatibility with distributed PV and BESS electrical installations, installation compliance is complex, and it is challenging to ensure that sites respond as expected to emergency backstop signals. Achieving this confirmation may be challenging in practice given existing smart meter infrastructure, the existing NEM metering regulatory framework, which has the primary objective of supporting accurate customer billing and energy market settlement[115], as well as physical site limitations (for example, two element meters on sites with multiple devices such as controlled loads or batteries, current ratings on auxiliary/second metering element terminals which are less than the inverter capacity).

Changes to these requirements should be approached with care, as introducing technical obligations outside the harmonised NEM metrology framework may risk impairing the operation of core settlement functions and constrain the broader development of the metering framework and the NEM retail market which it serves.

The forthcoming Flexible Trading Arrangements (FTA) rule change[116] will introduce the option for consumers to voluntarily activate Secondary Settlement Points (SSPs) for residential solar and other CER. If voluntary uptake becomes material, or if systems are commonly installed in an "SSP-ready" configuration, this could support capability for the separate measurement and management of DER.

5.1.4 Learnings

Smart metering systems may offer an alternative pathway for delivering emergency backstop functionality whilst delivering other capabilities including monitoring. However, they face the same installation compliance challenges identified for all emergency backstop mechanisms (see Section 2.3), and a compliance focus could deliver a similar uplift in outcomes. Verification of correct installation setup remains essential.

AEMO encourages the inclusion of all technical requirements for smart meters within the NER metering framework. Embedding these requirements in the NER, via Australian Energy Market Commission (AEMC) processes and in consultation with stakeholders and interested parties, leverages the framework's established compliance and enforcement mechanisms, which support effective implementation. This approach also maintains the integrity of the metering framework's primary retail market and settlement purposes and ensures alignment with the NEM governance and change management processes on an ongoing basis.

At the time of their establishment, the South Australian Government's arrangements required urgent implementation within a timeframe that could not reasonably be accommodated through the standard NER change processes.

[115] This framework operates under a single, transparent, and enforceable set of requirements harmonised across NEM jurisdictions. It includes access and assurance mechanisms within a compliance structure. These technical requirements are established under the NER and relevant AEMO procedures.

[116] The AEMC consultation on FTA is at https://www.aemc.gov.au/rule-changes/unlocking-CER-benefits-through-flexible-trading.

6 SCADA control

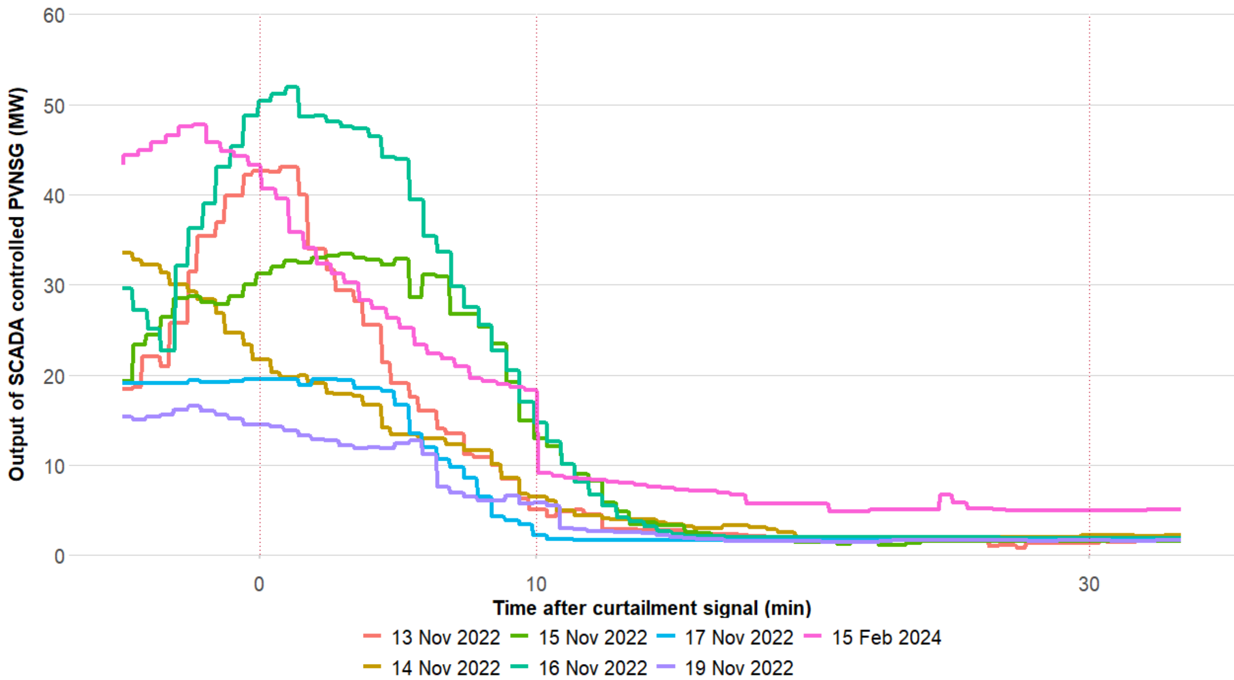
SCADA control uses DNSP SCADA systems to send a curtailment signal to PV systems. This is generally only applied to larger DER systems, since costs are prohibitive for smaller customer sites.

SCADA can provide close to real-time confirmation of curtailment response, with updates every few seconds. This improved visibility has many other benefits for network management and system security. Uplift may be required in DNSP systems to develop dashboards for control room visibility and ability to manage rapid simultaneous curtailment in an event across many different systems.

6.1.1 Case study: Curtailment delivered by South Australian sites on SCADA control

PV curtailment has been delivered in South Australia via SCADA control in seven historical system security events from November 2022 to February 2024. Figure 5 shows the response during these historical events, with each line representing total generation from all SCADA-controllable sites on the day.

Figure 5 Historical response profiles from all SCADA controllable sites in South Australia



Note: Data is from aggregated data on total generation from all SCADA-controllable sites in SAPN's network, sent to AEMO via ElectraNet.

The historical responses show SCADA control provides fast response with high performance, curtailing generation by more than 89% of pre-curtailment levels, with generation curtailing by ~71% within 10 minutes of the curtailment signal[117].

Curtailment capability from this method may be limited during emergency low demand conditions as larger PV sites have been observed to exhibit price-responsive behaviour, and wholesale prices are often low during MSL

[117] Full response is observed within 24 minutes (18 minutes on average), with average ramp rates of ~1.7 MW/min.

conditions in the NEM[118]. Of the >150 MW of installed capacity[119] in the South Australian SCADA-controlled fleet, Figure 5 shows ~50 MW or less has been generating during historical extreme conditions. This appears to be due to self-curtailment in response to low prices[120]. Further observations on this behaviour can be found in Appendix A1.1.

[118] The SWIS has a different market mechanism, and embedded generators in the SWIS do not appear to self-curtail during low demand periods.

[119] Installed capacity of SCADA-controllable sites in South Australia was approximately 150MW in November 2022, and approximately 185 MW in February 2024.

[120] In the 30 minute interval before the commencement of curtailment during each historical event, prices were typically below -$24/MWh, with the average being approximately -$45/MWh.

7 Further mechanisms to ensure system security

If sufficient emergency backstop capability is not available, the only mechanism remaining to increase operational demand to the levels required to maintain system security are measures with higher customer impact, discussed further in this section.

7.1 Emergency Voltage Management (EVM) for emergency backstop

In extreme conditions, some DNSPs have the capability to slightly increase distribution network voltages outside of the normal range to curtail distributed PV generation. DNSPs use various mechanisms to deliver distribution voltage increase for this purpose[121], and a range of terms has been used to describe voltage management for distributed PV curtailment across the NEM[122]. For consistency, this paper uses the term 'emergency voltage management' (EVM) to describe all forms of deliberate voltage increase to curtail distributed PV during extreme conditions. Where a DNSP uses a different term it is noted in the accompanying text.

EVM is a higher-impact emergency backstop method than active DER management. It involves moving voltages outside of the normal range, and therefore could have adverse impacts on customers and equipment if used frequently. It is therefore only recommended for use very rarely, and only if other active DER management methods are exhausted and further action is required to maintain system security. It is recommended that sufficient quantities of other forms of active DER management are developed in preference, and EVM is only for use in events where other forms of emergency backstop are insufficient to meet system security needs[123].

Given the anticipated shortfall in emergency backstop capacity in many regions in the NEM in the near term, and the long lead times needed for progressive rollout of active DER management (discussed in section 2.2), it is prudent for jurisdictions and DNSPs to thoroughly investigate the option of EVM, and conduct the necessary safety and technical analysis on whether EVM would be an appropriate and effective emergency backstop method

[121] These can include a combination of manual tap changes at a zone substation, advanced distribution management system (ADMS) controls, SCADA control, and new relays with pre-programmed profiles.

[122] These include:

- 'enhanced voltage management' in SAPN's Emergency standards cost pass through application (https://www.aer.gov.au/system/files/SA%20Power%20Networks%20-%20Cost%20pass%20through%20application%20-%20emergency%20standards%20%28PUBLIC%29.pdf),
- 'dynamic voltage management systems' (DVMS) in CPUE's Submission on Victoria's emergency backstop mechanism consultation paper (https://media.powercor.com.au/wp-content/uploads/2023/08/04131954/230802_Submission_CitiPower-Powercor-UE_emergency-backstop.pdf) and AusNet Services' Response to the Connection Charge Guideline review issues paper on static zero export limits (https://www.aer.gov.au/system/files/AusNet%20Services%20-%20Response%20to%20the%20AER%20-%20Issues%20Paper%20on%20static%20zero%20limits%20for%20micro%20EGs%20-%209%20September%202022.pdf), referring to the technology used to deliver voltage increase, and
- 'emergency voltage management' in the New South Wales Government's *Emergency backstop mechanism and CER installer portal consultation paper*. (https://www.energy.nsw.gov.au/sites/default/files/2025-02/NSW%20Emergency%20Backstop%20Mechanism%20and%20Consumer%20Energy%20Resources%20Installer%20Portal%20consultation%20paper.pdf).

This paper uses 'emergency voltage management' as it represents the clearest description of when and how the mechanism is applied for delivery of emergency backstop. DNSPs may choose to use other terms, particularly if the voltage increase mechanism they use delivers additional network benefits on top of emergency backstop capability.

[123] Including testing where needed to verify the safety, impact and appropriateness of EVM.

for their network[124]. AEMO is not in a position to assess the implications of EVM for safety or customer equipment and recommends this be done by DNSPs and/or other experts in the field[125].

7.1.1 Case study: Accelerated six-month EVM rollout in South Australia

EVM is also termed Enhanced Voltage Management by SAPN as it is also used to regulate voltage levels throughout the year and, under normal circumstances, maximise the amount of energy that distributed PV systems can generate. In early 2021, SAPN rolled out EVM to 138 zone substations within an accelerated timeframe of six months, at a total cost of $9.1 million[126]. SAPN's EVM delivery included a capital expenditure program to enable SCADA-controlled voltage management across 80% of its substations, which required rollout of upgraded voltage controllers. EVM completion within an accelerated timeframe of six months was enabled due to unusual conditions and measures; this included an initial underwriting by the South Australian Government before the AER approved the cost passthrough[127]. Design decisions were also made to meet the timeframe (for example, live telemetry of EVM response is not available because it would have taken longer to implement). SAPN noted that a similar rollout of SCADA-controlled voltage management capabilities could take 18-24 months under normal conditions.

7.1.2 Additional network benefits from EVM

Some types of physical network equipment used to deliver EVM capability may also be capable of utilisation under normal conditions to improve distribution voltage management, which benefits customers by improving DER hosting capacity and improving other power quality metrics. Some DNSPs may already have suitable hardware installed in their networks in many locations. To enable EVM capability for emergency backstop purposes in these networks would therefore require a process of testing, trials and assessment of the suitability of this approach. Further rollout of suitable equipment may also be appropriate in some cases to maximise this capability, as well as deliver benefits for voltage management outside of extreme conditions.

7.1.3 Case study: Use of EVM to maintain system security in South Australia

EVM has been used to maintain system security in South Australia on 14 March 2021[128] and 13-17 and 19 November 2022[129].

---

[124] EVM has the potential to bolster system security and enabled uninterrupted supply for customers by filling the anticipated shortfall in backstop capacity in the near term, and to provide a backup to other preferred mechanisms in the longer term.

[125] If EVM is used regularly for long periods of time, AEMO understands there could be some risks to customers and equipment.

[126] EVM was delivered by July 2021, as noted in SA Power Networks 2022, *Emergency Standards cost pass through application*, https://www.aer.gov.au/system/files/SA%20Power%20Networks%20-%20Cost%20pass%20through%20application%20-%20emergency%20standards%20%28PUBLIC%29.pdf.

[127] The AER's final determination on SAPN's cost passthrough application is in AER 2022, *Determination April 2022 emergency standards cost pass through SA Power Networks*, https://www.aer.gov.au/system/files/SA%20Power%20Networks%20April%202022%20Emergency%20Standards%20Cost%20Pass%20Through%20Determination%20Document%20-%20September%202022.pdf.

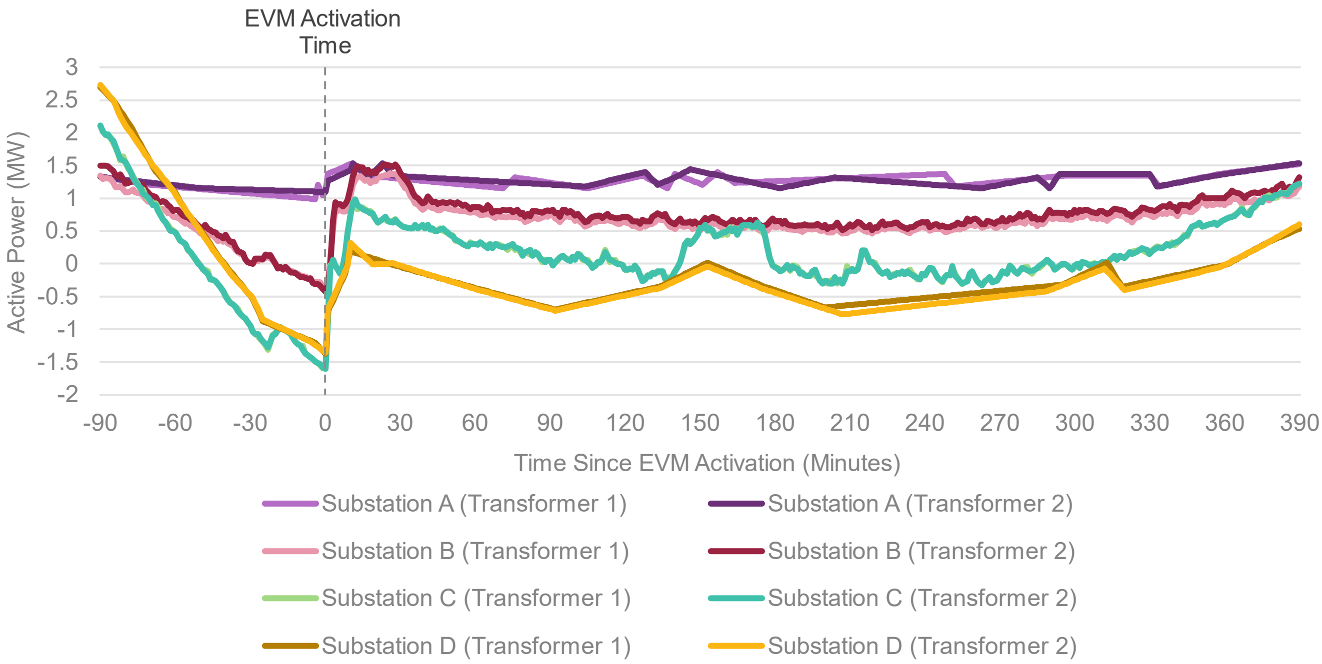
[128] AEMO (November 2021) *Maintaining operational demand in South Australia on 14 March 2021*, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/maintaining-operational-demand-in-south-australia.pdf?la=en.

[129] Curtailment was enacted on 13-17 and 19 November, following the initial incident on 12 November 2022. More information on RA performance can be found in Section 4.2.2 of AEMO's incident report on the event, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en.

On these occasions, EVM was only used when other active DER management methods were exhausted, and further action was required to secure the power system. It is estimated that EVM delivered at least 55-65%[130] of the DER curtailment required. Without this EVM capability, AEMO would have likely been unable to maintain a secure operating state in South Australia during periods of high distributed PV generation.

Figure 6 shows the operational demand profiles at four zone substations when EVM was used on 17 November 2022[131]. The dashed line indicates the start time of EVM use, and each line represents operational demand at the transformer where EVM was used. A clear increase in demand is observed following EVM use, with full response occurring within 10-15 minutes. EVM delivered operational demand increases of 12 MW at three of the four zone substations analysed. The zone substation with the least amount of response (substation A, with a 0.9 MW increase) had a different network configuration and is in an area of the distribution network which often has high voltages.

Figure 6 Changes in operational demand for zone substation transformers where EVM was activated on 17 November 2022



These observations indicate EVM provides a reliable, rapid bulk response. EVM may result in different levels of backstop capability at different substations, with EVM effectiveness varying across the network due to variations in network architecture. Trials, modelling and/or risk assessments can help to improve the estimate of backstop capability delivered from EVM and improve management of risks for safety or customer equipment.

130 As noted in Section 3.3.1 of the 14 March 2021 power system incident report (https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2021/maintaining-operational-demand-in-south-australia.pdf?la=en), and Section 4.2.4 of the 12 November 2022 incident report.(https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf?la=en&hash=A89F330CF6C979E52EF15EB86E5CF058).

131 As at March 2025, 17 November 2022 is the most widespread use of EVM, with SAPN activating all 15 EVM blocks, including three critical blocks. More detail can be found in Section 4.2.4 of this incident report: https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf.

7.1.4 EVM approaches

The use of EVM to deliver emergency backstop capability has the following benefits:

- Robust and reliable physical communications mechanism.
- No scalability issues (as observed for internet-based mechanisms).
- Able to achieve rapid response in a power system event.
- No material increase in cyber risk.
- Does not impact customers or installers at the time of installation (no requirement for capability testing).
- If equipment that can deliver EVM capability already exists in the DNSP network, and their use for EVM is deemed appropriate by the DNSP, there is potential to use this equipment for EVM to achieve a large and rapid bulk response in a power system event.

This approach has the following limitations:

- The implications for safety or customer equipment should be assessed (including through modelling, where needed) by DNSPs and/or other experts in the field. Based on advice from DNSPs, AEMO understands that EVM is not suitable for regular use for long periods of time, so the development of other preferred methods for emergency backstop delivery with lower customer impact is essential.
- Use of EVM impacts all DER on a feeder relatively indiscriminately. This may cause complications. For example, EVM has been observed to result in some distributed PV systems demonstrating cycling behaviour[132]. EVM also may cause distributed batteries to disconnect, including any systems involved in a virtual power plant (VPP) and enabled to deliver frequency response services. These frequency management services may be particularly important in a complex power system event where emergency backstop is being utilised.

If EVM is not available, the only remaining option to maintain power system security in an MSL event may be to shed entire reverse flowing feeders, discussed further in the following section.

7.2 Shedding of reverse flowing feeders (last-resort emergency backstop)

If sufficient emergency backstop capability is not available, shedding of reverse flowing feeders is the only mechanism remaining to increase operational demand to the levels required for system security. This sheds all consumer load on a feeder in reverse flow (for example, whole 11 kV or 22 kV circuits), and therefore has a very high impact on homes and businesses.

This last-resort mechanism has not yet been utilised in any region in practice to manage MSL conditions or when operational demand is near the MDT. However, DNSPs in South Australia and Victoria have prepared processes to deliver this capability if required.

Insights based on discussions with DNSPs include the following:

[132] As noted in Section 4.2.4 of the 12 November 2022 incident report, https://aemo.com.au/-/media/files/electricity/nem/market_notices_and_events/power_system_incident_reports/2022/trip-of-south-east-tailem-bend-275-kv-lines-november-2022.pdf? la=en&hash=A89F330CF6C979E52EF15EB86E5CF058.

- **Visibility challenges** – DNSPs need visibility of which feeders or relays are in reverse flow, ideally in real time. At present, not all DNSPs have live monitoring of reverse flowing feeders, so determining feeders in reverse flow may be challenging. Capital expenditure may be needed to increase visibility. Suitable bi-directional metering at suitable network levels (such as 11 kV/22 kV and 66 kV) can support measurement of reverse flows and facilitate efficient reverse flow feeder shedding.
- **Efficient real-time processes** – efficient delivery requires clear processes to identify and shed reverse flowing feeders, with consideration given to minimising customer impacts, particularly for sensitive loads including life support customers. This might involve developing pre-determined shedding schedules and automated control interfaces. These schedules will likely need to be different to those utilised in load shedding processes, to most efficiently deliver the different objective.
- **Rapid response** – ideally, DNSP systems should target full response in less than five minutes from receipt of instruction, aligned with typical load shedding response times. Automation of control interfaces may improve speed of response and resecuring of the power system. For example, in South Australia, the current process identifies reverse-flowing feeders and sheds them, substation by substation. SAPN is continuing to improve these interfaces to streamline delivery for controllers in complex power system events (for example, working towards putting controls for all reverse-flowing feeders in the same location on the control system).
- **Most granular response possible** – shedding reverse-flowing feeders at the lowest available voltage level (most granular level) maximises the operational demand increase delivered, and reduces customer impact as it impacts a smaller number of customers[133].

If emergency backstop capability and shedding of reverse flowing feeders remains insufficient to restore load back to required thresholds for system security, the power system may be operating insecure for extended periods, placing customers at elevated risk of system collapse.

AEMO recommends that all DNSPs prepare suitable schedules and processes to efficiently shed reverse flowing feeders if necessary, at the most granular level possible to minimise customer impact and maximise benefits. Improvements may be required to deliver adequate visibility of reverse flows, and to facilitate automation and efficient rapid response in a complex power system event.

[133] AEMO 2023, *Under frequency load shedding: Exploring dynamic arming options for adapting to distributed PV – Victorian case studies,* https://aemo.com.au/-/media/files/initiatives/der/2023/dynamic-arming-options-for-ufls.pdf?la=en&hash=F6B7A015C8EB872C83513BA9C95EFE5B.

8 Recommendations

As discussed in other reports, AEMO continues to recommend that operationally effective emergency backstop capabilities are implemented as soon as feasible in all NEM mainland regions[134]. These capabilities should be implemented as rapidly as possible (and may be operationally required by spring 2025), mindful of the practicalities outlined in this report.

To minimise the need for regular use of emergency backstop capabilities, AEMO also continues to recommend efforts towards:

- reform towards efficient market integration of CER, including market systems and strong incentives for customers to participate in markets, and encouraging investment in deep storage and responsive demand,
- pursuing alternative sources of system services during MSL periods, or when demand is close to the MDT, and
- high rates of compliance and conformance with AS/NZS4777.2:2020 technical standards[135,136], including implementation of a national regulatory framework for CER to enforce standards, as identified in the National CER Roadmap.

In considering implementation of emergency backstop measures, this report highlights many important learnings from the extensive experiences of various stakeholders in Australia who have been progressing major work programs to implement these capabilities. There is considerable value in proactively sharing learnings between regions.

Recommendations based on the learnings in this report are summarised below.

Table 11 Recommendations

Stakeholders	Key actions
Governments	• Ensure regulatory frameworks in all NEM mainland regions that deliver capabilities to manage system security in extreme low demand conditions. • Ensure regulatory frameworks allow for regular at-scale testing of emergency backstop.
Governments and DNSPs	• Allow for the long lead-times for implementing operationally effective active management of DER at scale, with significant resourcing for change management frameworks and industry collaboration, engagement and support. Given that operational timeframes are urgent in the NEM mainland regions[A], this may mean progressing other complementary activities to deliver the necessary capability, including the possibility for expanded use of EVM if deemed appropriate for the network. • Consider opportunities for consumer engagement around the positive opportunities from increased CER coordination. • Develop engagement frameworks and incentives to support high installation compliance to emergency backstop mechanisms.
DNSPs	• In implementing emergency backstop measures, continue to draw on the considerable learnings from experiences to date (including but not limited to those outlined throughout this report), and continue active knowledge sharing between DNSPs.

[134] AEMO (Q4 2024) Supporting secure operation with high levels of distributed resources, https://aemo.com.au/-/media/files/initiatives/der/managing-minimum-system-load/supporting-secure-operation-with-high-levels-of-distributed-resources-q4-2024.pdf?la=en

[135] AEMO (December 2023) Compliance of Distributed Energy Resources with Technical Settings: Update, https://aemo.com.au/-/media/files/initiatives/der/2023/oem_compliance_report_2023.pdf?la=en&hash=E6BEA93263DE58C64FCC957405808CA6

[136] AEMO (April 2023) Compliance of Distributed Energy Resources with Technical Settings, https://aemo.com.au/-/media/files/initiatives/der/2023/compliance-of-der-with-technical-settings.pdf?la=en&hash=FC30DF5A3B9EF853093709012242D897

Stakeholders	Key actions
	• Where feasible, design for: – high scalability of emergency backstop mechanisms, and – installer portals and systems to provide automatic notifications to installers (for example, if capability testing challenges are encountered), and – systems for data collection and provision to support consistent understanding of emergency backstop response rates across the NEM. • Prepare suitable schedules and processes to efficiently shed reverse flowing feeders if necessary, as a last resort measure, at the most granular level possible.
DNSPs and Australian Energy Regulator (AER)	• Anticipate significant levels of resourcing required to successfully implement emergency backstop mechanisms at operational scale, particularly for stakeholder engagement and support, scalable emergency backstop design and implementation, and testing to confirm correct setup to receive signals from the emergency backstop mechanism at the time of installation.
AEMO (with DNSPs, TNSPs, OEMs and other technology providers)	• Establish processes for routine at-scale testing of emergency backstop mechanisms across all NEM mainland regions.
All industry	• Continue to work towards national consistency in implementation of standards (such as CSIP-AUS), considering costs
Regulatory bodies	• Consider possible reform pathways to recognise and address governance gaps in: – defining and managing emergency backstop performance, – roles and responsibilities of assessing, enforcing and rectifying DER/CER compliance and conformance[B] with standards, such as emergency backstop and AS4777.2:2020, and – roles and responsibilities for ongoing customer protection, including ensuring return to service and continuity of connectivity. • Develop pathways to account for the important role of OEMs and other technology providers of active DER management (particularly for internet-based emergency backstop), and CER/DER integration and orchestration more broadly. OEMs and technology providers are now playing an essential and active role in real-time power system operation.

A. See https://wa.aemo.com.au/initiatives/major-programs/nem-distributed-energy-resources-der-program/managing-distributed-energy-resources-in-operations/managing-minimum-system-load.
B. The difference between conformance and compliance is outlined at https://www.safeworkaustralia.gov.au/law-and-regulation/duties-under-whs-laws/australian-and-other-standards.

A1. Detailed observations

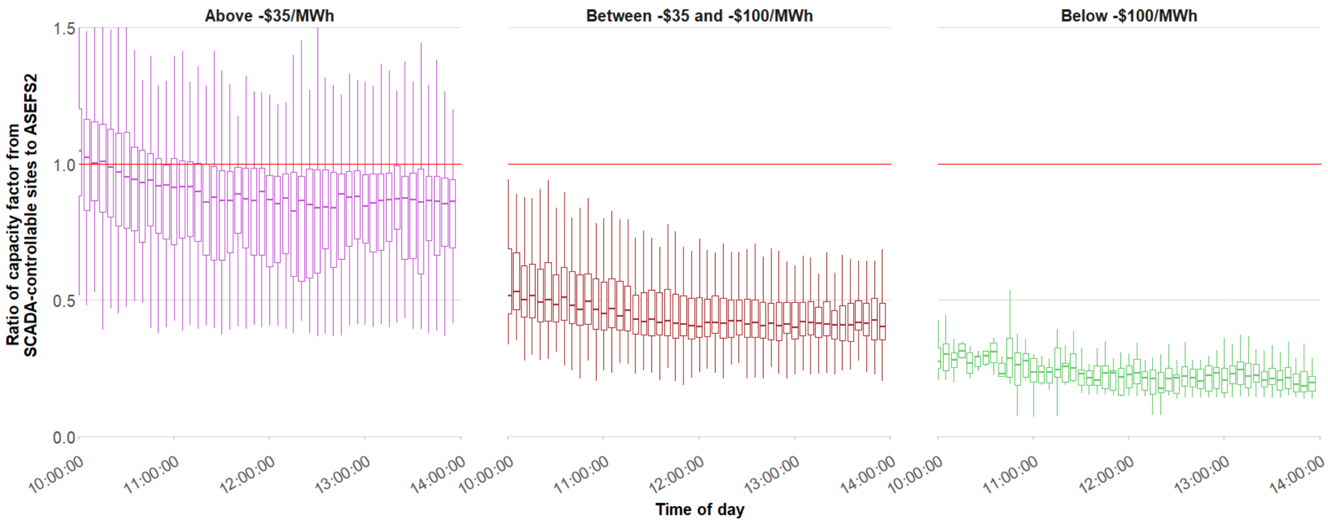
A1.1 Observations from SCADA-controllable sites

Most PVNSG in South Australia is SCADA-controllable. SAPN has consistently noted that SCADA-controllable sites appear to self-curtail during low price conditions (below -$35/MWh), which typically correspond to low demand conditions. They also note that further self-curtailment is observed as prices become more negative (below -$100/MWh).

AEMO assessed historical generation from SCADA-controllable sites for each five-minute dispatch interval in the most recent spring season (September-November 2024). Generation from SCADA-controllable sites is normalised against DER generation (AEMO's ASEFS2 estimated actual generation), on the assumption that ASEFS2 is a reasonable estimate of maximum solar generation available in that period. Values of approximately one (shown by the red line) indicate generation is close to the maximum available solar irradiance, while values below 1 indicate self-curtailment.

Figure 7 shows the results of this analysis, with the left-hand panel showing the spread of generation during high-priced intervals (above -$35/MWh). In these periods, the ratio of SCADA-controllable to ASEFS2 generation sits close to 1:1 (self-curtailment is minimal). The middle panel shows the range of generation during low price periods (below -$35/MWh), with the ratio reducing to 0.5:1, suggesting self-curtailment from SCADA-controllable sites. On the right hand panel, with very low prices (below -$100/MWh), there appears to be even more self-curtailment, with output reducing to 20-30% of typical generation levels.

Figure 7 Spread of SCADA-controllable generation in different price periods, September – November 2024



A1.2 Observations from SAPN RA activation

On 22 August 2024, SAPN initiated a 'fire drill' test of its entire emergency backstop fleet (both RA and FELs). Table 12 summarises the testing schedule.

Table 12 SAPN 'Fire Drill' testing schedule on 22 August 2024

Time (NEM time)	Component of emergency backstop fleet	Installed capacity of distributed PV	Average ASEFS2 CF (%) over test interval	Instruction
0830-0930hrs	One block of curtailment was enabled via RA	100 MW	12%	All systems signalled to curtail to zero site export or zero site generation, depending on the curtailment technology used by the site under the Relevant Agents framework
0930-1030hrs	Second block of curtailment enabled via RA	100 MW	22%	
1030-1130hrs	• Third block of curtailment enabled via RA	100 MW, including 24 MW of FELs	33%	
	• All inverters enabled for FELs (via CSIP-AUS)			All systems signalled to curtail to zero site exports
1430-1530hrs	Fourth and final block of curtailment enabled via RA	100 MW	43%	All systems signalled to curtail to zero site export or zero site generation, depending on technology available in inverter

A1.2.1 Assessment criteria

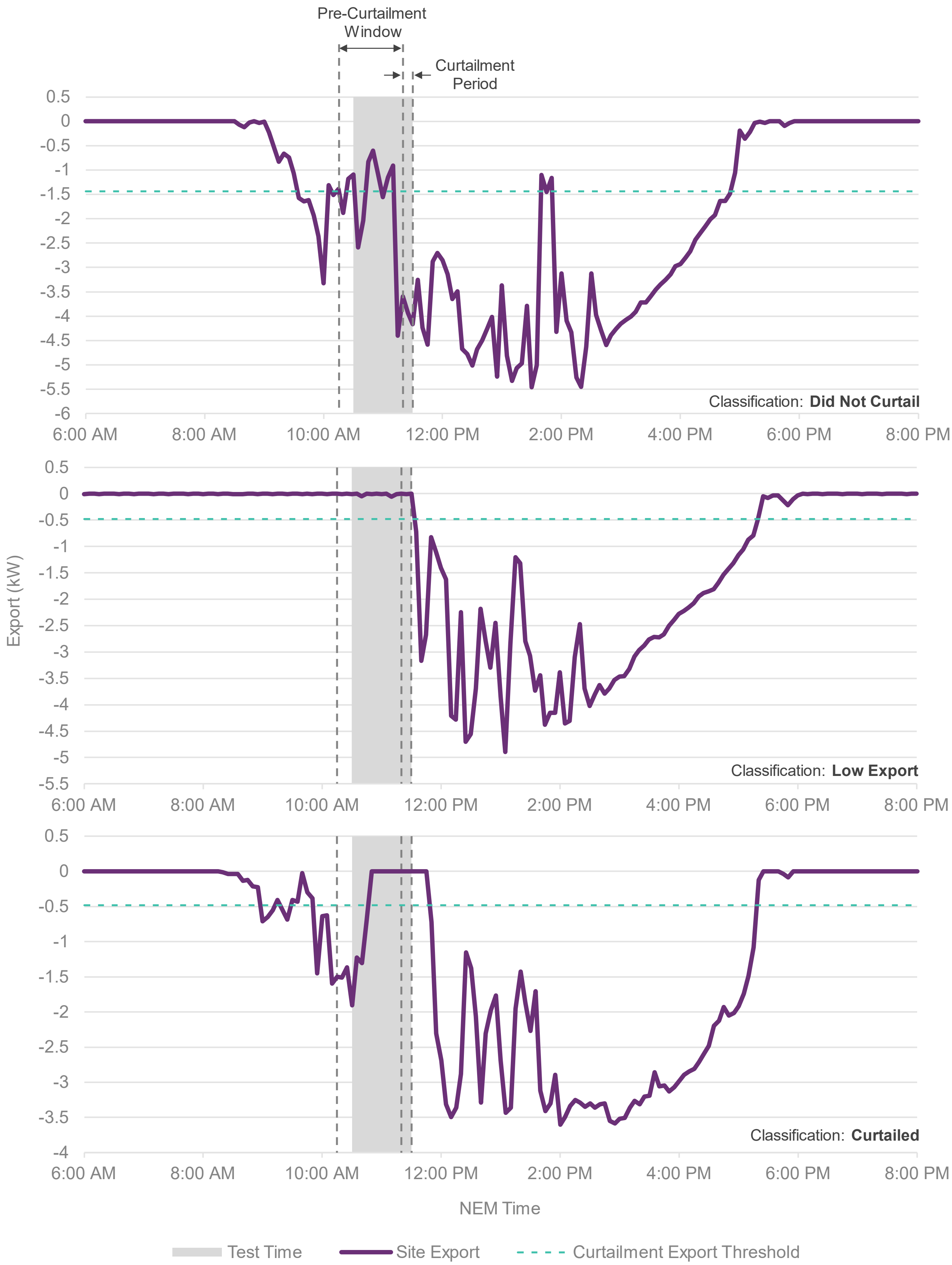
AEMO undertook analysis of five-minute smart meter data available in AEMO's settlement database over the 24-hour period of 22 August 2024 for the ~58,000 RA sites that were activated on the day. Sites were classified based on the criteria outlined in Table 13.

Table 13 RA assessment criteria

	Observed response	Description	
RA fleet	Curtailed	✓	Site exhibited a compliant response and reduced export to close to 0 kW following the curtailment signal.
	No clear response	✘	Site showed no clear response to the curtailment signal for the duration of the curtailment period (non-compliant).
	Low export	?	Response of these sites cannot be determined from the test interval. These sites were not exporting prior to and during the curtailment period.

When calculating the response rate of Relevant Agents to the curtailment instruction issued by SAPN, only sites classified as 'curtailed' or 'did not curtail' were considered. Sites classified as 'low export' were excluded as it is not clear whether these sites responded to the curtailment instruction. Examples are shown in the following figure.

Figure 8 Example classifications for three different sites. Test time: 10:30am -11:30am



A1.2.2 RA analysis results

Table 14 shows the aggregated curtailment numbers for all tests, where a site that curtailed in any test is counted as *curtailed*; sites that were not observed to curtail for any tests, and had sufficient export for a response to be observed, were counted as *no clear response*, and sites that were classified as *low export* in in at least one test and not classified as curtailed in any test are excluded.

Table 14 Aggregated curtailment numbers for the 22 August 2024 all test times (0830hrs, 0930hrs, 1030hrs and 1430hrs NEM time)

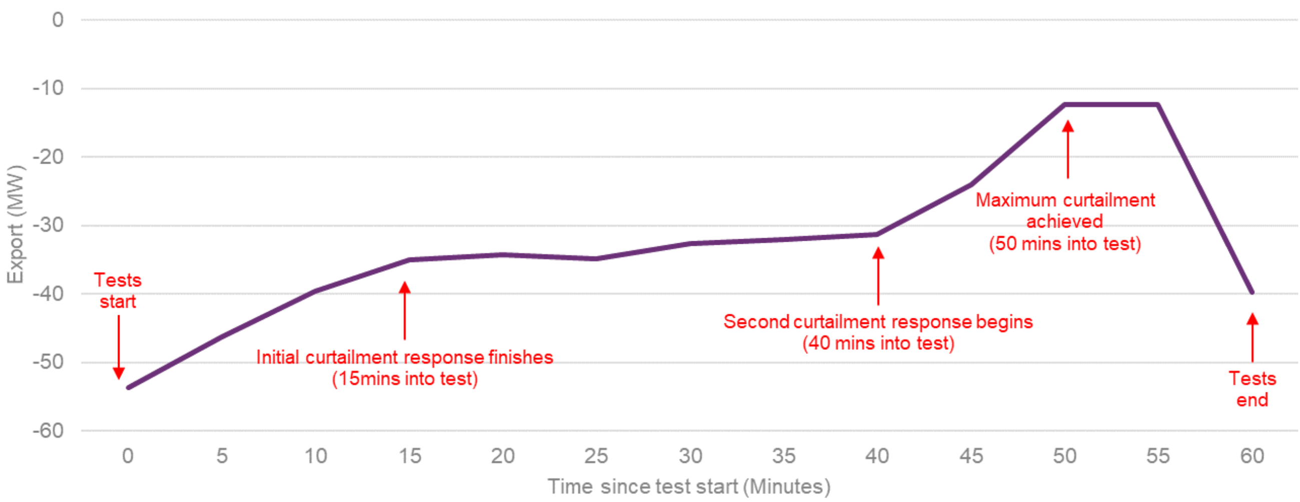
Classification	Number of Sites	% of Sites
Curtailed	19,668	49.3%
No clear response	20,231	50.7%
Total	39,899	100%

Note: this table exclude 18,503 sites that did not have sufficient export to be classified.

A1.2.3 Response profile – RA

Figure 9 illustrates an estimated overall aggregated response curve if the entire RA fleet had been activated at the same time. As capacity factor varied in each of the test periods, RA response in each of the four test periods was scaled to represent expected generation levels based on a solar insolation level associated with a capacity factor of 65%[137] and their start times aligned to estimate the total aggregated RA response. Approximately 41 MW of curtailment was estimated to be delivered within 50 minutes, the maximum curtailment achieved over the test window.

Figure 9 Aggregated RA response curve estimated based on 22 August 2024 fire drill test



Note: this figure contains aggregated RA response across the four test periods: 0830, 0930, 1030 and 1430 (NEM time).

[137] This was the capacity factor during the most recent backstop activation to maintain system security, on 15 February 2024.

A1.3 Observations from SAPN FELs activation

FELs was activated during SAPN's 22 August 2024 fire drill test, and to manage system security on 15 February 2024. AEMO analysed FELs response during both events.

A1.3.1 Assessment criteria

Five-minute smart meter data for all sites eligible for FELs was obtained from AEMO's internal settlement database. The meter data was assessed against the criteria outlined in Table 15.

Table 15 Assessment criteria applied to all sites in SAPN network eligible for FELs on 15 February 2024

	Observed response	Description
Static export limit	**Not compliant to static limit**	Site exported consistently beyond the fixed export limit of 1.5 kW/phase
	Compliant to static limit	Site met the fixed export limit of 1.5 kW/phase
FELs fleet which passed capability tests	**Curtailed**	Site reduced export to close to 0 kW following the curtailment signal.
	Correct fallback response	Site appears to have lost communication with the CSIP-AUS server and exhibited the correct fallback response (reducing export to the fallback threshold for the duration that it did not have active comms).
	Did not export	Response of these sites cannot be determined from this test interval. These sites were not exporting prior to, during and after the curtailment period[A].
	No clear response	Site showed no clear response to the curtailment signal for the duration of the curtailment period.

A. This type of response was found to be especially common in SAPN's 'fire drill' test on 22 August 2024, likely due to the fact that the test occurred in the morning. Sites with BESS typically charge during the morning and only export once the BESS is full, which typically occurs in the afternoon (hours after the test ended).

The following figures show illustrative examples of the sites which fell into each of these categories, with each individual line representing meter data from a site. Several thresholds are used to analyse responses:

- **Measurement capabilities** – approximately ±0.4kW allowance is given to account for metering sensitivities.
- **Curtailment threshold** – the level to which the site is curtailed to in order to be considered compliant. FELs is designed to curtail DER export from the site, meaning self-consumption (where the customer consumes electricity generated by the PV system) can still take place at the site. The curtailment threshold used for this is analysis is 0.48 kW per phase (including the 0.4 kW measurement allowance), shown as the horizontal dashed orange line.
- **Fallback threshold** – the level to which the site is curtailed to if the site loses communications. SAPN has set this fallback threshold at 1.5 kW per phase (1.9 kW per phase including the 0.4 kW measurement allowance), shown as the horizontal dotted green line.
- **Time taken to respond** – the time taken for the site to ramp down to its curtailment threshold. Sites which curtailed within 50 minutes following the curtailment signal being sent out (shown by the dotted vertical line) are considered 'curtailed'.

The examples shown use the 15 February 2024 activation as it was a longer activation and response patterns can be more clearly observed. However, the same assessment criteria and thresholds were applied to both events.

Figure 10 FELs sites categorised as 'curtailed' (15 February 2024)

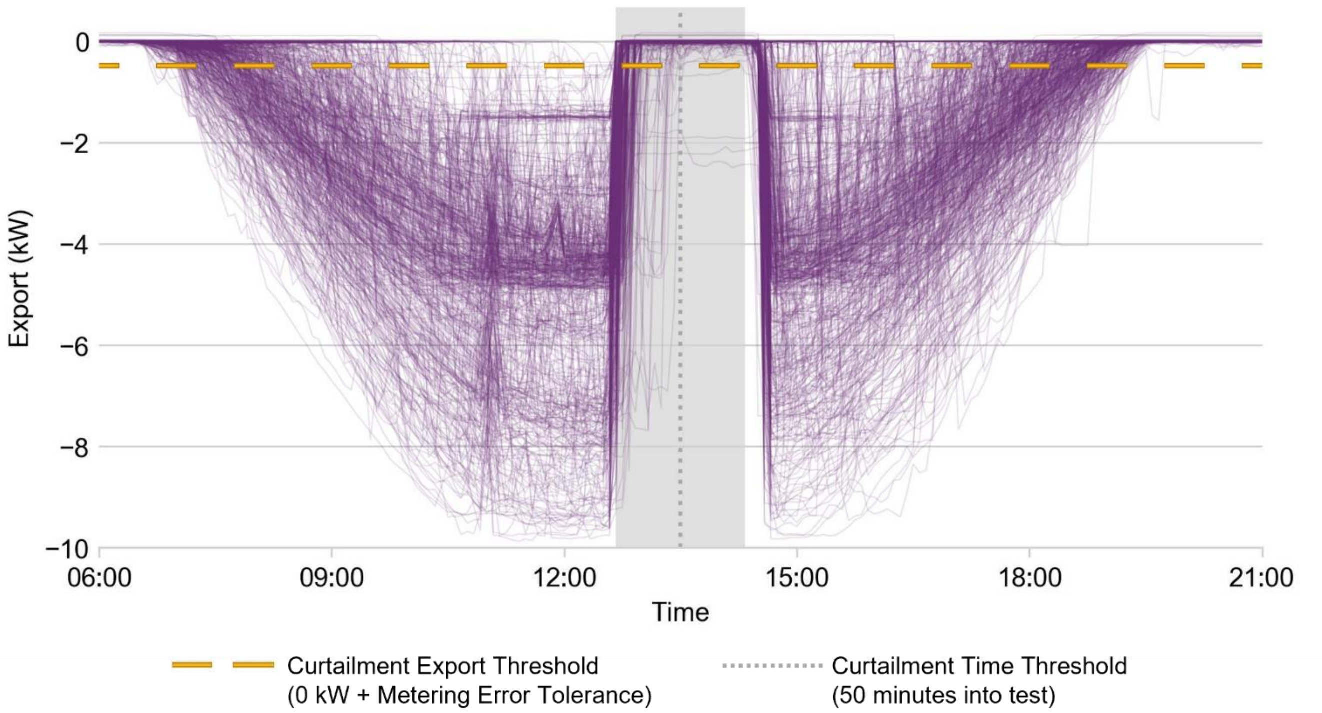


Figure 11 FELs sites categorised as 'correct fallback' (15 February 2024)

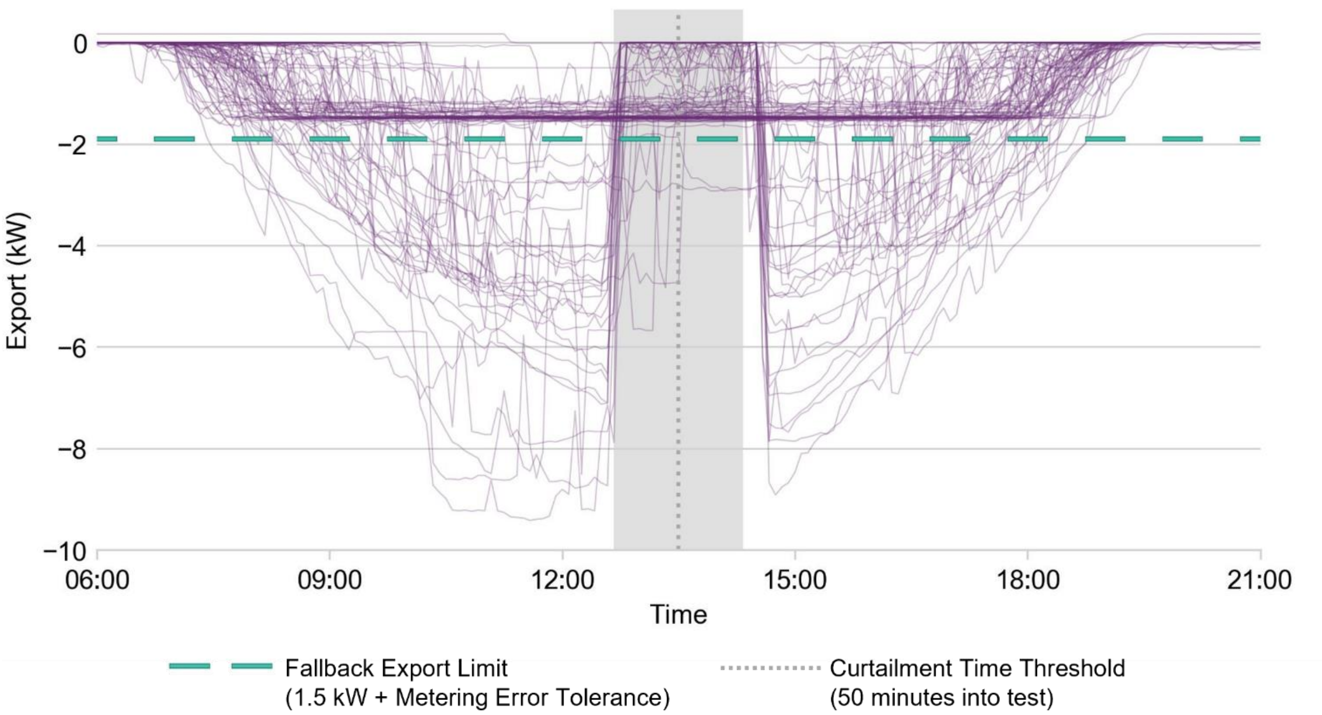


Figure 12 FELs sites categorised as 'did not export' (15 February 2024)

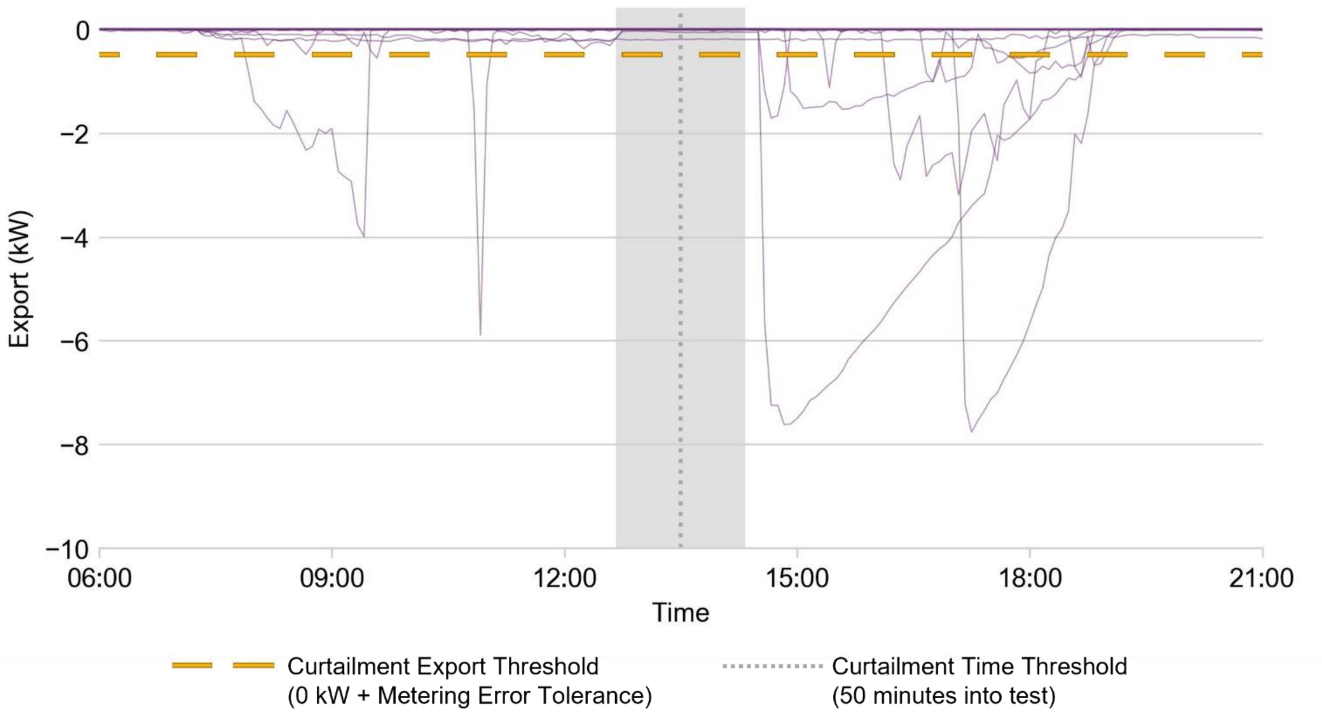
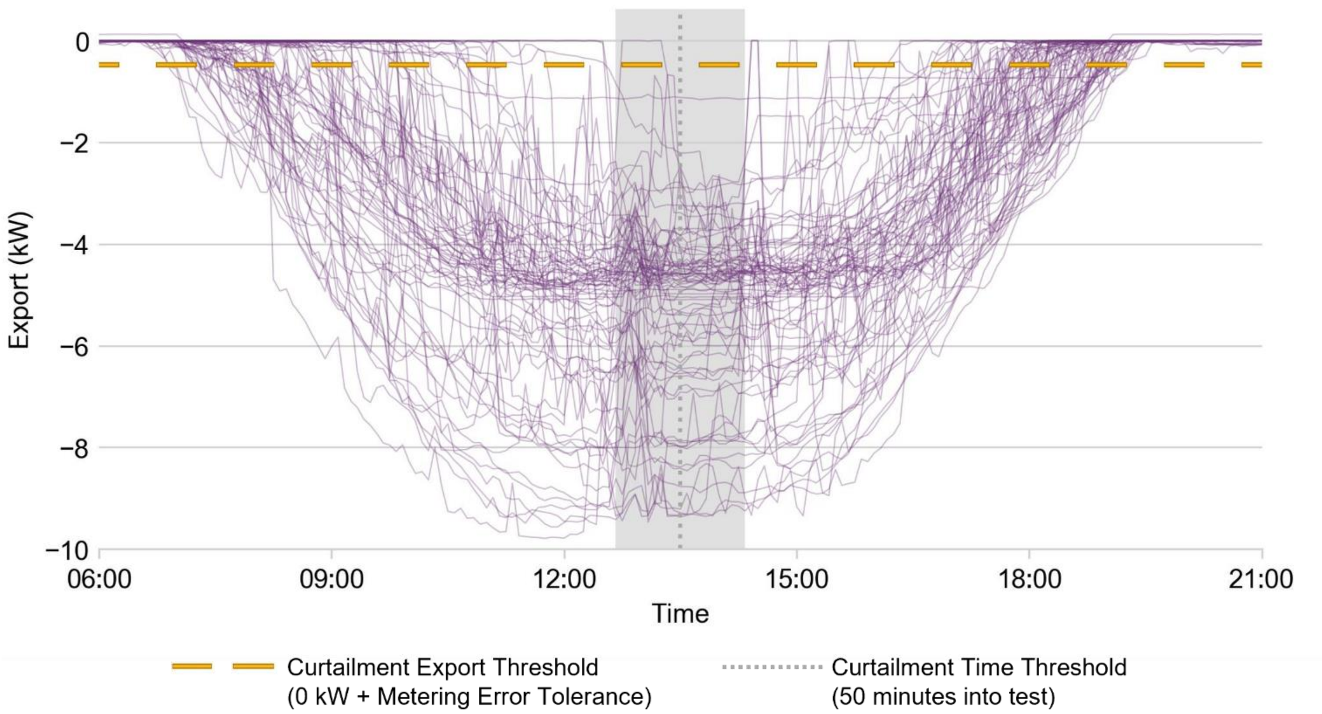


Figure 13 FELs sites categorised as 'no clear response' (15 February 2024)



A1.3.2 FELs analysis results

The response of FELs sites during the 15 February 2024 and 22 August 2024 activations is summarised below in Table 16. Sites that were classified as 'did not export' are excluded from the figures for each activation, as the response of these sites cannot be determined from the two events.

Table 16 FELs Activation Results – 15 February 2024 and 22 August 2024

	15 February 2024 Activation to manage system security		22 August 2024 Fire Drill Test	
Classification	Number of sites	% of sites	Number of sites	% of sites
Curtailed	661	74.4%	1,774	76.0%
Correct Fallback Response	104	11.7%	288	11.7%
No clear response	124	13.9%	273	12.3%
Total	**889**	**100%**	**2,335**	**100%**

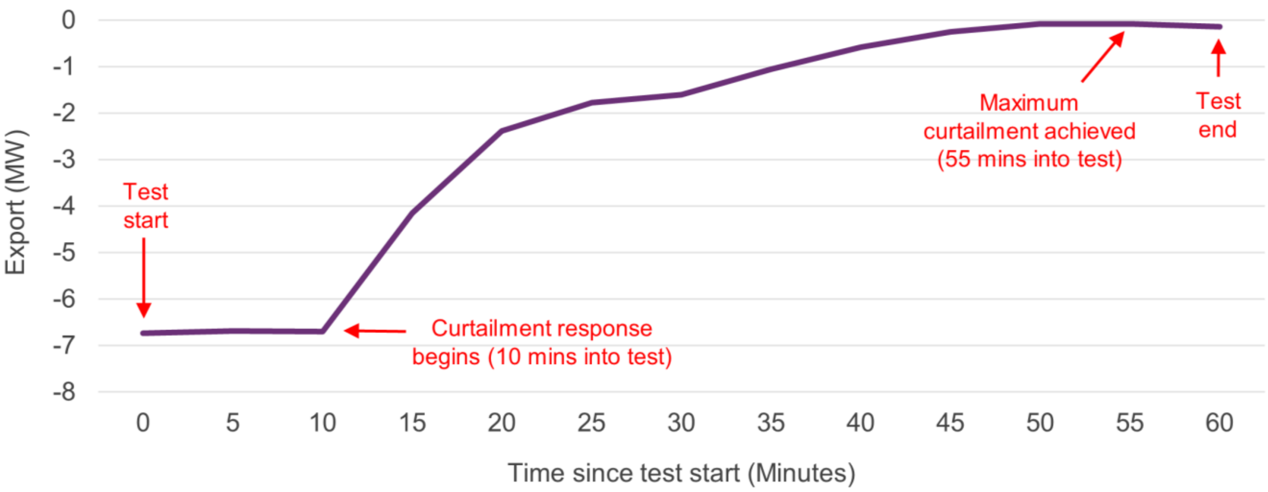
Note: there were 27 sites for the 15 February 2024 activation, and 449 sites for the 22 August 2024 test, that were classified as 'did not export' and are excluded from these results.

Of the sites correctly set up on FELs and passing capability tests, 74%-76% respond correctly during at-scale activations, and 10-15% exhibit correct fallback behaviour. The remaining 10-15% show no clear response to the curtailment signal for the duration of the curtailment period.

A1.3.3 Response profile – FELs

Figure 14 illustrates an estimated overall response profile for the subset of the FELs fleet that responded to the curtailment signal, scaled to a capacity factor of 65%[138]. Approximately 6.7 MW of curtailment was estimated to be delivered within 50 minutes, with the maximum curtailment achieved after 55 minutes.

Figure 14 Aggregated FELs response curve estimated based on 22 August 2024 fire drill test



[138] This was the capacity factor during the most recent backstop activation to maintain system security, on 15 February 2024.

Abbreviations

Acronym	Explanation
AEMC	Australian Energy Market Commission
AER	Australian Energy Regulator
AFLC	Audio Frequency Load Control
AMI	Automated Metering Infrastructure
API	Application Programming Interface
ASEFS	Australian Solar Energy Forecasting System
BESS	Battery Energy Storage System
CER	Consumer Energy Resources
CERR	Clean Energy Regulator Register
CF	Capacity Factor
CPUE	Citipower, Powercor and United Energy
CSIP-AUS	Common Smart Inverter Profile – Australia
Commonwealth DCCEEW	Australian Government Department of Climate Change, Energy, the Environment and Water (distinct from New South Wales DCCEEW)
DCWA	Deemed to Comply Wiring Arrangements
DEBS	Distributed Energy Buyback Scheme
DEECA	Victorian Department of Energy, Environment and Climate Action
DER	Distributed Energy Resource
DERR	Distributed Energy Resource Register
DNSP	Distribution Network Service Provider
DPV	Distributed PV
DPVC	Distributed PV Contingency
DVMS	Dynamic Voltage Management Systems
DVMS	Dynamic Voltage Management System
EDPR	Electricity Distribution Price Review
ESM	Emergency Solar Management
EVM	Emergency Voltage Management / Enhanced Voltage Management
FELs	Flexible Export Limits
FTA	Flexible Trading Arrangements
GMM	Generation Monitoring Meter
GSD	Generation Signalling Device
MDP	Meter Data Provider
MDT	Minimum Demand Threshold
MOPS-MLTS	Moorabool to Mortlake 500kV line
MSL	Minimum System Load
NEM	National Electricity Market
NER	National Electricity Rules

Acronym	Explanation
New South Wales DCCEEW	New South Wales Government Department of Climate Change, Energy, the Environment and Water (distinct from Commonwealth DCCEEW)
NMI	National Metering Identifier
NSG	Non-Scheduled Generation
NSP	Network Service Provider
OEM	Original Equipment Manufacturer
ONSG	Other Non-Scheduled Generation
PPG	Private Power Generator
PVNSG	PV Non-Scheduled Generation
RA	Relevant Agent
RPEQ	Registered Professional Engineers of Queensland
SAPN	SA Power Networks
SCADA	Supervisory Control and Data Acquisition
SEC	Smart Energy Council
SLA	Service Level Agreements
SSP	Secondary Settlement Points
STC	Small-Scale Technology Certificate
SWIS	South West Interconnected System
TNSP	Transmission Network Service Provider
VBM	Victorian Backstop Mechanism
VPP	Virtual Power Plant
VSR	Voluntary Scheduled Resource
WEM	Wholesale Electricity Market