Australian Energy Market Commission

REVIEW

DISCUSSION PAPER

MECHANISMS TO ENHANCE RESILIENCE IN THE POWER SYSTEM - REVIEW OF SOUTH AUSTRALIA BLACK SYSTEM EVENT

15 AUGUST 2019

INQUIRIES

Australian Energy Market Commission
PO Box A2449
Sydney South NSW 1235

E aemc@aemc.gov.au
T (02) 8296 7800
F (02) 8296 7899

Reference: EPR0057

CITATION

AEMC, Mechanisms to enhance resilience in the power system - Review of South Australia Black System Event, Discussion paper, 15 August 2019

ABOUT THE AEMC

The AEMC reports to the Council of Australian Governments (COAG) through the COAG Energy Council. We have two functions. We make and amend the national electricity, gas and energy retail rules and conduct independent reviews for the COAG Energy Council.

CONTENTS

1	Introduction	1
1.1	Background to the review	2
1.2	Scope of this paper and submissions	2
1.3	Assessment framework	3
2	Context and background	5
2.1	A changing power system risk profile	5
2.2	Wind farm feathering and circumstances arising from the pre black system period in South Australia on 28 September 2016	7
2.3	Power system resilience to more severe (HILP) events	9
2.4	A general framework for extending system security arrangements to manage indistinct event risk	13
3	Managing credible indistinct risks	15
3.1	Introduction	15
3.2	Significance of 'contingency' within existing frameworks for maintaining a 'secure' state	15
3.3	Proposals for change	17
4	Enhancing resilience to non-credible indistinct risks	21
4.1	Introduction	21
4.2	How resilience relates to existing arrangements for system security	21
4.3	Frameworks for providing resilience in the NEM – gap analysis	22
4.4	Expanding the existing Power System Frequency Risk Review	24
4.5	Enhancing the existing protected events framework	27
4.6	Framework for monitoring the interconnector flows against a standard	36
	Abbreviations	40
	APPENDICES	
A	Circumstances in South Australia prior to the black system	41
A.1	Circumstances during the pre-black system event period	41
B	Commission and Panel decisions on related frameworks	43
B.1	Declaration of lack of reserve conditions	43
B.2	Amendment of the definition of generating event in the frequency operating standards (FOS)	44
C	Resilience frameworks existing in September 2016	46
C.1	A strong power system	46
C.2	A smarter power system	47
C.3	A more interconnected power system	48
D	Resilience work completed since September 2016	49
D.1	A stronger power system	49
D.2	A smarter power system	50
D.3	A more interconnected power system	51
E	AEMO's Power System Frequency Risk Review	52
E.1	What is a PSFRR?	52
E.2	Why was the PSFRR introduced?	54

F Benefits of the Generalised Power System Risk Review 56
F.1 Time to translate identified risks into a protected event 56
F.2 Better coordination of system risks and services 57
F.3 Consideration of risks associated with distributed energy resources 58

FIGURES

Figure 1.1: Review and paper scopes 3
Figure 2.1: Power system resilience and avoidance, survival and recovery 11
Figure 2.2: Options for enhancing power system resilience 12
Figure 2.3: General framework for extending system security arrangements to manage indistinct event risk 14
Figure 3.1: System security state diagram 16
Figure 4.1: Enhancing system security through a more resilient power system 22
Figure 4.2: Resilience mechanism assessment 23
Figure 4.3: Enhancing system security through a more resilient power system 30
Figure E.1: Process flow of the Power System Frequency Risk Review 53

1 INTRODUCTION

South Australia experienced a 'black system' event at 16:18 AEST on Wednesday 28 September 2016 (the event). The total cost of the black system event to South Australian business was estimated at $367 million and affected approximately 800,000 customers.[1] On 16 December 2016, COAG Energy Council provided terms of reference to the Australian Energy Market Commission (AEMC or Commission) to build on AEMO's incident report and the AER's compliance investigation, by identifying systemic issues that contributed to the black system event in South Australia, or affected the response.[2]

On 7 August 2019 the AER commenced legal proceedings in respect of market participant compliance during the black system event period.[3] As legal proceedings are currently under way, the Commission will not be considering specific issues arising during the period between the loss of the transmission lines in South Australia's mid North and the occurrence of the black system condition.

As a result, this review is therefore limiting its consideration of detailed matters to those arising in respect of the pre and post event periods of the black system event.

This staff discussion paper outlines a set of initial policy positions for stakeholder feedback. It expands on the issues and approach paper that was published on 18 April.[4] This discussion paper provides stakeholders with additional opportunity to provide feedback to the Commission in several key areas prior to the publication of a draft report.

This paper reflects current staff thinking and views in relation to several key policy areas. The Commission's formal policy positions in relation to these issues will be set out in the draft report for the review, which is intended to be published in late September 2019.

Submissions to this paper are due by 6 September 2019.

This paper is structured as follows:

- section 1 introduces the review and purpose of this supplementary consultation paper
- section 2 provides context to the issues being considered in this paper
- section 3 presents initial policy options for managing credible, indistinct risks to power system security, and
- section 4 presents initial policy options for enhancing power system resilience.

The remainder of this section provides background to the review and the Commission's approach to conducting the review. Further relevant information, and more extensive background material, is provided in the issues and approach paper available on the project

1 AEMO, Integrated final black system incident report, March 2017, p. 5.

2 COAG Energy Council, Terms of Reference – Review of the black system event in South Australia on 28 September 2016, 16 December 2016.

3 https://www.aer.gov.au/news-release/south-australian-wind-farms-in-court-over-compliance-issues-during-2016-black-out

4 The issues and approach paper provides comprehensive information regarding the terms of reference, assessment framework, and issues included in the broad scope of the review.

page which can be found at https://www.aemc.gov.au/markets-reviews-advice/review-of-the-system-black-event-in-south-australi

1.1 Background to the review

COAG Energy Council's terms of reference require the Commission to identify and report on any systemic issues that contributed to the black system event in South Australia, or affected the response. Specifically the review is required to build on the findings from the AER compliance and AEMO incident reports by considering whether the power system security frameworks and procedures specified in the NER operated effectively leading up to, during and following the black system event in South Australia on 28 September 2016.[5]

AEMO published its final integrated incident report into the South Australian black system event in March 2017 and in December 2018, the AER published its pre- and post-black system compliance assessment. The AER's published assessment did not consider compliance associated with the circumstances leading to the black system itself, with the AER limiting its reporting to events prior to the loss of transmission lines in SA's mid north and events following the commencement of system restoration.

Although this review is titled the 'South Australian Black System Review', the circumstances of 28 September 2016 are relevant only in as much as they form the starting point for considering how the NER could manage emerging risks to power system security. This review is therefore forward-looking, which seeks to learn from the lessons of 28 September 2016, to deal with future risks.

This review will therefore consider what changes to existing regulatory and market frameworks are necessary to address the systemic issues identified following the SA black system event, rather than further investigating the specifics of the South Australian black system event itself.

1.2 Scope of this paper and submissions

COAG EC's terms of reference can be broadly divided into two key categories being:

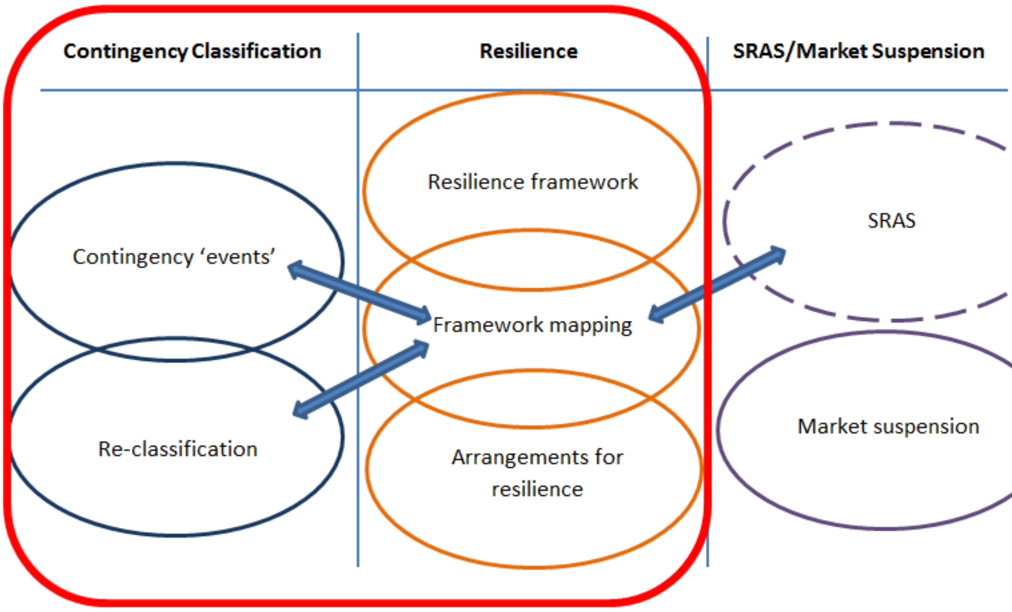
- Whether the power system security frameworks and procedures specified in the National Electricity Rules (NER) operated effectively leading up to, during and following the event, and
- the effectiveness of the power system security framework established under the NER, and other relevant regulatory frameworks to manage high impact, non-credible events.

In addition, the terms of reference require consideration of any improvements in existing processes, tools available to the system operator or components of the electricity system in South Australia (for example, the availability of additional ancillary/system balancing services, additional interconnection with eastern states) that would assist in preventing a recurrence of the events experienced.

5 COAG Energy Council, Terms of Reference – Review of the black system event in South Australia on 28 September 2016, 16 December 2016.

This discussion paper presents a set of high level, draft policy positions in each of these areas for stakeholder feedback, prior to the Commission publishing a draft review report in September 2019. The draft policy positions presented here do not cover the entire scope of the review, focusing on the contingency classification and resilience elements of the review's scope, as set out in the issues and approach paper. Figure 1.1 illustrates the review's scope with issues addressed in this paper indicated by the bold red box. These represent the priority focus areas for the review, as they represent relatively incremental reforms that appear likely to materially increase the resilience of the power system.

Figure 1.1: Review and paper scopes



Source: AEMC

As mentioned in section 1.1, stakeholders are invited to provide submissions to this consultation paper by 6 September 2019. Stakeholders are also welcome to arrange ad-hoc meetings with AEMC staff.

Where practicable, submissions should be prepared in accordance with the Commission's guidelines for making written submissions. All submissions are published on the AEMC website, subject to any claims of confidentiality.

All enquiries on this project should be addressed to graham.mills@aemc.gov.au on (02) 8296 7800

1.3 Assessment framework

The overarching objective guiding the Commission's approach to this review is the National Electricity Objective (NEO). The Commission's assessment of any recommendations must consider whether the proposed recommendations promote the NEO. The NEO is set out in section 7 of the National Electricity Law (NEL), which states:

BOX 1: NATIONAL ELECTRICITY OBJECTIVE

To promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to -

- price, quality, safety, reliability and security of supply of electricity; and
- the reliability, safety and security of the national electricity system.

In addition to the NEO, the Commission has set out a number of principles to guide the assessment of options on potential changes to market and regulatory frameworks relevant to the scope of the review. These principles are:

- Efficient framework design
- proportionality and materiality
- technology neutrality
- flexibility
- risk allocation, and
- effective governance

In making policy recommendations that advance the NEO, the Commission will be considering the trade off between security benefits, weighed against the costs of the proposed policies. In particular:

- additional costs borne today to provide a higher level of protection against adverse circumstances that affect the power system (which could include additional costs from implementing a stronger, more interconnected, or smarter power system), against
- uncertain future benefits associated with a reduction in the consequences of adverse events.

The issues and approach paper presents additional information on, and discussion of the assessment principles guiding the review and the manner in which economic costs and tradeoffs are to be considered.

QUESTION 1: ASSESSMENT FRAMEWORKS

Do stakeholders agree with the Commission's assessment framework?

2 CONTEXT AND BACKGROUND

The nature of the NEM power system risk profile is changing. In addition to the historic forms of variability of load and generation, new forms of generation and other technological changes are creating new kinds of variability, and therefore new risks to be managed through the NER frameworks.

The circumstances leading up to the black system event in South Australia on 28 September 2016 provide a particular illustration of this changing power system risk profile. As such, they motivate consideration of how existing NER frameworks need to evolve, to effectively manage risks arising in a changing power system.

This section provides context and background relevant to the policy proposals outlined in sections 3 and 4. In particular this section introduces:

- concepts relating to a changing power system risk profile
- uncertainty as to whether the existing contingency framework can manage the full set of power system security risks present in a transitioning power system
- a framework for describing power system resilience from a security perspective, and
- a general framework for extending system security arrangements to manage indistinct event risk

2.1 A changing power system risk profile

Historically, the NEM was made up of generally controllable, scheduled generation, which was dispatched at lowest cost to satisfy variable, but forecastable, load. Two distinct types of variability needed to be managed in this situation; slowly varying load during normal operating conditions and the sudden loss of network elements or blocks of generation / load in an emergency. The loss of network elements or blocks of generation / load could be anticipated to the extent that they may or may not reasonably occur, but not when they would occur. This sudden loss of network elements or blocks of generation / load were classified as contingencies and system security frameworks were developed to manage their consequences.

Historically in power system operation, the loss of a single thermal generating unit is a significant event. The large size of these units meant that the loss of a relatively limited number of large generating units needed to be guarded against for power system security purposes. The modes of failure which lead to their sudden unexpected failure or removal from service generally involved internal plant failure given the complex electro-mechanical systems and sub-systems involved. These distinct contingency events have therefore been characterised as the discrete loss of a specific identifiable generating unit, the failure of which was not correlated with the failure of any other single generating unit. A century of experience indicates this approach to be highly effective in managing the range of risks to power system security in a power systems characterised by a small number of large units.

Although these kinds of contingency events still exit, the system is rapidly changing and will increasingly include a new suite of risks. This is because the variability affecting the power system is changing, as the system transitions from one dominated by a relatively small number of large, scheduled generating units, to a system with a relatively large number of smaller, non- and semi-scheduled, variable renewable generating units.

Power systems with high penetrations of variable renewable generation are made up of a much larger number of generating units (each wind turbine may be considered a generating unit in its own right), potentially dispersed over a wide geographical area. These variable renewable generators are also dependent on the availability of their underlying energy resource, either wind speed or solar irradiation. The events which lead to fast renewable variability are often not internal to the unit, but involve weather conditions, such as changes in sunlight intensity or wind speeds. These changes are generally distributed, and can affect a significant number of units and systems in a surrounding area.

These larger, distributed events, such as may arise from a storm front passing across a region, require the aggregate impact on generating systems in the affected area to be considered, rather than the impact on a specific unit.

Growing penetrations of variable renewable generation now produce variability on a spectrum, from small /slow, to large /rapid changes in available generation. While this variability in generation may be managed through dispatch and regulation FCAS where it is relatively small in size, or slow in speed, under certain circumstances the variability may be large and fast enough to create power system security risks.

Furthermore, instead of the event involving a mechanical failure leading to the sudden removal of a specific generating unit (which are generally instantaneous and un-forecastable), renewable generating units and systems can be affected by weather conditions over a period of time, from minutes to hours, and even days. As a result, weather events causing fast renewable generation variability are forecastable, but also include an element of temporal and locational uncertainty.

This review will consider the extension of existing power system security arrangements, to allow for the effective management of these kinds of risks.

This review draws a fundamental distinction between two types of system security events, described here as distinct and indistinct. Distinct risks are taken to be those involving events causing the sudden unexpected loss of a discrete/specific generating system or network element. These events are those that have typically been experienced in historic power systems.

Indistinct risks are associated with distributed events, such as weather conditions, which act on multiple generation and network assets in an affected area, over time. There is substantial uncertainty as to the aggregate size of these events, which are not discrete but may still involve rapid changes in aggregate generation or damage to power system assets. These kinds of indistinct risks can have similar impacts to those associated with the discrete events.

The nature of this new variability, and associated risks, creates challenges for existing security frameworks. This is because those frameworks were designed around the distinct nature of variability and associated risks present in historic power systems. Frameworks must be able to deal with the full set of risks present in a changing power system. Circumstances arising during the South Australian black system event illustrate this changing risk profile and the extent to which the existing NER frameworks benefit from more explicitly addressing these risks; by way of illustration, we provide a brief summary of these examples in the following sections.

In particular:

- During the pre-event period wide area wind farm feathering contributed to Heywood interconnector flows which exceeded their secure limits.[6] While these events were not material in the black system event itself, the AER identified risks to system security which were not actively managed due to uncertainty as to the applicability of system security frameworks to such events.[7] We consider methods to address these kinds of risks in the following sections.
- The tornadoes and storm super cells which were responsible for the loss of transmission lines in the South Australian mid-north are an example of a High Impact Low Probability (HILP) indistinct system security event which challenges the resilience of the power system. These kinds of severe, distributed but indistinct events are not well accounted for under existing frameworks. We have proposed methods to deal with these kinds of events in section 4.

2.2 Wind farm feathering and circumstances arising from the pre black system period in South Australia on 28 September 2016

Through its investigation of AEMO's compliance during the pre-black system event period, the AER uncovered a fundamental disagreement with AEMO as to what kinds of events on the power system can be identified as contingency events. Under existing frameworks for power system security, identification of an event as a contingency event is a crucial first step, before AEMO can take actions to address the risks due to the event.

In the lead up to the black system event, AEMO was operating the South Australian power system with interconnector import limits set to cover the loss of what was considered to be the largest credible contingency within South Australia, being the loss of the 260 MW Lake Bonney wind farm.[8]

However, during this period, the AER's analysis found that there were several extended periods during which the Heywood interconnector experienced flows significantly exceeding its import limits. This occurred due to rapid reductions in wind farm output in South Australia, which are understood to be least partly due to feathering of multiple distributed wind

6 Feathering is an event which involves a wind turbine's control system detecting excessively high wind speed conditions and adjusting the angle at which the wind turbine blades meet the wind, to reduce the aerodynamic load on the machine. This is a known turbine safety mechanism that affects each turbine according to its local meteorological conditions. It is generally understood that feathering begins to occur for wind speeds of 90 km/hr which was significantly below the forecast maximum wind speed on 28 September 2016. When a wind farm undergoes feathering its active power output can drop significantly, and may remain low for as long as the high wind speed conditions remain.

7 AER, The black system event compliance report, p. 190

8 AER, The black system event compliance report, p. 58

turbines across the South Australian region (wind speeds at the time significantly exceeded the 90 km/h feathering threshold).[9] In brief, wind farm feathering refers to the activation of overspeed protection mechanisms on wind farms, which change the pitch of wind turbine blades to reduce speed during high wind speeds, to prevent damage to the generator. This reduces the power output from the windfarm. On aggregate, these reductions can have material impacts on total energy output in a region, if a large number of wind farm generating units in an area all feather at the same time. Appendix A provides an introduction to wind farm feathering and relevant circumstances during the pre black system event period.

AEMO's view was that the NER contingency identification, classification and reclassification framework caters only for the loss of large generating units or transmission elements, which are sudden and unpredictable events. AEMO argued that dispersed and non-instantaneous variations in supply or demand, such as caused by feathering of multiple wind farms, are instead addressed through the dispatch process and are not considered a security issue.[10]

In contrast, the AER considered AEMO to have broad, flexible discretion to decide what constitutes a contingency event under existing arrangements. The AER considered that high wind speeds can potentially cause a loss of output, or failure of wind farm generation units, and thus meets the contingency definition of removing from service one or more generating units. The AER considered that the current contingency definition, and classification / reclassification framework therefore allowed AEMO sufficient flexibility to deal with system security risks caused by feathering.I[11]

A contingency event is defined under clause 4.2.3(a) of the NER as:

"an event affecting the power system which AEMO expects would be likely to involve the failure or removal from operational service of one or more generating units and/or transmission elements".

Key aspects of this definition include:

- an 'event' affecting the power system, and
- 'failure or removal from operational service' of one or more generating units and/or transmission elements.

Clause 4.2.3(a) of the NER is expressed quite broadly, with significant room for interpretation as to its applicability to indistinct events such as wind farm feathering. It is therefore important to have a contingency event definition which is clear as to its applicability to the range of sources of risk to power system security. The following sections present options for managing system security risks from indistinct events as opposed to contingency events involving the 'failure or removal from operational service' of one or more generating units and/or transmission elements.

9 Ibid, p. 42
10 AER, The black system event compliance report, p. 52.
11 bid, p. 32.

2.3 Power system resilience to more severe (HILP) events

The events in South Australia which led to the black system itself involved tornadoes and super cells which brought down a number of transmission lines in SA's mid north. The storm in South Australia and the resulting tornadoes and super cells are an example of a High Impact, Low Probability event (HILP) which tests the resilience of the power system. The review's terms of reference require the Commission to consider power system resilience to HILP events.

Large, distributed power systems like the NEM are routinely subject to a number of disturbances, of varying severity and frequency. The power system is planned and operated on the basis of the frequency and severity of these disturbances, in terms of the impact that the disturbance has on the operation of the power system.

The majority of the disturbances that affect the operation of a power system are classed as credible events. These are disturbances that occur reasonably frequently, with small to moderate impacts, which can easily be modelled. The NER requires AEMO to operate the power system in a secure operating state, which means that the power system is required to return to a satisfactory operating state following a credible contingency event or protected event.[12]

However, power systems can also experience more severe disturbances, such as those experienced in SA, which occur much less frequently than credible contingency events. These events are often referred to as HILP events, and are generally difficult to model. This means their impact is much less predictable, while their probability of occurrence is much less known.[13]

These more severe HILP events can expose the power system to potential cascading failures,[14] which can result in the widespread loss of supply to a large number of customers, or even a black system event.

In a general sense, the ability of the power system to avoid, survive and recover from HILPs can be described as the "resilience" of the power system. This section will present the Commission's framework for understanding power system resilience from a system security perspective. This framework will be applied in developing the policy proposals presented in section 4.

12 See clause 4.2.4 of the NER. The power system is in a satisfactory state when the power system frequency and voltages are within acceptable limits defined by the relevant standards, the power system equipment is operating within its ratings, the fault level is within the rating of the circuit breakers and the system is stable. See clause 4.2.2 of the NER.

13 The causes of HILP events are varied and may include natural events such as floods, cyclones, tornadoes, earthquakes, tsunamis or space weather events. In addition, cyber-attacks or physical attacks on power system infrastructure may also severely impact the operation of the power system.

14 A cascading failure can also be described as an uncontrolled failure of parts of the power system, which can lead to a major supply disruption, or ultimately a black system event. As an example, a cascading failure may occur where the loss of a single generator disturbs the system to such an extent that a subsequent generator trips, in turn further destabilising the system and causing further units to trip. A cascading failure is still possible following a credible contingency if the system's behaviour does not match models. This can occur if generators or network plant do not meet the required performance requirements or the models are deficient.

2.3.1 A framework for power system resilience

In a general sense, the ability of the power system to avoid, survive and recover from HILPs can be described as the "resilience" of the power system. Power system resilience is a relatively new concept and there is not a commonly accepted understanding of what it denotes and how it can be modelled.[15] However, as discussed in further detail below, in this paper, we will generally consider power system resilience in the NEM in the context of the following ways in which it responds to high impact, low probability events:

- **avoidance:** The avoidance phase involves preparing the power system for HILP events. This can include:[16] 1) developing new special protection and emergency frequency control schemes that would limit the severity of a severe event (an example of an emergency frequency control schemes would be an automatic under-frequency load shedding schemes), 2) changing generator technical performance standards to enhance the ability of connected generators to withstand disturbance conditions, and 3) reclassification of a non-credible contingency as credible, where there is sufficient cause to do this.
- **survival:** The ability of the power system to survive a HILP event will depend on the technical performance of generating systems and network being maintained at a sufficiently high standard to be able to support the operation of the system and remain operating during disturbances. For example, having sufficient inertia, system strength and other services within the power system will support the operation and survival of the system during a HILP event. Other survival mechanisms include the effective operation of special protection schemes and emergency frequency management schemes designed to shed load, generation or trip network elements in order to arrest the progress of a cascading outage.
- **recovery:** The ability to restore the functionality of the power system to the pre-contingency level following a major disturbance will depend on a period of time following the disturbance where the status of the power system is assessed and an action plan developed to return the power system to its pre-disturbance level of functionality. This relies on the operation of system restart services, where there has been a major supply disruption or black system event, restarting of any additional generation necessary to meet demand, reconnection of supply to affected customers, and the repair of damaged equipment, which may take several weeks and be necessary to restore supply to some customers.
- **learning:** The ability of stakeholders, particularly AEMO as the system operator, to learn from major power system incidents will depend on the quality and quantity of measurement data, post event analysis and reporting following a major power system incident, the level of compliance analysis by the relevant regulators and the flexibility of the governance arrangements for the NEM.

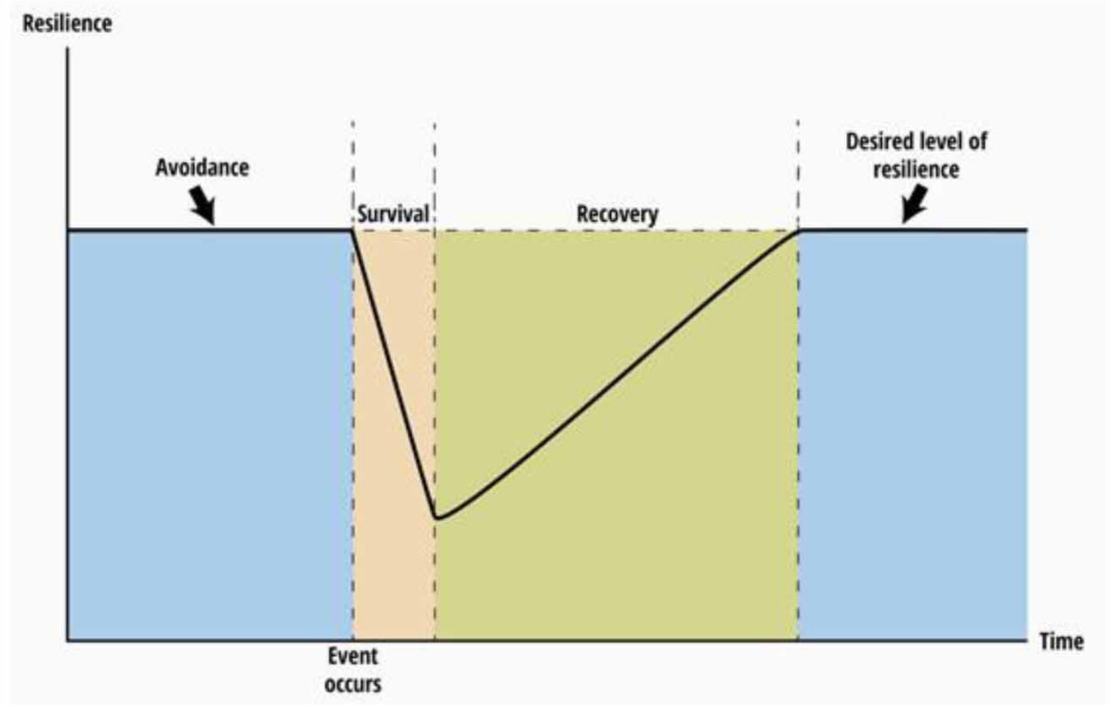
---

15 However, a number of papers have been published which propose ways of conceptualising resilience. In particular, we have utilised the conceptual framework described in the following paper, as a way to think about resilience in the NEM. See: *Power systems resilience assessment: hardening and smart operational enhancement strategies*, M. Panteli, D. Trakas, P. Mancarella and N. Hatziargyriou, Proceedings of the IEEE, Vol. 105, No. 7, July 2017.

16 Several of the measures listed are applicable across avoid, survive and recover.

Figure 2.1 illustrates each of these stages (avoidance, survival, and recovery) in response to a high impact - low probability event affecting the power system.

Figure 2.1: Power system resilience and avoidance, survival and recovery

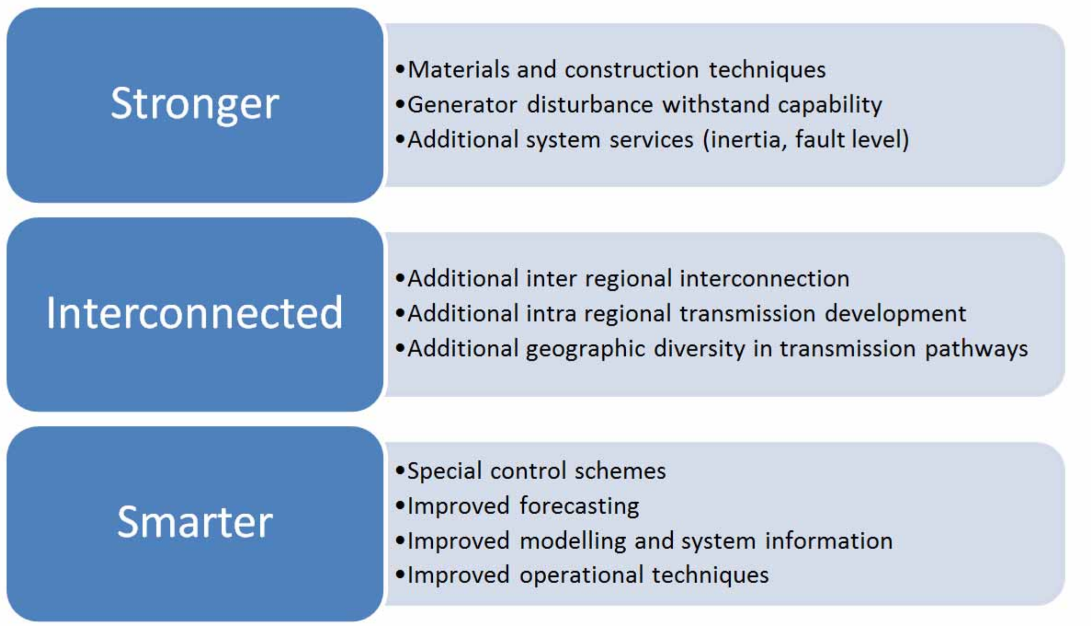


Source: AEMC

The resilience of a power system may be enhanced through a range of measures. These measures can be classified as a more interconnected grid, a stronger grid or smarter processes to avoid or survive emergency events.[17] Figure 2.2 provides a visual summary of some the classes of options that can be used to provide and enhance power system resilience.

17 See: *The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience*, M. Panteli, P. Mancarella, IEEE Power and Energy Magazine, June 2015.

Figure 2.2: Options for enhancing power system resilience



Source: Adapted from - *The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience*, M. Panteli, P. Mancarella, IEEE Power and Energy Magazine, June 2015

Stronger - A stronger grid can be achieved by increasing the level of certain power system services (such as inertia and fault level) and increasing the ability of generating systems to withstand voltage and frequency disturbances.

For example, in South Australia, the retirement of the Northern Power Station in March 2016 reduced the amount of synchronous generation in the SA region and contributed to the loss of physical attributes that have traditionally been provided as an inherent characteristic of energy generated by synchronous generators. The loss of physical inertia was particularly important in the events leading to the South Australian black system event.

Interconnected - A more interconnected grid involves physical changes to network configuration. These changes may act to make the network less vulnerable to severe events. This can include additional geographic diversity in transmission line siting, re-routing transmission lines to areas less affected by extreme weather, and introducing additional interconnection between regions. Arrangements in the NEM for increasing interconnection are particularly contemplated by the review's terms of reference which require the Commission to consider whether additional interconnection with the eastern states would assist in preventing a recurrence of the South Australian black system event.

Smarter - A smarter grid can involve a broad set of actions that improve the observability, controllability, and operational flexibility of the power system in responding to HILP events. In addition to decision-making regarding re-classification of certain disturbances, the implementation of special protection schemes which pre-emptively shed load on observation of a high impact low probability event, and improvements in modelling and forecasting of such events, are also examples of smart measures to improve the resilience of the power system. Smart measures may be thought of as additional 'tools' for the system operator as specified by the review's terms of reference.

As described above, the NEM regulatory frameworks already include a number of measures that provide a degree of resilience to HILP events. Section 4 will present a gap analysis identifying areas for future framework development to enhance power system resilience.

2.4 A general framework for extending system security arrangements to manage indistinct event risk

System security arrangements that are fit for purpose should account for the full range of risks to power system security. As the risk profile of the power system changes and indistinct events grow in frequency and magnitude, there will be an increasing need for existing frameworks to be clarified and extended to manage these risks.

This paper presents some indicative policy positions for extending system security frameworks to address risks from indistinct events arising in respect of a transitioning power system.

Figure 2.3 graphically depicts a general framework for extending system security arrangements to manage indistinct event risks. The top two quadrants represent the traditional framework for system security. The top left-hand quadrant represents the set of all credible, 'distinct' contingency events for which AEMO is required to maintain the power system in a secure state (green). The top right-hand quadrant represents the set of all distinct, non-credible events, for which emergency under frequency load shedding is implemented and system restart services are procured (yellow).

As the risk profile of the power system changes, there is a need to expand this conceptual framework to include the bottom two quadrants shown in Figure 2.3. These additional quadrants are intended to capture the new kinds of risks to the power system, arising from indistinct events that are uncertain and for which the impact on the power system cannot be easily linked to a single, identifiable power system asset.

The green bottom left quadrant, covers indistinct events considered to be reasonably possible and therefore credible. Under the proposed framework we set out in section 3, AEMO would face a requirement to maintain the system in a secure state for these risks. The bottom right quadrant involves arrangements for managing indistinct, non-credible risks such as the HILP events described above. We describe some potential new mechanisms to managing these events in section 4.

This paper considers arrangements for managing indistinct power system security risks in the bottom two quadrants. We have described indicative policy positions for the development of new arrangements for managing risks associated with renewable variability which is reasonably possible (an example being the wind farm feathering experienced during the pre-black system period), and arrangements for efficiently enhancing power system resilience to more severe HILP events, such as the super cells and tornadoes that bought down transmission lines in South Australia's mid north leading to the black system event.

Figure 2.3: General framework for extending system security arrangements to manage indistinct event risk

Source: AEMC

QUESTION 2: CONTEXT AND BACKGROUND

- Do stakeholders agree with the staff view on the need to extend system security frameworks to clearly manage risks from indistinct events?

3 MANAGING CREDIBLE INDISTINCT RISKS

3.1 Introduction

This section proposes arrangements for extending existing frameworks for managing risks to power system security associated with indistinct events which are reasonably possible and therefore credible. The focus is on arrangements in the bottom left quadrant in Figure 2.3, specifically involving system security frameworks for maintaining the power system in a secure state.

This section initially describes the significance of 'contingency' within existing frameworks for maintaining a 'secure' state, before proposing a set of arrangements in the following areas:

- adjusting the criteria for AEMO to operate the system in a secure state, to account for the consequences of different forms of variability arising from indistinct events
- providing for the use of a probabilistic approach to characterising variability arising from indistinct events relevant to system security settings, and
- setting thresholds for the variability arising from indistinct events requiring management through system security frameworks.

3.2 Significance of 'contingency' within existing frameworks for maintaining a 'secure' state

The preliminary policy position is that the criteria for maintaining the power system in a secure state needs to be augmented, to extend the frameworks to manage system security risks so that they apply to the variability arising from indistinct events and conditions which are considered reasonably possible, and therefore credible.

The NER defines power system security as the safe scheduling, operation and control of the power system on a continuous basis in accordance with the power system security principles.[18] The power system security principles include the following key elements:

- to the extent practicable, the power system should be operated in a secure operating state, and
- following a contingency event (whether a credible or non-credible contingency) AEMO should take all reasonable steps to return the power system to a secure operating state as soon as practicable and in any case within 30 minutes.

A "secure" operating state has a particular meaning under the NER. Specifically, clause 4.2.4 of the NER states that the power system is defined to be in a secure operating state if, in AEMO's reasonable opinion, taking into consideration the appropriate power system security principles:

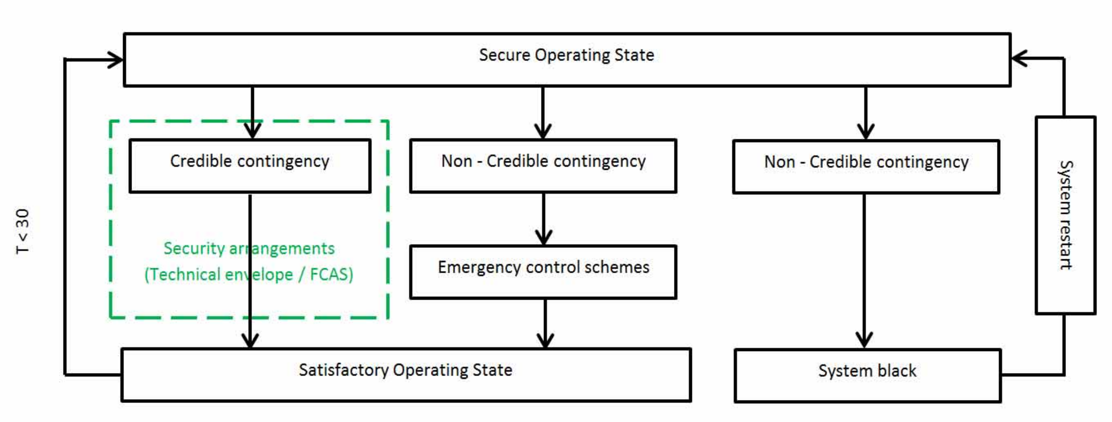
- the power system is in a satisfactory operating state, defined under the NER, and

18 Chapter 10 of the NER, Glossary

- the power system will return to a satisfactory operating state following the occurrence of any credible contingency event or protected event in accordance with the power system security standards.

The criterion for a secure state, being that the power system will return to a satisfactory operating state following the occurrence of any credible contingency event, is an example of an n -1 criteria. This determines the constraints applied to the operation of the power system. These in turn determine, amongst other things, the amount of ancillary services procured, and allowable network and interconnector flows.

Figure 3.1: System security state diagram



Source: AEMC

In order to remain in a satisfactory operating state following a credible contingency, AEMO applies constraints to dispatch to define a technical envelope within which the power system is to be operated (the technical envelope represents operating limits applied to each element of the power system) and provides sufficient reactive power and frequency response to manage any credible contingency.[19] These arrangements are represented by the left most path in the above figure, which shows a credible contingency event surrounded by a dashed green box. This dashed green box represents the technical envelope and other security arrangements which maintain the power system in a secure state given the occurrence of any credible contingency.

19 The technical envelope is reflected in the operational constraints applied to the operation of the power system. Constraints include inter-regional interconnector flows, intra-regional transmission flows, and generator dispatch. These constraints are to reflect thermal, voltage, and transient stability limits in the power system.

The criteria for maintaining the system in a secure state, as implemented by AEMO, currently only account for distinct contingency events and does not allow the technical envelope to be adjusted to manage system security risks which are not considered to be contingency events.

These are the circumstances that applied in respect of wind farm feathering during the pre-black system period on 28 September 2016. AEMO did not consider the existing criteria allowed it to adjust the technical envelope, by constraining Heywood interconnector flows, as it did not consider wind farm feathering to be a contingency event and therefore could not be included in the set of contingencies considered in maintaining the system in a secure state.

Circumstances arising in South Australia illustrate that, as the risk profile of the power system evolves, arrangements regarding the technical envelope may require clarification so it appropriately reflects the full range of risks present in the power system. In order to extend existing frameworks to manage indistinct risks which are considered reasonably possible, and therefore credible, the criteria for maintaining the system in a secure state requires consideration and clarification.

3.3 Proposals for change

Given the above, existing system security frameworks can be expanded, to clearly address the changing risk profile of the power system, including the emergence of indistinct system security risks. In particular, such risks are arising from increased generation variability due to distributed weather conditions.[20]

This section recommends an approach to integrating these indistinct risks into system security frameworks, allowing for the management of events which are reasonably possible and therefore considered credible. Arrangements for managing indistinct risks which are not reasonably possible, and therefore considered non-credible, will be addressed in section 4. This section will set out high level policy positions in the following areas:

- adjusting the criteria for a secure state to account for the consequences of different forms of variability arising from indistinct events
- providing for the use of a probabilistic approach to characterising variability relevant to system security time scales, and
- setting thresholds for the variability requiring management through system security frameworks.

3.3.1 Augmenting the criteria for a secure state

The current criteria for maintaining the power system in a secure state can be described as an n-1 requirement. Under this approach, the power system is operated to account for distinct credible contingencies. This requirement obliges AEMO to maintain the system in a satisfactory state, and avoid load shedding, in response to the loss of any *single* network element or generating system.

20 Note that distributed weather conditions are not the sole source of such variability which can include load variability and generator non-conformance with dispatch instructions. Renewable generation variability is a focus of this assessment given the specific circumstances arising during the pre-event period of the South Australian black system event.

However, in a power system with high penetrations of variable renewable generation, weather conditions lead to indistinct events giving rise to generation variability. Some level of variability can always considered present, due to the daily variability in weather conditions. Under more adverse weather conditions, more significant levels of variability can be expected, such as the wind farm feathering experienced in South Australia during the pre black system event period.

The key issue to be considered in developing criteria for secure operation is therefore what level of renewable variability is considered reasonably possible, and what level is considered not reasonably possible.

Further to this, while significant levels of renewable variability may be reasonably possible on their own, it may not be considered reasonably possible for this variability to occur at the same time as a distinct contingency event, or during the period when AEMO is restoring the power system to a secure state following a contingency event.[21]

When considering the renewable variability that can be considered reasonably possible, we have identified a need to break levels of variability into the following two categories:

- levels of variability considered reasonably possible at the same time as a credible contingency event (in combination), and
- levels of variability considered reasonably possible, and therefore credible *on a standalone basis*, but which are not reasonably possible to occur in combination with a distinct credible contingency.

The first of these two categories identifies a certain amount of renewable variability which must be guarded against, at the same time as the largest credible contingency. This could be implemented by augmenting the existing n-1 criteria to become an "n - 1 (plus)" criteria.

As an example, a possible n – 1 (plus) criteria may require AEMO to operate the power system by setting the technical envelope to account for the largest distinct credible contingency, plus the amount of variability that is considered reasonably possible in the area being considered. In effect, this n-1 (plus) approach builds in an amount of "headroom" above the largest distinct credible contingency, to account for the variability associated with distributed, variable generation.[22]

The second of these categories represents the largest amount of forecast variability considered reasonably possible in the area being considered, but which would not be considered reasonably possible to occur at the same time as the largest credible contingency. The probability of the two conditions occurring together would be too low to be considered reasonably possible. However, this largest amount of forecast variability could be considered reasonably possible on a standalone basis during a given forecast period, and would represent a stand-alone event to be guarded against, in its own right.[23]

21 It is not credible for two credible contingencies to occur together.

22 This could be assessed based on day ahead or hour ahead forecasts.

23 This could be assessed on the basis of forecast conditions.

The decision as to what is reasonably possible, and therefore which of the two categories would be used, will change over time. Obviously, as more information becomes available closer to real time, AEMO will be better positioned to decide what events have become reasonably possible. Staff are interested in applying a probabilistic approach for this purpose.

3.3.2 Utilising a probabilistic measure for characterising uncertainty arising from indistinct events

A probabilistic approach may be used to characterise renewable variability arising from indistinct events considered reasonably possible, for the purpose of managing the power system in a secure state. A probabilistic approach would allow this variability to be characterised, enabling AEMO to form a view on how much is reasonably possible given a set of forecast conditions. The outcome of this process would allow the additional headroom considered under the n – 1 (plus) approach to be determined.

A probabilistic approach is already utilised in forecasting of reserve levels in the NEM, as part of the operational reliability frameworks. The declaration of lack of reserve conditions (LOR) rule change changed the process of declaring low reserve levels in the NEM from being a deterministic process, based on the largest contingency, to utilising a probabilistic approach. This change was made to allow AEMO to account for factors not currently considered when assessing reserve conditions such as forecast error in load and generation (further details on this decision are provided in Appendix B).[24]

AEMO has implemented the forecasting uncertainty measure (FUM) as a probabilistic approach for this purpose. This approach involves characterising the magnitude of forecast error according to forecast lead time, temperature, wind, solar, and other forecast weather conditions. AEMO has implemented a Baysian belief network with historic data for this purpose. The Baysian belief network produces a distribution of possible forecast errors which may arise from applicable conditions. LOR levels are then triggered on the basis of the largest of the distinct contingency based approach and forecast uncertainty.

While the current application of the FUM is for reliability, the FUM is an approach that may also be applied to characterising fast renewable variation as a function of a wider set of risk factors than simply the set of distinct credible contingencies. Staff are considering the practicalities associated with applying an analogous approach to the FUM in a system security setting.

3.3.3 Thresholds applying to variability relevant to system security time-scales

In contrast to the discrete change in generation associated with a distinct contingency, renewable generation variability arising from indistinct weather events exists on a spectrum of speed and significance. For example, under certain circumstances, renewable variation can be sufficiently rapid and large to impact system security. At other times, renewable variability may be slow or small enough to be considered immaterial from a system security perspective. To incorporate these events in system security frameworks, a view is required on the speed and size of the generation variability that qualifies as a risk to system security.

24 AEMC, declaration of lack of reserve conditions – final determination, p. ii

The Reliability Panel considered this matter when it amended the definition of generation event in the FOS to include rapid ramping (further details on this decision are provided in Appendix B). The Panel specified sub 30 second variability and a magnitude of at least 50 MW as the speed and significance thresholds to qualify as a generation event for frequency management purposes. The 30 second threshold was selected to reflect limitations in the response speed of the regulation FCAS system. The 30 second threshold may, or may not, be appropriate for managing indistinct event risk in system security frameworks more generally. Further consideration will need to be given to different approaches to setting the speed of variability which qualifies for system security management purposes.

The other relevant threshold involves the size of the generation variability required to be a system security risk. One of the defining characteristics of the events that give rise to fast renewable variation, such as storm fronts, is their distributed nature. The impact of such events therefore needs to be considered in terms of the aggregate change in generation across the generating systems in an affected area. Therefore, the size threshold in MW, will depend on the area affected by the event. From this, generation variability thresholds could be defined on several scales from system level, sub-regional, regional, to NEM wide.

The areas considered when setting specific variability size thresholds may be informed by the system risks being considered. Thresholds relating to frequency or transient stability may be defined at a regional level considering all variable generation within that region, while thresholds relating to voltage or system strength may be best defined at a sub-regional, or even generating system level, given their more localised nature.

There may also be several thresholds defined in respect of a single area. As an example, a frequency threshold may apply to South Australia as a whole, but with a voltage threshold reflecting network constraints applying to the wind farms in the state's mid-North. Therefore, a wide range of different significance thresholds may need to be defined to capture the full set of risks arising from indistinct events, rather than a single 50 MW threshold as is the case in the FOS. Staff intends to consider these issues further.

QUESTION 3: MANAGING VARIABILITY ARISING FROM CREDIBLE INDISTINCT RISKS

- Do stakeholders agree that the criterion for a secure system requires amendment to account for risks arising from generation variability due to indistinct weather events?
- How do stakeholder see a probabilistic approach being applied in practice and integrated into AEMO operational practices, such as forecasting and pre-dispatch?
- What characteristics of variability should apply to the variability qualifying for management under system security arrangements (speed, and significance)?
- What governance arrangements and arrangements for transparency, such as the issuance of market notices, should apply to this process?

4 ENHANCING RESILIENCE TO NON-CREDIBLE INDISTINCT RISKS

4.1 Introduction

The COAG Energy Council's terms of reference require the Commission to consider the effectiveness of the power system security framework to manage high impact, low-probability (HILP) events.

In this paper the term resilience refers to the ability of the power system to contain and manage the risk of a cascading (uncontrolled) failure following a disturbance event, particularly a HILP event. Other uses of the term resilience in power systems are out of the scope of this paper.[25]

This section addresses existing and potential future frameworks for resilience in the NEM and is divided into the following parts:

1. results from a gap analysis of arrangements relevant to power system resilience in the NEM
2. expanding the existing Power System Frequency Risk Review process
3. enhancing the existing protected events framework to manage non-credible indistinct event risk, and
4. developing a standard for managing and monitoring interconnector flows within secure limits.

4.2 How resilience relates to existing arrangements for system security

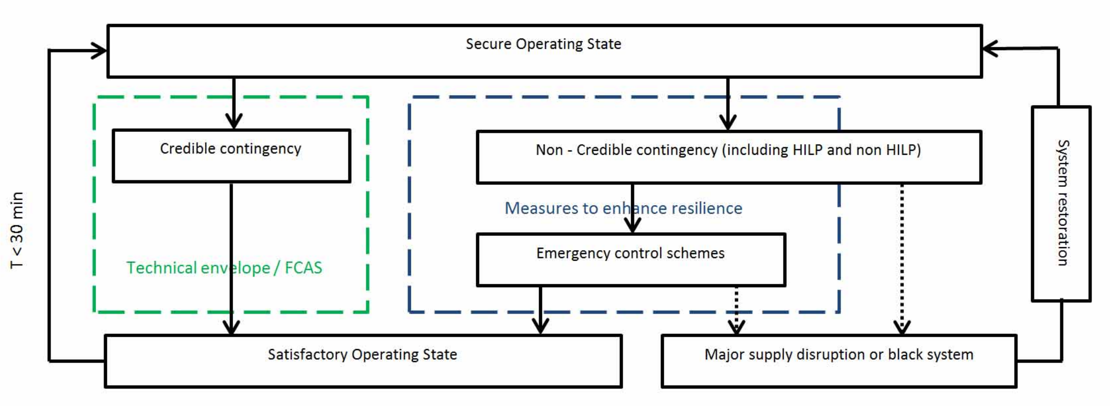
As introduced in section 2.3, this review considers system resilience mainly through the lens of avoiding, surviving, recovering and learning from HILP events, by enhancing the strength, smartness and interconnectedness of the power system. Existing NER frameworks include arrangements which already provide measures relevant to power system resilience. As such, resilience should be viewed in the context of the existing NER frameworks and the extent to which they can be evolved, rather than completely new frameworks.

Figure 4.1 demonstrates how resilience relates to the existing NER frameworks for system security. Measures to enhance resilience increase the probability of the power system ultimately returning to a satisfactory operating state following a non-credible contingency, rather than ending in a major supply disruption or black system event. Measures to enhance power system resilience are represented in this figure by the dashed blue box which complement arrangements for a secure power system represented by the dashed green box.

25 There are a number of other definitions of resilience that have been used historically. Firstly, this includes automation of the distribution network, which improves the resilience of the network to disturbances such as severe storms or other attacks. The impact of high impact-low probability events within large distribution networks is also a major concern in some power systems. An example of such an event would be hurricane Sandy in 2012 that resulted in power outages to over 8 million people across 21 states, for days and even weeks. Secondly, resilience is sometimes used in reference to the reliability of the power system, where reliability outcomes are improved when the system is resilient to the loss of a major power station or an unexpected reduction in intermittent generation.

Importantly, Figure 4.1 demonstrates that a system may be resilient while also allowing some load shedding to occur following a HILP event. Controlled automatic load shedding may be a key component of the survive stage of resilience, provided it prevents an uncontrolled, cascading failure and degradation to a black system. This represents a key distinction between arrangements for power system resilience to HILP events and the requirement for maintaining the system in a secure state for credible contingencies.

Figure 4.1: Enhancing system security through a more resilient power system



Source: AEMC

The concept of power system resilience focusses on how a stronger, more interconnected and smarter grid may enhance the ability to avoid, survive, and recover from HILPs. However, enhancing power system resilience may also assist in keeping the power system stable and secure in the presence of credible contingency events. For example, requiring additional inertia or fault level to provide greater resilience for non-credible events may also improve the performance of the power system to credible contingencies, potentially relaxing the technical envelope or requiring less ancillary services to maintain the system in a secure operating state. That is, a more interconnected, stronger, and smarter grid may also reduce the operational measures required to maintain the power system in a secure state under existing frameworks.

The benefits of actions to enhance power system resilience will therefore not only include a reduction in the costs associated with high impact low probability events, but may also reduce the ongoing costs associated with the actions AEMO takes to manage power system security.

4.3 Frameworks for providing resilience in the NEM – gap analysis

This section sets out a high level gap analysis by applying the framework for power system resilience presented in section 2.3 to NEM arrangements. The gap analysis allows the contribution of existing frameworks to be understood, thereby allowing areas for future framework development to be identified.

Figure 4.2 shows a summary matrix of this mapping, through the dual lenses of avoid–survive-recover-learn and stronger-smarter-interconnected. The table is not intended as an exhaustive set of mechanisms in the NER and NEM power system, but rather provides an overview of the main mechanisms that provide resilience. The mapping is colour coded into three groups:

- **Black** - mechanisms that existed at the time of the South Australian black system event
- **Blue** - mechanisms that have been introduced since September 2016
- **Green** - areas identified for future framework development.\

Figure 4.2: Resilience mechanism assessment

	Avoid	Survive	Recover	Learn
Stronger	• intermittent forecasting • interconnector limits • NSCAS • additional FCAS • updated power system models • refined forecasting	• FCAS • NSCAS • GTPS • GTPS update • minimum inertia and fault level • primary frequency control and other services	• SRAS • updated power system models • GTPS update • enhanced SRAS and restoration frameworks	• AEMO incident reports • generalised power system risk review (discussed in Part 2)
Interconnected (all major network augmentations)	• TNSP APRs • RIT-T • ISP interconnections	• TAPRs • RIT-T • ISP interconnections	• more SRAS options • restart using interconnectors	• AEMO incident reports • ISP for potential projects
Smarter	• contingency classification • demand forecasting • intermittent forecasting • power system models • protected events • enhanced protected events (discussed in Part 3) • interconnector flow management (discussed in Part 4)	• network and generator protection schemes • under-frequency load shedding scheme • special protection schemes • protected events • System Integrity Protection Scheme (SIPS) in South Australia • SPS (new) • post-cascade islanding • management of smart controller software upgrades	• Updated power system models, aiding in SRAS procurement • more effective SRAS testing processes	• AEMO incident reports • updated power system models • power system frequency risk review • generalised power system risk review (discussed in Part 2) • interconnector flow monitoring (discussed in Part 4)

Source: AEMC

Appendices C and D provides a detailed breakdown and consideration of the mechanisms listed in Figure 4.2. From this analysis staff have identified the following as focus areas for potential new mechanisms. Specifically, the three mechanisms discussed in following parts of this section being:

- a generalised power system security review
- an enhanced protected events framework, and
- new arrangements for monitoring and managing interconnector flows.

These mechanisms have been identified as they represent relatively incremental changes, are inter-related, can be implemented reasonably quickly and are likely to deliver material resilience benefits.

A number of the other mechanisms identified in Figure 4.2 as candidates for future framework development are currently being considered as part of other AEMC processes, such as the primary frequency response rule change requests. Others will be more appropriately considered through other processes, after this review, including joint work programs between the AEMC, AEMO and the AER.

4.4 Expanding the existing Power System Frequency Risk Review

The Power System Frequency Risk Review (PSFRR) was introduced in 2017 as a part of the Emergency Frequency Control Schemes rule change.[26]

The PSFRR is an integrated, transparent framework for the consideration and management of risks associated with some non-credible contingencies.

AEMO is required to undertake, in collaboration with Transmission Network Service Providers (TNSPs), an integrated, periodic review of power system frequency risks associated with non-credible contingency events. Conducted at least once every two years, the PSFRR considers non-credible contingency events that could involve uncontrolled increases or decreases in frequency leading to cascading outages or major supply disruptions.

The PSFRR has two main purposes. It seeks to reveal to the market:

- whether, in order to limit the consequences of some non-credible contingency events, there is a need to introduce, modify or adapt automatic schemes to shed load or generation, or
- whether it would be economic for AEMO to operate the power system in a way that limits the consequences of certain high consequence non-credible contingency events, should they occur. This process can lead to the declaration of a protected event by the Reliability Panel.

The PSFRR, however, specifically focuses on *frequency* risks for a range of non-credible contingency events, and therefore does not consider all possible risks associated with non-credible contingency events in the NEM.

Given the changing risk profile in the NEM, staff propose holistically identifying the range of risks arising from uncertain and indistinct non-credible contingencies, through some form of overarching risk identification and assessment process.

Any such risk assessment framework should account for the full range of risks to power system security. These extend beyond frequency management, and may include consideration of factors such as voltage management, system and transient stability, system restoration and new types of operational risks resulting from managing a changing generation mix. This review should also extend beyond the large scale, transmission level power system, to consider emerging risks associated with the rapid uptake of DER at the distribution level.

26 AEMC 2017, Emergency frequency control schemes, Rule Determination, 30 March 2017,

Staff have identified an opportunity to expand the scope of the PSFRR into a 'General Power System Risk Review' (GPSRR). This risk identification and assessment process would expand on the existing governance arrangements and areas of focus in the PSFRR. The objective of a GPSRR would be to provide a comprehensive stock-take of all security related risks existing in the NEM, as well as formulating an integrated, transparent framework that develops recommendations for addressing all risks in a systematic manner.

In considering expanding the PSFRR into the GPSRR, stakeholders have raised a number of issues in relation to the existing process:

1. it takes too long for AEMO to undertake the PSFRR process to identify a system need, and too long to translate this need into an application to the Reliability Panel for declaring a protected event. Stakeholders have also argued it takes too long for the Panel to assess AEMO's application and declare a protected event
2. the scope of the PSFRR is too narrow, and should be expanded to consider a broad range of risks to the power system, including fault levels, inertia, voltage, new operational risks and resource variability, and
3. the PSFRR is too shallow, as it only requires AEMO to undertake a periodic review in collaboration with TNSPs (and not DNSPs), and does not consider emerging risks on distribution networks, particularly those attributable to increased DER. Increasingly, the changing DER landscape may result in new and uncertain risks to the security of the power system, which are best identified and addressed through collaboration between AEMO and all relevant NSPs.

Staff propose to address these issues through the development of the GPSRR. The specifics of these changes are provided in detail in Appendices E and F, and are summarised below:

- Given the pace of change in the power system, staff consider a GPSRR process should reduce the time taken to translate identified risks into a protected event, or the development of other solutions to address those risks. In particular, various options exist for streamlining the existing two stage Reliability Panel approval process for declaration of a protected event. Streamlining may include introducing a mechanism similar to the NEL expedited rule change process, to reduce consultation to one stage after publication of a consultation paper, after which the Reliability Panel would proceed to publish a Final Determination. Such an approach may be appropriate where AEMO has proposed a low cost protected event, where a majority of stakeholders are likely to be supportive of the proposed change. However, an option could be included to defer to a full process, if either the Panel or stakeholders consider more thorough analysis is required.
- Better coordination of system risks and services. The PSFRR specifically considers frequency risks. However, a sole focus on frequency does not capture all possible risks associated with non-credible contingency events in the NEM. There are existing processes followed by AEMO that, if coordinated and integrated into a holistic GPSRR assessment process, could provide for a more comprehensive understanding of changing system security requirements, and a more efficient pathway to managing the risks these changes present. A coordinated assessment of all system security risks, through the GPSRR, could therefore assist in a more efficient deployment of system services to address system

needs. These include frequency and, voltage control, measures to enhance system strength, as well as allowing identification of potential future services as the power system transitions.

- Consideration of risks associated with distributed energy resources. AEMO has identified that high DER penetration, in particular small rooftop PV, may have increasing implications for the secure operation of the system. The proposed GPSRR would require the involvement of DNSPs alongside TNSPs as currently required under the PSFRR, and would include consideration of distribution level issues, particularly increased DER penetration. The formal inclusion of DNSPs in the GPSRR would capture and allow for the management of emerging risks associated with DER is a systematic manner.

A more complete discussion of the potential benefits of, and options for a GPSRR is provided in Appendix F.

QUESTION 4: EXPANDING THE EXISTING POWER SYSTEM FREQUENCY RISK REVIEW

What are stakeholder views on:

- Incorporating all assessment of system service requirements (inertia and fault level) as part of the single risk review process?
- Incorporating DNSPs as formal members of the process in order to capture risks associated with high levels of DER?
- How an expanded GPSRR would be integrated with other AEMO planning processes, notably the ISP?
- How the GPSRR should best facilitate a time efficient process of identifying risks and implementing arrangements to manage those risks (through the declaration of a protected event, or RIT-T/D)?
- How frequently should the GPSRR be published - would a yearly publishing requirement adequately balance the time required for AEMO conduct a thorough review, against the need to regularly capture the changing risk profile of a transitioning power system?

4.5 Enhancing the existing protected events framework

This section sets out our high level approach to developing a mechanism to manage indistinct, HILP events primarily identified through the GPSRR.

The current framework in the NER for managing risk to power system security was designed for distinct contingency events, such as the disconnection of a transmission element or generating unit. Historically, this approach worked well for the management of risks to system security.

As discussed in section 2.2, indistinct events do not fit clearly into the existing definition of a contingency event. This section therefore proposes enhancements to the protected event framework to enhance power system resilience to indistinct, non-credible events.

4.5.1 Existing protected event framework

The NER currently includes a protected events framework that enhances power system resilience by allowing AEMO to take certain actions to manage power system security risks arising from specific non-credible contingencies. Protected events are declared by the Reliability Panel, following a request by AEMO in respect of a risk identified in the PSFRR. Once a protected event is declared by the Panel, AEMO is required to take sufficient actions so that a protected event should not lead to a cascading failure and hence a major supply disruption and a black system event.

In practice, protected events represent a sub-category of non-credible contingencies, where the probability and consequences of a specific non-credible contingency event are such that special action is warranted to limit the consequences of the event.

Importantly, AEMO is allowed to take some ex-ante actions for a protected event, such as constraining dispatch or procuring additional FCAS. This differs from a normal non-credible contingency, where AEMO does not take ex-ante actions to manage its consequences, but instead relies only on measures like emergency automatic under-frequency load shedding schemes to stabilise the system following occurrence of the event. AEMO is also obligated to manage power system frequency to a wider band for a protected event (as compared to that which is required for a credible contingency), which means that some load shedding may occur following the event.

The protected event framework is linked to the PFSRR. The PSFRR is the process via which non-credible contingency events are identified as candidates for declaration as a protected event. Following identification of a non-credible contingency which can be managed through the protected events framework, AEMO applies to the Reliability Panel for declaration as a protected event. In doing so, AEMO must propose a solution, which may include network augmentations or non-network solutions, as well as specific ex-ante operational actions to manage the protected event. The Reliability Panel is responsible for assessing the application and deciding whether to declare the protected event.

The first protected events declaration was made for South Australia on 20 June 2019. This is summarised below.

BOX 2: SOUTH AUSTRALIAN PROTECTED EVENT DECLARATION

In its 2018 PSFRR, AEMO concluded that the risk of transmission faults in South Australia causing significant loss of generation, which may subsequently lead to the loss of the Heywood interconnector, is heightened in periods when 'destructive wind conditions are forecast in the region. In these conditions, AEMO considered there to be a heightened risk that the magnitude of generation loss will cause cascading failures leading to large-scale blackouts.

AEMO therefore submitted a request to the Reliability Panel in November 2018 seeking the declaration of a protected event in order to assist the management of power system security in South Australia.

To manage the event, AEMO recommended:

- upgrading the existing System Integrity Protection Scheme (SIPS); and
- limiting the total import capacity over the Heywood interconnector to 250 MW at times when destructive wind conditions have been forecast in South Australia.

The Panel accepted AEMO's cost benefit assessment and approved AEMO's recommended option as the most robust and cost-effective approach for managing the risks identified.

In declaring the protected event, the Panel made AEMO's use of the protected event subject to certain requirements, including:

- The pre-contingent import limit applied to the Heywood Interconnector during forecast destructive wind conditions is to be initially set at 250 MW and reviewed by AEMO through the PSFRR or in the event of any power system conditions changing
- The issuing of forecasts for destructive wind conditions in the South Australia region as the trigger event for AEMO applying the pre-contingent import limit on the Heywood

As the South Australian protected event declaration was the first application for a protected event, a number of potential issues with the framework were identified during its assessment. The following three key issues were identified:

- uncertainty whether the protected events framework allows for the consideration of changing environmental conditions
- the relative inflexibility of the framework, and
- the time taken to identify and implement a protected event.

During the assessment process, there was some uncertainty as to whether the protected events framework allows for the consideration of changing environmental conditions. In particular, it was uncertain whether a protected event could be declared to apply only during high wind conditions, as requested by AEMO, rather than on a standing basis. While the Panel's protected event declaration ultimately allowed for this (and legal advice suggests it is not explicitly precluded by the NER), the framework was not explicitly developed for that purpose.

The protected events framework is also tied to the existing definition of contingency event.[27] As discussed in section 2.2, the NER is unclear whether indistinct, weather dependent events qualify as contingency events. It follows that there may be some uncertainty whether such events are captured by the existing protected event frameworks.[28]

Secondly, AEMO has said the existing protected events framework is inflexible, as it only allows AEMO to take action on occurrence of specific conditions, as pre-identified in the protected events declaration. For example, AEMO may only take action under the declared SA protected event on forecasts of "destructive winds" (defined as winds above a limit of 140kph by the Bureau of Meteorology). This means that AEMO cannot take pre-emptive action in the presence of potentially damaging winds which do not quite meet this fixed threshold, regardless of potential consequences.[29]

The current framework also does not allow AEMO to take pre-emptive action for events other than those defined in the protected event declaration. For example, if the declared protected event is related to high wind speeds, AEMO would not be able to take action for other types of supply side variability, such as heavy, rapidly moving cloud fronts creating large fluctuations in solar availability.[30]

Finally, as discussed in section 4.4, some stakeholders have argued that the time taken to request and declare a protected event is too long. This can mean that AEMO may be less able to adjust its operational processes to account for new and emerging threats to system security.

Given these issues, there is a need to evolve the protected events framework to effectively enhance the resilience of the power system to indistinct, non-credible events. The following sections describe the proposed evolved protected events framework, its operation, and associated governance arrangements.

27 The NER define a protected event as "a non-credible contingency event that the Reliability Panel has declared to be a protected event under clause 8.8.4, where that declaration has come into effect and has not been revoked. Protected events are a category of non-credible contingency event".

28 It is acknowledged that the Panel's final declaration of a protected event allowed for what could be loosely defined as non-traditional event, being the "loss of multiple transmission elements causing generation disconnection in the South Australia region during periods where destructive wind conditions are forecast by the Bureau of Meteorology ". The fact that multiple, unspecified elements are referenced, conditional on the occurrence of general weather conditions, could be argued to reflect the kinds of indistinct / non-traditional events we considered in the 9 July paper. However, it is also the case that the NER frameworks that underpinned the Panel's decision do not make it particularly clear that this is an appropriate interpretation. In any case, we consider there is benefit from the provision of further clarity and guidance.

29 Other than reclassification.

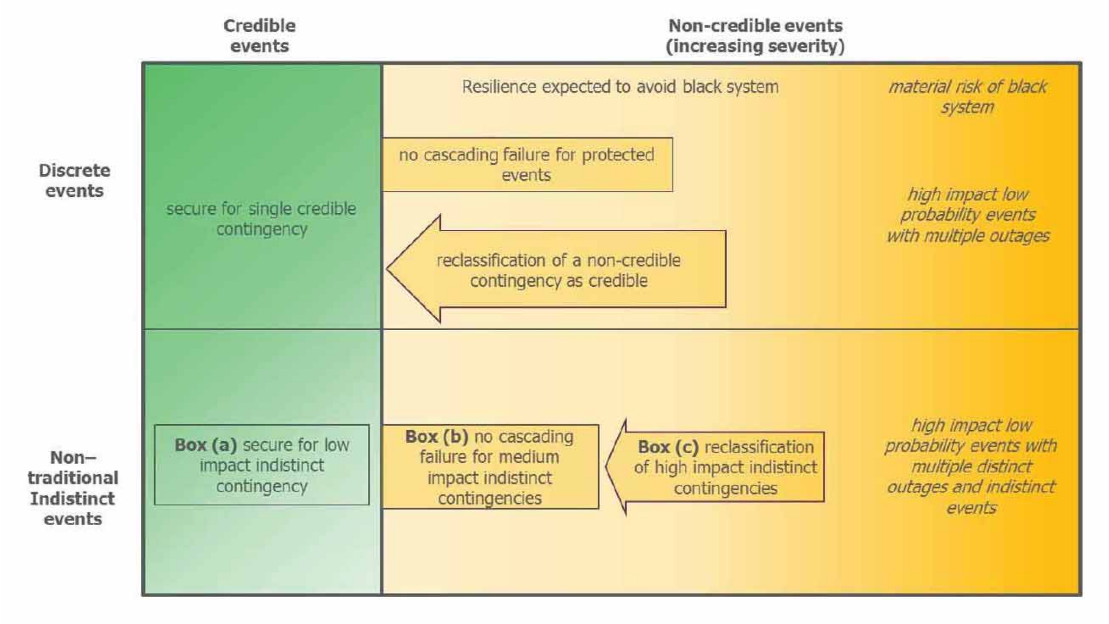
30 It is acknowledged that these kinds of solar ramping events do not yet appear to be posing a significant threat to system security. However, this may change as penetrations of utility scale PV continue to increase.

4.5.2 Evolved protected events framework

This section provides an overview of the protected events framework which has been evolved and expanded to effectively enhance power system resilience to non-credible indistinct events and conditions which are not clearly covered by the existing contingency framework.

Figure 4.3 provides a high level overview of the proposed framework. It takes the general framework presented in section 2.4 and provides additional detail on the mechanisms through which power system resilience will be enhanced. Moving rightwards on the horizontal axis of the figure represents the increasing severity of an event, with the less severe credible contingency events on the left and more severe non- credible contingency events (including indistinct HILP events) on the right.

Figure 4.3: Enhancing system security through a more resilient power system



Source: AEMC

The top left / top right quadrants describe existing arrangements for managing distinct credible and non-credible contingencies, and protected events which do not relate to indistinct events. This framework was designed for discrete contingency events and the review is not considering changes to these arrangements.

Arrangements in the bottom left-hand quadrant, for managing indistinct events which are considered reasonably possible, and therefore credible, were discussed in section 3. The bottom right quadrant (indistinct, non-credible events) represents more severe indistinct events, including indistinct HILP events. As identified above, existing frameworks may not effectively capture these kinds of events and therefore, a new mechanism is proposed to enhance power system resilience in this area.

This mechanism, as depicted in figure 4, includes

- a new category of "**standing**" indistinct protected event (box b) which accounts for indistinct events, the occurrence of which creates a risk of cascading failure, and the likelihood of which does not change according to external conditions, and
- provides for AEMO to declare a period of "**protected operation**", (box c) during which it can take ex- ante actions to limit the risk of cascading failure from an indistinct event. Protected operation accounts for indistinct events, the occurrence of which creates a risk of cascading failure under specific, external conditions, and allows AEMO to take ex-ante action where the presence of those external conditions has caused the likelihood of the event to increase.

Protected operation may also come in two parts being **formal protected operation** and **ad-hoc protected operation**. These two types of protected operation differ in the level of flexibility available to AEMO to take action.

Formal protected operation would involve planned operational actions to manage risks identified through the GPSRR process. Ad-hoc protected operation represents emergency operational measures taken by AEMO to respond to an indistinct risk which was not previously foreseen through the GPRSS process. Ad-hoc protected operation measures are intended to provide AEMO with flexibility to respond to emergency situations only and not as a day to day option for managing non-credible contingency events. Section 4.5.4 will consider the governance arrangements which apply to ad-hoc and formal protected operation declarations.

4.5.3 Operation of the evolved protected events framework

This section describes the operation of the framework for the two types of indistinct protected events being standing events and periods of protected operation.

<u>Standing indistinct protected events:</u>

Box (b) can be defined as "standing" indistinct protected events. These are indistinct, non-credible events that could occur at any time. Expressed another way, these are more severe indistinct events, the probability of which are independent of any specific, external conditions.

For these events, it is desirable that action be taken to prevent a cascading failure, should they occur. Examples of these kinds of standing indistinct protected events could potentially include:

- unpredictable responses of a large portion of the inverter connected fleet to power system conditions
- protection system malfunction and

- cyber attack.[31]

These standing, indistinct protected events would need to be assessed to determine whether the cost of taking action to protect the system does not exceed the expected benefits. Therefore, it would be expected that this type of protected event would follow an approval pathway that is generally similar to the existing protected event framework and be approved by the Reliability Panel following consideration of costs and benefits.

In practice, it is likely such events would be managed through the deployment of some form of asset build, such as a special emergency protection scheme (the SIPS scheme in SA is an example). This is on the basis that as the event could occur at any time, it is unlikely to be economic for it to be managed through the permanent application of constraints to dispatch. However, this is a question that would be subject to assessment by the Reliability Panel, on a case by case basis.

<u>Protected operation:</u>

Box (c) represents indistinct, non-credible events which become more likely only during abnormal conditions (such as severe storms or bushfires), and which carry an associated risk of causing a cascading failure only during these periods. Such conditions may be highly uncertain in their impact on the power system but are more forecastable than events managed by a standing protected event.

Given that the likelihood and consequences of these events only increases under abnormal conditions, it is only necessary to change the operational profile of the system to reduce the risk of cascading failure during the occurrence of those conditions. The recently declared SA protected event for loss of the Heywood interconnector during abnormal conditions (destructive winds) is an example of the type of event that might be classified in Box (c). This is because it is not a standing risk, with the probability and consequence increasing dramatically once wind speeds exceed a given level.

We define actions taken by AEMO to manage forecastable indistinct events as AEMO entering a period of "protected operation".

Under the protected operation framework, AEMO would be required to identify that the indistinct event defined in Box (c) had become more likely to occur due to abnormal conditions, and that there was an increased risk of cascading failure.[32] AEMO would then declare a period of protected operation, and change the operating profile of the system to manage this risk. This process is represented in Figure 4 by the arrow between Box (c) and Box (b).

31 Staff acknowledges that the exact nature of the events that fall into this category are less clear than for other kinds of event, such as weather driven events. However, we consider that the inclusion of this type of contingency allows for as yet unspecified risks to be captured, improving the robustness of the framework for future uncertainty.

32 The project team will give further consideration as to what kind of test might be applied here in regards to the probability of the event and risk of cascading failure. Various options exist: for example, under the traditional reclassification process, AEMO reclassifies where occurrence of the event has become "reasonably possible". However, the declaration of abnormal conditions under the existing NER refers to non-credible contingency events having become "more likely". We will give further consideration as to what level of test is appropriate for this new framework, noting the trade-offs that can exist between certainty and operational flexibility.

During a period of protected operation, AEMO would be able to use ex-ante measures to manage the system, with its primary goal being to reduce the risk of a cascading failure. Importantly, as with the existing distinct protected event, this would mean some load shedding could occur, provided that the system stayed stable and an uncontrolled, cascading outage was prevented.

To achieve this, for the duration of the protected operation period, AEMO could take ex-ante measures, to augment the operation of any associated special emergency protection scheme, including:

- increase the procurement of ancillary services (e.g. FCAS)
- constrain the associated interconnector flow to lower level, to provide headroom
- pre-emptively feather affected wind turbines or constrain the output of large solar systems
- dispatch or direct one or more synchronous generating units to provide additional fault level and inertia.

Staff consider that the period of protected operation would only be allowed to last for as long as the occurrence of the relevant abnormal conditions. This means that AEMO's ability to alter the technical envelope would be constrained by the presence of these conditions. Limiting the duration of protected operation to the period of the abnormal conditions will limit the costs associated with declaring protected operation.

4.5.4 Governance arrangements

Governance arrangements will be important as there is a need to allocate roles and responsibilities in decision-making, provide transparency and accountability in addition to allowing flexibility and timeliness.

AEMO is the party with the information and skills to assess consequences and risks of indistinct events, which is necessary to define and develop appropriate solutions to address the risks of a protected event. However, AEMO is not a party which is well positioned to make economic decisions that are likely to sit more appropriately with other market bodies. For this reason the existing protected event framework allocates responsibility for assessing costs and benefits with the Reliability Panel as the body that approves a protected event application made by AEMO.

The careful assessment of costs and benefits however needs to be balanced against the benefits of allowing AEMO discretion to declare protected operation periods in real time, in response to the rapid emergence of new, unexpected events. Governance arrangements are therefore proposed which include robust cost benefit assessment for actions which involve significant costs while providing flexibility under emergency conditions.

Staff consider that a governance framework for the proposed enhanced indistinct standing protected event / protected operation framework would need to meet certain design principles including:

- have sufficient oversight so that the national electricity objective is advanced

- utilise AEMO's detailed knowledge of the operation of the NEM power system and the emerging risks of cascading failures
- account for the economic trade-offs for what is included in the three boxes, including:
  - the cost of any special protection scheme required to manage the risk of a cascading failure for the events in Box (b)[33]
  - the cost of any special protection scheme required to manage the risk of a cascading failure for the events in Box (c), as well as the cost to the market of the network constraints and additional ancillary services during the period of protected operation.
- provide transparent information to market participants in terms of how events are determined and allocated to each category by AEMO
- be sufficiently flexible so emergency conditions associated with new, unforseen, risks can be managed without unnecessary delay

Practically, we consider that a general governance framework for standing indistinct protected events, and protected operation periods, would follow a general process for approval, described as follows.

Standing indistinct protected events would follow a process equivalent to the existing protected events framework. That is, AEMO would identify the standing indistinct protected event in the GPSRR, with progression either through the RIT-T or Reliability Panel process.

As with existing protected events, this process would be suitable for events that can be planned for and where permanent measures can be put in place to manage the risk of the event

Protected operation periods would need a more flexible, iterative governance framework. This is because one of the key benefits of the framework is that it allows AEMO to adjust to and manage rapidly emerging risks, in an operational time frame. That is, the framework provides AEMO with sufficient operational discretion to do what it needs to do to keep the system secure, if new risks arise. However, noting the potentially material cost impacts associated with these actions taken by AEMO to keep the system secure, clear accountability and transparency requirements are also critical, to help limit cost implications for consumers.

As a general outline, we consider this framework would include the following processes, broadly grouped into ad-hoc and formal protected operation declarations.

Formal protected operation:

- As part of the GPSRR, AEMO would turn its mind to the kinds of abnormal conditions that could give rise to the kinds of events described in Box (c).
- Based on this assessment, AEMO would then publish criteria that set out how and when it intends to declare periods of protected operation, including the nature of the event, the triggering abnormal conditions, and what actions it intends to take to manage the event.

33 As discussed above, we consider it less likely that the costs of permanently changed system operation (such as permanent constraints on dispatch) would be justified for these kinds of standing events, given that they would be permanently invoked. However, the protected events framework would still allow for consideration of the costs of such actions, if proposed by AEMO.

- Parallel to this, AEMO may also consider the identified protected operation period in its assessment of whether there is a need for a general or special EFCS, as part of a separate assessment for a distinct or indistinct protected event. This may then influence the assessment of the benefits of any such scheme.

Ad hoc protected operation:

This process would be followed where AEMO identified a new and severe non-credible, indistinct event, where it was necessary to take action urgently, before completion of the formal protected operation process described above.

- In response to a new and previously unforseen risk, AEMO would have the discretion to declare an "ad-hoc" period of protected operation. This ad-hoc declaration would include notices to market setting out the nature of the event, including the triggering abnormal conditions, and what actions AEMO intended to take to manage the event.
- After the event, AEMO would then be required to feed its learnings back through the GPSR, triggering the formal protected operation process above.

QUESTION 5: ENHANCING THE EXISTING PROTECTED EVENTS FRAMEWORK

The governance arrangements for standing protected events and formal protected operation are equivalent to those currently in place for protected events:

- does this give AEMO sufficient ability manage foreseeable security risks?
- does this provide appropriate oversight from the Panel?
- should additional requirements be included?

The proposed arrangements give AEMO an ad-hoc power to declare a period of protected operation for indistinct events during abnormal conditions:

- does it give AEMO sufficient ability manage unforeseeable security risks?
- what information should to be included in market notices?
- what post event reporting requirements should be placed on AEMO?
- are there sufficient links to the GPSSRR?
- is additional oversight required (e.g. the Panel)?

4.6 Framework for monitoring the interconnector flows against a standard

This section considers measures to gain greater visibility regarding interconnector flows and potential standards to define what these flows should be.

These measures are intended to make the power system more resilient through introducing *smarter* mechanisms, to improve the ability of the system to *avoid* HILP events, and to *learn* from them when they do occur.

Where AEMO identifies that there is a risk that the interconnector flows could be outside the proposed standard, it will need to consider approaches to manage the risk. This could potentially include AEMO considering the issue as part of its GPSR.

4.6.1 Frequency control as an analogy to interconnector flow control

The frequency of the power system is a useful measure of the state of the power system and its resilience to disturbances.

AEMO and participants face various obligations that result in the power system frequency being managed to a value at, or close to, a nominal value of 50 Hz. In addition, the effectiveness of the control of the NEM frequency can be compared to the frequency operating standards, which are determined by the Reliability Panel.[34]

These standards, and monitoring against the standards, provide a transparent benchmark for good operational practice. This provides guidance to AEMO, and certainty to the market, as to how the power system should be operated.

4.6.2 Potential approach to monitoring interconnector flow

In a similar vein to the monitoring of frequency control, monitoring of interconnector flows can provide a measure of the "health of the power system".

<u>Manangement of interconnector flows in the NEM.</u>

At present the interconnector flows are not directly controlled by the AEMO dispatch engine NEMDE but result as the consequence of the loads and generation in the regions. That is, the interconnector flows are the differences between the generation and loads within the regions.

In addition, the NEMDE solution includes security constraints on the interconnector flows. That is, the dispatch process dispatches the scheduled generation and scheduled loads, and in some cases the semi-scheduled generation, within a region such that the interconnector flows are kept within secure limits. This is achieved using constraint equations within the NEMDE solution and is necessary to maintain the NEM power system in a secure operating state.

For the purposes of this section the following definitions have been assumed:

34 Clause 8.8.1(a)(2) of the NER requires the Panel to review and, on the advice of AEMO, determine the power system security standards. The NER glossary definition of the power system security standards includes standards for the frequency of the power system.

- **secure operating limit** - the interconnector limit that AEMO considers is the boundary of the technical envelope, beyond which the system may be in an insecure operating state
- **operating margin** - the margin that AEMO includes within the constraint equation to allow for modelling and measurement errors etc.
- **operating limit** - the limit used within the NEMDE solution to provide confidence that the interconnector flow is within the technical envelope, equal to the secure operating limit less the operating margin
- **dynamic operating limit** - a lower limit used by AEMO to constrain an interconnector flow below its operating limit, when the actual flows are systemically above the operating limit.

<u>Causes of interconnector flows to vary from their dispatch targets</u>

An interconnector flow can differ from the dispatch target determined by NEMDE for a number of reasons, including whenever:

- a scheduled generating unit does not conform with its MW target
- there are errors in the forecast of regional load, non-scheduled or semi-scheduled generation in a region (including wind turbine feathering during high winds and solar ramping due to clouds)
- a generator or load contingency occurs in a region and frequency is controlled using frequency control ancillary services or primary frequency response in another region.

These variations in interconnector flows are generally small and resolved when NEMDE runs in the dispatch interval (i.e. five minutes later). Larger contingencies, such as the tripping of a large generating unit or load, may take several runs of NEMDE to reduce the interconnector flows as various generating units are ramped up or down in response to the contingency.

<u>Consequences of interconnector flows exceeding their secure limit</u>

It is generally not a problem when an interconnector flows does not precisely match its target, However, when an interconnector flow that is exceeding its secure limit means that there is at least one credible contingency event that could, should it occur, cause the flow to exceed its satisfactory limit and trip the interconnector. Thus failing to adequately manage the interconnector can increase the risk of load shedding and/or plant damage that could trigger a cascading failure that could result in a major supply disruption or even a black system event. Of particular concern is when the flow exceeds a stability limit as occurrence of the associated credible contingency event could lead to a region being islanded and a potentially an uncontrolled cascading failure.

This kind of event was highlighted by the AER in its report on the 28 September 2016 black system event. The AER noted that during the period leading up to the black system event itself, rapid variability of wind farm output in South Australia caused flows on the Heywood interconnector to exceed secure limits. For this reason, the AER found that they could not conclusively state that the power system was known to be in a secure operating state during the pre-event period.

<u>Interconnector flow monitoring</u>

Introducing a requirement for the monitoring of interconnector flows would provide a valuable source of information on the performance of the power system. This monitoring would entail public reporting on operational time-scale interconnector flows, and the extent to which secure limits were approached and/or breached. This monitoring could be based on some form of standard for interconnector flows, as discussed in the next section.

Factors that would need to be considered could include:

- whether the operating limit or secure operating limit are being exceeded, i.e. the extent to which the operating margin is being relied on
- the duration when the operating limit and secure operating limit are being exceeded over a period (e.g. a month)

If this monitoring indicates that an interconnector standard was not met, this could trigger AEMO to assess the risk and consider what measures would efficiently and effectively address it, including identifying the root causes of any breaches.

Possible approaches to addressing breaches of the standard could include:

- if only minor breaches of the standard are observed then this could be managed by increasing the safety margins used in the formulation of the interconnector constraint equations, particularly during periods of higher variability of intermittent generation
- where larger system breaches of the standard are observed then the need to develop a form of tie line bias may be considered, where the AGC could use regulating FCAS to reduce the interconnector flow when it exceeds the limit.

<u>Interconnector flow standard</u>

In addition, an option exists for the Reliability Panel, on the advice of AEMO, to develop a standard for interconnector flows that:

- defines what constitutes a breach of the secure interconnector limit, accounting for AEMO's safety margins
- for what period of time a breach can occur, before it is regarded as a material risk
- what proportion of the time in a breach is regarded as a material risk
- which constraint equations are being breached, and the likely consequences if the associated contingency event occurs

The risks associated with interconnector flows not being maintained within their secure limits should be incorporated into the generalised power system risk review, as discussed in part 2.

QUESTION 6: INTERCONNECTOR STANDARD

What are stakeholder views on:

- the value of and rationale for monitoring and reporting on interconnector flows?
- the proposed approach to monitoring and reporting on interconnector flows?
- the proposed role for the Reliability Panel in developing an interconnector flow standard?

ABBREVIATIONS

AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
Commission	See AEMC
MCE	Ministerial Council on Energy
NEL	National Electricity Law
NEO	National electricity objective
NERL	National Energy Retail Law
NERO	National energy retail objective
NGL	National Gas Law
NGO	National gas objective

A CIRCUMSTANCES IN SOUTH AUSTRALIA PRIOR TO THE BLACK SYSTEM

The review is motivated by the circumstances arising from the South Australian black system event. During the pre-black system event period, the AER considered that fast renewable variability due to wind farm feathering in the South Australian region placed power system security at risk. AEMO's lack of operational action to manage these risks exposed uncertainty as to whether fast renewable variability, arising from non-traditional events such as storm fronts, could be categorised as contingency events and managed through system security frameworks.

This section describes the circumstances arising from the South Australian black system event and provides a summary of AEMO and the AER's views on whether wind farm feathering could be considered a contingency event. Staff's initial view as to the applicability of the existing definition of contingency event to wind farm feathering and fast solar ramping is then presented.

A.1 Circumstances during the pre-black system event period

In its compliance report, the AER identified a number of issues related to the operational management of risks to power system security due to high wind speeds in South Australia during the pre-event period on 28 September 2016. These issues included the extent to which the contingency classification framework as set out in the NER could be applied to manage system security risks arising from wind farm feathering. While wind farm feathering did not contribute to the system black event itself, the AER considered that power system security was compromised during the pre-event period due to these events.[35]

On 28 September 2016, and during the days leading up to it, a severe storm was forecast heading towards SA with forecasts of high wind speeds including gusts of up to 140 km/h.[36] The generation mix serving South Australia during the pre-event period was characterized by high wind generation and high interconnector flows into South Australia from Victoria. With 613 MW served by Victoria via the Heywood interconnector, only 330 MW (18%) of South Australian demand was being satisfied by South Australian synchronous generation. Wind generation as a proportion of total SA generation exceeded 50% most of the time.[37]

In the lead up to the black system event, AEMO was operating the South Australian power system with interconnector import limits set to cover the loss of what was considered to be the largest credible contingency within South Australia, being the loss of the 260 MW Lake Bonney wind farm.[38]

However, during the pre-event period, the AER's analysis found that there were several extended periods during which the Heywood interconnector experienced flows significantly

35 AER, The black system event compliance report, p. 14

36 AEMO, Integrated final black system incident report, March 2017, p. 24

37 Ibid, p. 25

38 AER, The black system event compliance report, p. 58

exceeding its import limits. In one case, the import limit exceedence reached 156 MW.[39] This occurred due to rapid reductions in wind farm output in South Australia, which are understood to be least partly due to feathering of multiple distributed wind turbines across the South Australian region (wind speeds at the time significantly exceeded the 90 km/h feathering threshold).[40]

In its compliance report, the AER considered that this situation represented a risk to power system security, as the actual metered flows on the Heywood interconnector were sufficiently high to raise the possibility of separation between South Australia and Victoria, had the 260 MW largest credible contingency been experienced. That is, the feathering of the multiple wind turbines pushed Heywood flows to a point where, had the identified credible contingency (loss of Lake Bonney WF) occurred; there was a real risk of excessive flows tripping the Heywood interconnector.[41]

During the pre-event period, AEMO identified the risk of wind farm feathering to interconnector flows. To manage this risk AEMO took a number of actions including arranging for several network assets to be bought back into service.[42] AEMO however did not adjust the technical envelope to manage the risk of separation between South Australia and Victoria by constraining the interconnector and bringing on additional generation in the South Australian region. Despite identifying these risks, AEMO did not take operational action as they did not consider wind farm feathering to represent a contingency event as defined in the rules.[43]

The concept and definition of a contingency event is directly relevant to the structural issues identified through the AER's assessment of the events of 28 September 2016. This is because the AER found that AEMO did not identify forecast wind feathering events as a contingency event.[44]

This meant that AEMO did not then reclassify the loss of generation (due to feathering across multiple affected wind farms) from non-credible to credible contingency status, which in turn meant it did not take ex-ante action to manage the potential consequences of this event. While the AER did not find AEMO to be non-complaint, it was unable to conclusively find that the South Australian power system was in a secure state during the pre-event period.[45]

39 Ibid
40 Ibid, p. 42
41 AER, The black system event compliance report, p. 52
42 Ibid, p. 61
43 Ibid, p. 61
44 Ibid, p. 32
45 Ibid, p. 60

B COMMISSION AND PANEL DECISIONS ON RELATED FRAMEWORKS

There are two processes which are particularly relevant to arrangements being considered in this work stream. These are:

- Declaration of lack of reserves (LOR) rule change, and
- The amendment of the definition of generating event in the frequency operating standards (FOS).

This section summarises these changes in terms of their elements most relevant to the issues considered in this work stream.

B.1 Declaration of lack of reserve conditions

The declaration of lack of reserve conditions (LOR) rule change changed the process of declaring low reserve levels in the NEM from being a deterministic process, based on the largest contingency, to being a probabilistic approach. This change was made to allow AEMO to account for factors not currently considered when assessing reserve conditions such as forecast error in load and generation. The LOR rule change will allow AEMO to account for a wider range of risks when determining reserve levels in the NEM than currently allowed under the deterministic contingency based approach.

Traditionally, AEMO would declare a LOR2 low reserve condition when reserve levels were smaller than the largest credible contingency in a NEM region. Higher load and generation uncertainty now sees certain periods in parts of the NEM where errors in load and generation forecasts exceed the size of the largest credible contingency. In requesting the rule change, AEMO considered that due to the changing power system, a solely contingency based approach did not reflect the true risk to reserve levels; particularly during periods of extreme weather. AEMO therefore proposed to replace these deterministic criteria with a probabilistic approach that captures the full set of risks given a changing power system.

The Commission elected to make the rule proposed by AEMO with some revisions to enhance transparency. In coming to its view, the Commission agreed that the current framework for declaring low reserve conditions based on credible contingency sizes was no longer fit for purpose.[46] While contingency sizes still affect reserve levels, the Commission considered that they are no longer the only, or main, factor that needs to be accounted for. The Commission considered the proposed rule would better reflect the risk of load shedding, and by extension better reflect the risk faced by the market.

AEMO is trialling a probabilistic approach to declaring low reserve conditions, its forecasting uncertainty measure (FUM). This approach involves characterising the magnitude of forecast error according to applicable conditions. Applicable conditions include forecast lead time, temperature, wind, solar, and other forecast weather conditions. AEMO is training a Baysian belief network with historic data for this purpose. The Baysian belief network produces a

46 AEMC, declaration of lack of reserve conditions – final determination, p. ii

distribution of possible forecast errors which may arise from applicable conditions. LOR levels are then triggered on the basis of the largest of the traditional contingency based approach and forecast uncertainty.

While the LOR rule change involves reliability, it is responding to a situation that is highly analogous to that being considered in this work stream. Specifically, it is addressing the limitation of a traditional contingency based framework to capture the full set of risks present in a changing power system. AEMO's probabilistic approach to managing reserve level declaration, being the FUM measure, may also be applied to characterising fast renewable variation as a function of a wider set of risk factors than simply the set of traditional credible contingencies. A 'FUM type' statistical measure could be used to account for fast renewable variation and complement the traditional contingency approach for maintaining the system in a secure state. Staff understands that AEMO is investigating extending the FUM into security applications. Further discussion of a potential use of the FUM, or a close equivalent, is provided in the section on options for expanding system security frameworks.

B.2 Amendment of the definition of generating event in the frequency operating standards (FOS)

The FOS was reviewed by the Panel in 2017. As part of this review, the Panel amended the definition of generation event to include rapid ramping events. Rapid ramping events were included as a category of generation event alongside, but distinct to, generation events arising from credible contingencies. The definition of generation event was expanded to include the following:

1. "an event that results in the sudden, unexpected and significant, increase or decrease in the generation of one or more generating systems of more than 50MW within a period of 30 seconds or less."[47]

By revising the definition of generation event in the FOS, AEMO is permitted to procure additional fast acting contingency FCAS to manage generation variability alongside regulation FCAS. The approximate response time of the regulating FCAS service is 30 seconds. In its application for a change to the definition of generation event, AEMO proposed a 30 second time threshold as the speed of the events that are sufficiently fast to require management through contingency FCAS.[48]

This change was motivated by the increasing risks to frequency in the NEM associated with rapid solar PV ramping combined with localised cloud cover. In coming to a decision, the Panel understood that historically the definition of generation event had been interpreted as covering the tripping of a generating unit as a result of a credible contingency. However, this

47 Stage 1 of the FOS review, final determination, p. 38

48 Ibid, p. 43

interpretation was insufficient to capture the rapid variation in output from one or more PV generating systems given cloud conditions.[49]

The panel considered whether fast renewable ramping events should be considered as a contingency within the definition contained in the FOS. AEMO initially proposed that rapid changes in output should be considered to be a contingency event and that the FOS should point clearly to the existing NER clauses that describe contingency events and credible contingency events.[50] The Panel however did not elect to link changes to the definition of generation event to the rules definition of credible contingency event. The Panel elected to set out changes to the definition of generation event that clearly define the kinds of events that AEMO should include in its consideration of what constitutes a generation event.[51]

The Panel's amendment to the definition of generation event in the FOS is directly relevant to this review work stream for several key reasons:

- it changed part of the overall framework for system security (being arrangements for the management of frequency and procurement of FCAS) to manage generation variability occurring due to non-traditional events
- it considered whether to define these events as contingency events, and
- it formed a view on the speed and size of events necessary to qualify as a risk to system security.

The amended definition of generation event includes a set of parameters which define the speed and magnitude of events which qualify for management via contingency FCAS. These include a required speed of 30 seconds and a magnitude of at least 50 MW. These thresholds are relevant for the review to consider in characterising the type of variability which is captured by expanded system security frameworks.

The panel also elected to separate out fast renewable ramping 'events' from generation events occurring as a result of credible contingencies. It did this due to uncertainty about the type of events which could be considered to be contingencies and a desire for clarity and transparency as to the type of events that could be considered generation events.[52] The Panel's decision may be relevant for the Commission to consider in deciding whether to augment the existing definition of contingency event to capture fast non-traditional risks due to renewable ramping or whether to define them as system security events separate to the set of traditional contingencies managed by AEMO. This question is considered further in the following section.

49 Ibid
50 Ibid
51 Ibid, p. 44
52 Ibid

C RESILIENCE FRAMEWORKS EXISTING IN SEPTEMBER 2016

This appendix provides an overview of the mechanisms in the NER frameworks that provided a level of resilience in the NEM power system in September 2016. These mechanisms are typical of the modern power system and have generally existed from prior to the commencement of the NEM in 1998. In between the commencement of the NEM and September 2016 a number of changes to these mechanisms have been made.

C.1 A strong power system

The NEM power system has been inherently strong in the past as it contained multiple large synchronous generating units. These units inherently provide the system with satisfactory levels of fault level and inertia to stabilise power system frequency and voltage in the event of most disturbances. However, the changing mix of generation has lead to a reduction in the fault levels and inertia of the system, and this particularly the case in South Australia by September 2016.

In addition to the inherent inertia and fault level provided by the large synchronous generating units, additional ancillary services have been procured. These include:

- frequency control ancillary services (FCAS) for both regulating the frequency during normal operation[53] and to restore the frequency to normal value following credible contingency events[54]
- network support and control ancillary services (NSCS) to provide reactive power support or network loading support

Another important source of strength in the power system are the generator technical performance standards (GTPS). The GTPS specify the performance requirements that connecting generating units and systems are required to be able to met. These standards include:

- the ability to inject or absorb reactive power during a disturbance to assist maintain the voltage within acceptable limits
- the ability to continue to operate following one or more faults on the power system
- the ability to continue to operate when the power system frequency or voltage deviate from their nominal values[55]

Thus the GTPS require the generating units and systems to support the power system during faults and disturbances, thus providing a level of resilience to non-credible contingency events. This resilience means that a material risk of a cascading failure or black system is

53 Regulation services are procured by AEMO and are currently used by the automatic generation control (AGC) to manage frequency variations within the normal operating frequency band (NOFB), which is set to 49.85Hz to 50.15Hz.

54 Contingency services are procured by AEMO to return the frequency back to the NOFB following a single credible contingency event such as the tripping of a large generating unit or system, a large load tripping or the loss of a major transmission element.

55 The performance requirements on generating systems match the frequency operating standards (FOS) and the voltage standards in the NER.

expected to be limited to the most severe contingency events. In addition, the NER requires that the generators have compliance programs to ensure that the performance of their generating units is maintained at the levels negotiated at the time of connection.

The reliance of the power system, and hence its ability to withstand severe non-credible contingency events, will be improved by limiting the flows on major transmission lines, such as interconnectors. This is because contingency events generally increase the flows on such lines, potentially resulting in overloading or a loss of synchronism between regions. AEMO is required to keep the flows on the major transmission lines within secure limits, that is, the flows are limited so that a credible contingency event would not result in a cascading failure of the power system.

In the event that a very severe event occurs then there is a risk of a cascading failure that results in a major supply disruption or black system event. Following a cascading failure it will be necessary to restore supply to affected customers, and this would including restarting the power system following a black system event. Therefore, AEMO procures system restart ancillary services (SRAS) that can, in the event of a black system, assist in the restarting of the large generating units in the affected area.

C.2 A smarter power system

A smarter power system can be achieved through a broad set of actions that can improve the observability, controllability, and operational flexibility of the power system in responding to extreme events.

Ensuring that the state of the power system is known can reduce the risk of a cascading failure. This is achieved using the NEM SCADA systems to monitor the current state of the system, as well as by forecasting the expected demand and the output of the intermittent solar and wind generation. This allows AEMO to maintain sufficient services in the system and secure limits on interconnector flows to be in secure operating state, as well as providing a level of resilience to more severe non-credible contingency events.

A smarter power system is also more able to survive a severe contingency event through the protection systems on the power system plant, as well as special protection schemes. Protection systems detect the presence of a fault within the power system and disconnect the affected plant to limit damage and for safety, as well as to limit the risk of a cascading failure to the remainder of the system. Protection systems need to discriminate the location of the fault to minimise the amount of plant to disconnect, and to operate sufficiently quickly to limit damage to the affected equipment and to reduce the risk of a cascading failure propagating throughout the power system.

Each region of the NEM also includes an under frequency load shedding scheme (UFLSS). The operation of the UFLSS aims to arrest a sudden drop in frequency by progressively reducing the load in predefined blocks if the frequency drops below the lower limit of the operational frequency tolerance band (OFTB).[56] Thus the UFLSS is only expected to operate

56 The operational frequency tolerance band is specified in the frequency operating standards. The lower limit of the OFTB is 49Hz on the mainland and 48Hz in Tasmania.

under emergency conditions following the non-credible tripping of multiple generating units or the non-credible islanding of a region, but will reduce the risk of the frequency reaching the lower limit of the extreme frequency excursion tolerance limit (EFETL)[57] where most generating units will trip, resulting in a black system event.[58]

In addition to protecting individual items of plant and UFLS, the NEM also includes a number of special protection schemes (SPS). The SPS are dedicated to managing specific risk to the security of the power

system and are generally designed prevent a cascading failure that could lead to a major supply disruption or black system event.

Power system resilience is also enhanced using appropriate models of the operation of the power system. Thus the NER requires generators to provide AEMO and the NSPs with accurate models of their generating units and systems. This allows AEMO and the NSP to assess the expected impact of contingency events, thus ensuring whether the power system is in a secure operating state, as well as assessing the effectiveness of the NEM protection systems, UFLSS and SPS. In addition, the detailed models can be used by AEMO to assess the effectiveness of the procured SRAS so that effective system restart plans can be developed.

C.3 A more interconnected power system

The level of interconnection of the power system is generally determined to provide reliable supply to the customers in each region and to increase the market benefits by allowing trade between the regions. Potential additional interconnection has been assessed by AEMO through the ESOO and the NTNDP (recently replaced by the Integrated System Plan (ISP).

In addition to increasing the benefits of inter-regional trade and improved reliability of the power system in each region, interconnection also provides a number of resilience benefits including:

- providing a greater redundancy within the network, increasing the ability to survive severe contingency events
- the ability to restart a part of the power system following a black system event.

57 The extreme frequency excursion tolerance limits are specified in the frequency operating standards. The lower limit of the EFETL is 47Hz, both on the mainland and in Tasmania.

58 Schedule S5.2.5.3 of the NER requires that generating units be capable of operating within the EFETL. Outside the EFETL the generating units generally trip to prevent them being damaged.

D RESILIENCE WORK COMPLETED SINCE SEPTEMBER 2016

The Commission has made a number of relevant rule changes since the SA black system event in 2016. Both the Commission and AEMO's work programs have been undertaken in the context of recommendations made by Chief Scientist Alan Finkel in the Independent Review into the Future Security of the National Electricity Market (the Finkel Review).[59] This section introduces relevant work that has been completed since the SA black system event, divided into changes which make the power system stronger, smarter, and more interconnected.

D.1 A stronger power system

Synchronous generators provide a set of inherent system services associated with the inertia and fault current produced by the rotating masses of synchronous generator turbines. Inertia and fault level act to stabilise power system frequency and voltage in the event of a disturbance event. As system strength and inertia have declined in parts of the NEM such as South Australia, the power system in these areas will experience voltage and frequency disturbances that are deeper, more widespread and longer lasting, undermining the stability, security, and resilience of the power system.

Historically, these critical system services were inherently provided as a bi-product of synchronous generation. They were in plentiful supply as the power system was dominated by synchronous generating systems. However, a changing generating mix is seeing these inherent services decline as aysnchronous, inverter connected, generation (such as wind and solar PV) do not provide inertia or system strength at comparable levels. The South Australian region is a case in point. The black system event exposed a set of vulnerabilities which had emerged in South Australia due to low fault levels and very low levels of synchronous inertia due to the retirement of synchronous generating systems.

The Commission's system security work program has taken a first step towards defining the 'missing services' identified due to declining levels of synchronous generation in the power system. Relevant rule changes include the:

- Managing fault levels rule - specified a process and allocated roles and responsibilities for maintaining power system fault currents above the minimum level required for system security[60]
- Managing the rate of change of power system frequency rule - provided a mechanism and specified roles and responsibilities for maintaining inertia at sufficient levels to prevent rates of change of frequency exceeding critical levels following a contingency.[61]

59 Commonwealth of Australia, Independent Review into the Future Security of the National Electricity Market - Blueprint for the Future, June 2017.

60 AEMC, National Electricity Amendment (Managing power system fault levels) Rule 2017.

61 National Electricity Amendment (Managing the rate of change of power system frequency) Rule 2017.

The other element of a stronger power system is its ability to withstand disturbances without causing a cascading generator outage. Following the South Australian black system event, the Commission has enhanced requirements for generating systems to maintain continuous uninterrupted operation given multiple disturbances. Relevant rule changes include:

- the Generator technical performance standards rule - amended technical requirements for connecting generators to require higher capabilities to maintain continuous uninterruptedoperation given multiple disturbances as well as providing critical power system voltage support during disturbance conditions.[62]

D.2 A smarter power system

A smarter grid can involve a broad set of actions that can improve the observability, controllability, and operational flexibility of the power system in responding to extreme events. Following the South Australian black system event, which involved the failure of the existing emergency under frequency load shedding system, the Commission made a rule change which included an enhanced regime for planning for and managing high impact non-credible events. The Emergency frequency control schemes rule includes arrangements for the implementation of special protection schemes which pre-emptively shed load on observation of a high impact event. Relevant rule changes include the:

- Emergency frequency control scheme rule - implemented a framework to regularly review current and emerging power system frequency risks, an enhanced process to develop emergency frequency control schemes, and implemented a new classification of contingency event, the protected event, giving AEMO new tools to manage non-credible contingencies.[63]
- Generating system model guidelines rule - clarified the scope and level of detail of model data that registered participants and connection applicants are required to submit to the Australian Energy Market Operator (AEMO) and network service providers. The Generating system model guidelines rule enhances AEMO's ability to accurately model power system behaviour under low system strength conditions as apply in South Australia.[64]
- Review of the frequency operating standard - stage one determination - revised of the definition of 'generation event' to include the sudden, unexpected and significant change in output from one or more generating systems of 50MW or more within a 30- second period. This revision is being made it clear that AEMO is able to use contingency FCAS to manage sudden variations of generation output from the increasing quantity of larger variable renewable generation power stations.[65]

62 National Electricity Amendment (Generator Technical Performance Standards) rule 2018.
63 National Electricity Amendment (Emergency frequency control schemes) Rule 2017.
64 National Electricity Amendment (Generating System Model Guidelines) Rule 2017.
65 Reliability Panel, Stage one draft determination, review of the frequency operating standard, 12 September 2017, p. ii.

D.3 A more interconnected power system

AEMO, in its Integrated System Plan, has identified a need for additional interconnection between South Australia and NSW. The security and resilience of South Australia's power system is challenged by its reliance on the Heywood interconnector, following the retirement of Northern Power Station.[66] The ability to securely operate the power system in SA relies on the transmission network connecting South Australia to Victoria remaining in service and uninterrupted. Risks associated with this reliance on the Heywood interconnector are most acute when there are high flows from Victoria to South Australia, as was the case during the pre-event period on 28 September 2016. The Commission has made a rule change which will speed up the regulatory processes associated with the development of this additional interconnector.

- Early implementation of Integrated System Plan priority projects – the Commission is currently considering a proposed rule change to streamline regulatory processes for three projects (including an additional interconnector between South Australia and New South Wales 'Project EnergyConnect') which have been identified by AEMO as priority projects in its inaugural Integrated System Plan (ISP).[67]

66 AEMO, Power System Frequency Risk Review Report, September 2017.

67 AEMC, early implementation of ISP priority projects rule change, consultation paper, 24 January 2019.

E AEMO'S POWER SYSTEM FREQUENCY RISK REVIEW

E.1 What is a PSFRR?

In March 2017, the Australian Energy Market Commission (AEMC) made a final rule, National Electricity Amendment (Emergency frequency control schemes), to enhance the frameworks for emergency frequency control in the National Electricity Market (NEM).

The final rule placed a clear obligation on AEMO to undertake, in collaboration with Transmission Network Service Providers (TNSPs), an integrated, periodic review of power system frequency risks associated with non-credible contingency events. Conducted at least once every two years, the PSFRR must review non-credible contingency events that could involve uncontrolled increases or decreases in frequency leading to cascading outages or major supply disruptions. The Power System Frequency Risk Review (PSFRR) has two main purposes. It seeks to reveal to the market:

- whether, in order to limit the consequences of some non-credible contingency events, there is a need to introduce, modify or adapt automatic schemes to shed load or generation, or
- whether it would be economic for AEMO to operate the power system in a way that limits the consequences of certain high consequence non-credible contingency events, should they occur.

The PSFRR outlines a different process for AEMO to follow for each purpose. For the former, once a need to introduce, modify or adapt such an emergency frequency control scheme is identified through the PSFRR:

- the assessment, design, implementation and monitoring of the scheme will largely proceed through the existing framework for NSP planning in the National Electricity Rules (NER)
- the Regulatory Investment Test for Transmission (RIT-T) or Distribution (RIT-D) will be used to assess the economic case for the change

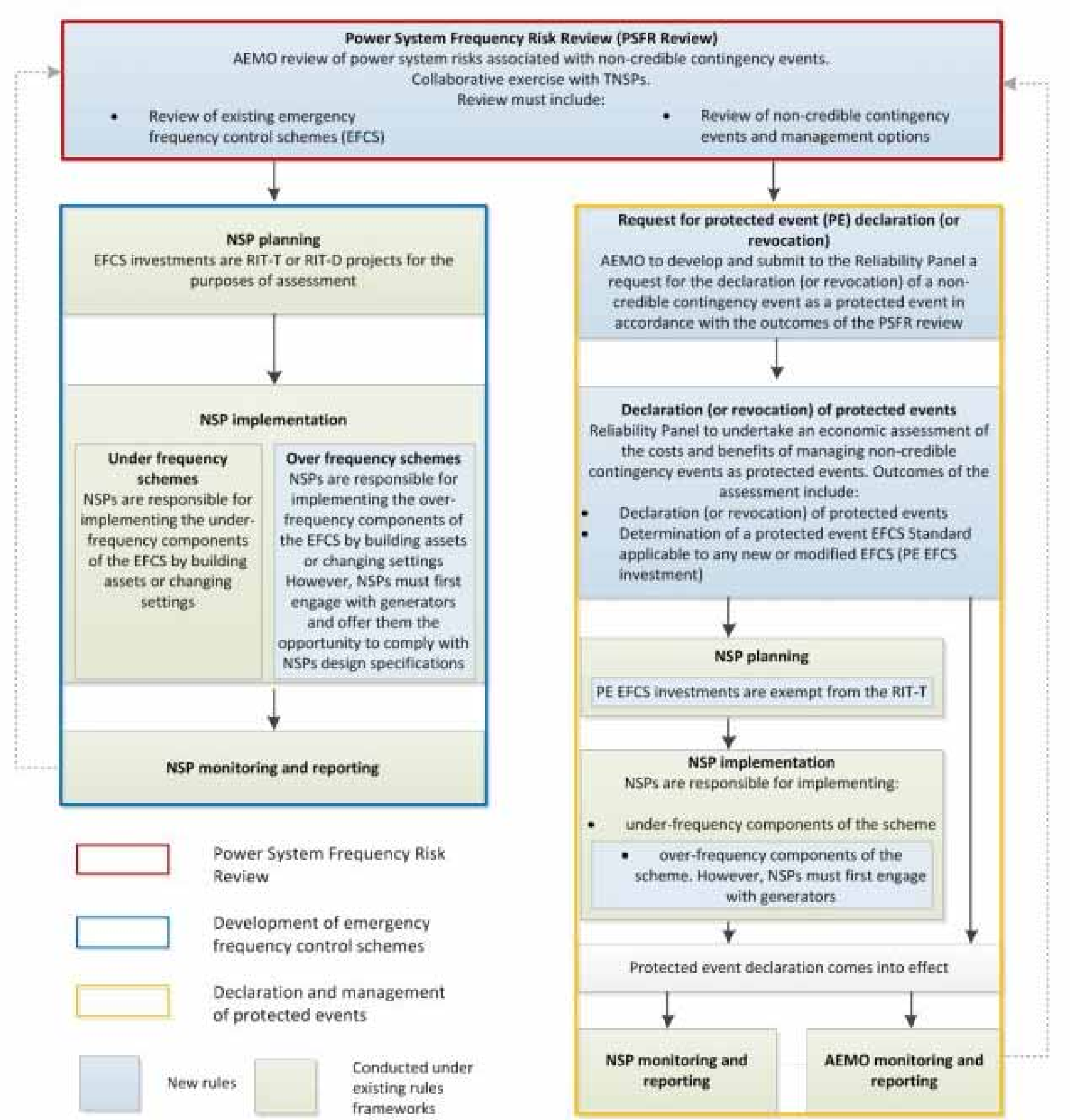
For the latter purpose, whether it would be economic for AEMO to change its operation of the power system, if AEMO identifies through the PSFRR one or more non-credible contingency events which it considers it may be economically efficient to manage using existing ex-ante operational measures:

- AEMO would submit a request to the Reliability Panel to have the event declared to be a "protected event"
- Such ex-ante measures may be intended to be used to manage an event either alone or in combination with a new or modified emergency frequency control scheme
- The Reliability Panel would undertake an economic assessment of the request by weighing the costs of the options for managing the event against the avoided cost of the consequences of the non-credible contingency event should it occur and not be managed. Where the benefits of managing the event outweigh the costs of doing so, the Reliability Panel would declare the event a protected event

- Where the efficient management option includes a new or modified emergency frequency control scheme, the Reliability Panel would set a "protected event EFCS standard", which is a set of target capabilities for the scheme.

Importantly, the second process notes that NSPs would be exempt from having to undertake the RIT-T or RIT-D where this would otherwise have been applicable. This is because the Reliability Panel would have already undertaken a cost benefit analysis of the option recommended by AEMO in the PSFRR. This process is detailed graphically in figure 1.

Figure E.1: Process flow of the Power System Frequency Risk Review



Source: AEMC

In clause 5.20A.1,[68] the NER set out obligations that AEMO are required to complete when conducting and submitting a PSFRR. Along with identifying current power system arrangements and the likelihood and likely outcomes of non-credible, high consequence frequency contingencies, AEMO is required to review options for managing these events in the future, their technical and economic feasibility, and the most appropriate range of options to do so, which may include:

1. new or modified emergency frequency control schemes
2. declaration of the event as a protected event
3. network augmentation
4. non-network alternatives to augmentation

E.2 Why was the PSFRR introduced?

The National Electricity Amendment (Emergency frequency control schemes) made in March 2017 noted the NEM is experiencing a significant shift away from conventional generators towards new technologies. Managing the different technical characteristics of these technologies is having major impacts on power system security, and complicated the way AEMO, obliged to maintain and improve system security, could manage changing risks considered reasonably possible. Before the rule change:[69]

- For credible contingency events considered reasonably possible, AEMO manages power system frequency to stay within defined limits by buying ancillary services and constraining the power system
- For non-credible contingency events, Under Frequency Load Shedding schemes shed load to arrest a fall in frequency, caused, for example, by a loss of multiple generators
- AEMO could reclassify a non-credible event as credible, if abnormal conditions make the event reasonably possible.

The rule change identified key trends that made these arrangements insufficient, and that made it necessary to introduce new frameworks to deal with changing risks arising from a transitioning power system:

- Schemes historically installed by NSPs designed to quickly respond to changes in frequency when sudden disturbances cause supply imbalances were becoming ineffective, as frequency can change much faster with a different generation mix
- The NER lacked an integrated, transparent framework for the consideration and management of power system frequency risks arising from non-credible contingency events.

In countering these trends, the final rule introduced arrangements that would allow AEMO, the Reliability Panel and market participants to better manage new risks, because:

68 Power System Frequency Risk Review, AEMO, 2018, p. 1
69 AEMC 2017, Emergency frequency control schemes, Rule Determination, 30 March 2017, Sydney p.ii

- Including an economic assessment framework that allows for the severity of the consequences of certain non-credible contingency events to be balanced against the price outcomes associated with managing the event
- the introduction of a clear and transparent framework around the development of emergency frequency control schemes will enable new technologies and solutions to provide more effective emergency frequency control schemes to be identified and considered
- the introduction of a contingency event classification for protected events will allow for more efficient operation of the power system, providing both security and reliability benefits for consumers
- the rule clarified and enhances the arrangements for load shedding schemes used to manage under-frequency events and, for the first time, establishes in the rules a governance framework for the implementation of schemes to shed generation to manage over-frequency events.[70]

70 AEMC 2017, Emergency frequency control schemes, Rule Determination, 30 March 2017, Sydney p.iii

F BENEFITS OF THE GENERALISED POWER SYSTEM RISK REVIEW

F.1 Time to translate identified risks into a protected event

Staff consider that reforms to the PFSRR process, and subsequent protected event declaration, could help speed the process of delivering solutions to address emerging system risks. This section steps through some of these proposed solutions. Discussion of the proposed protected operation framework, and related governance framework changes, are discussed in part 3.

Through the PSFRR, AEMO can recommend the declaration of a protected event, if AEMO considers it economic to operate the power system in a way that limits the consequences of certain high impact non-credible contingency events. Staff have determined the current process for identification, declaration and management of a protected event is transparent and systematic, but also prone to potentially unnecessary delays that detract from AEMO's ability to respond flexibly to power system security risks in a way that may be more optimal.

Staff have identified potentially unnecessary delays existing in the current process both prior to, and after, AEMO recommends the Panel consider declaring a protected event. In particular, the team considers that processes could be sped up for:

- AEMO to undertake the PSFRR process to identify a system need
- the translation of this need into an application to the Reliability Panel for declaration of a protected event, and
- the Reliability Panel to assess AEMO's application and declare a protected event.

AEMO is currently required by the NER to conduct a PSFRR at least every two years.[71]

Over a two stage draft-final process, AEMO must hold full consultations with TNSPs to assess system risks and, in the event of recommending new or modifications to existing emergency frequency control schemes, full consultations with affected DNSPs also. Following publishing a draft review, AEMO must invite written submissions from stakeholders on its report, only after which they can submit recommendations to the Reliability Panel for new or modified EFCSs, or the declaration of a protected event.

This ex-ante process provides a transparent and systematic framework to identify anticipated power system security risks well in advance of their occurrence. However, the process also makes delivery of the solutions to address these identified risks contingent on completion of a lengthy review process. Staff consider changes included in a GPSRR could help alleviate these concerns.

After completion of its review process, AEMO can submit a request to the Reliability Panel for an event to be declared a protected event, if it considers it economically efficient to manage one or more non-

71 See clause 5.20A.2 of the NER.

credible contingency events using existing ex-ante operational procedures.[72] The criteria required to justify declaration of a 'protected event' are detailed further in Appendix D.

Currently, the Reliability Panel is required to follow a process that requires:[73]

1. publication of a consultation paper in relation to AEMO's request for a protected event declaration. Stakeholder submissions are requested and considered
2. publication of a draft determination outlining how the Reliability Panel proposes the event be managed. Stakeholder submissions are requested and considered
3. publication of a final determination.

Although comprehensive, stakeholders have argued that the existing process is overly lengthy. Given the pace of change in the power system, and the speed at which new risks can emerge, this may result in inefficient outcomes and create risks to the secure operation of the power system.

Staff therefore recommends this process be streamlined to support faster identification of risks, and development of solutions to identify those risks. However, in doing so, we consider that processes for evaluating costs and economic impacts be preserved, and that appropriate parties remain accountable.

Various options exist for streamlining the Reliability Panel's protected events declaration process. This could include introducing a mechanism similar to the NEL expedited rule change process, to reduce consultation to one stage after publication of a consultation paper, after which the Reliability Panel would proceed to publish a Final Determination. Such an approach may be appropriate where AEMO has proposed a low cost protected event, where a majority of stakeholders are likely to be supportive of the proposed change. However, an option could be included to defer to a full process, if either the Panel or stakeholders consider more thorough analysis is required.

Staff will explore these potential mechanisms and set out more detail in subsequent papers.

F.2 Better coordination of system risks and services

Staff considers any framework that seeks to describe system security arrangements should account for the full range of risks to power system security. The PSFRR specifically considers frequency risks. However, this may not capture all possible risks associated with non-credible contingency events in the NEM.

The NER outlines, and AEMO operationalises, system security services that respond to meet the system needs of the NEM to survive and recover from different types of disturbances. These may be grouped into three broad categories of frequency management, voltage management and system restoration.[74] AEMO is also required to consider the minimum

72 AEMC 2017, Emergency frequency control schemes, Rule Determination, 30 March 2017, p. ii

73 Reliability Panel, AEMO request for protected event declaration, Final report, 20 June 2019

74 Power System Requirements Reference Paper, AEMO, 15 March 2018, p. 9

inertia[75] and minimum fault level[76] requirements of the power system, and declare shortfalls where these are identified.

While the system needs outlined above are detailed separately, individual system services are frequently capable of addressing more than one system need. There are overlaps and interplays between the benefits system services may provide for system security, while a deficiency in one system service may lead to issues in several system need categories. A coordinated assessment of all system security risks, through the GPSRR, could therefore assist in a more efficient deployment of system services to address system needs.

There are existing system services employed by AEMO that, if coordinated and integrated into and GPSRR and broader system planning, can provide a more comprehensive understanding of changing system security requirements, and an efficient pathway to managing the risks these changes present. These existing frameworks and processes include:

- AEMO's power system frequency risk review, required under Clause 5.20A.1 of the NER
- System strength impact assessment guidelines under clause 4.6.6 of the NER, which, among other obligations, requires AEMO to develop a system strength requirements methodology from which it can determine the minimum required fault levels at locations in the transmission network
- Clause 4.4.5 of the NER that provides instructions for AEMO to enable system strength services to maintain the minimum three phase fault level when the fault level at a fault level node is below the minimum standard
- Clause 5.20B of the NER, which among other obligations, requires AEMO to determine inertia requirements for inertia sub-networks and remediate inertia shortfalls, and requires inertia Service Providers to make inertia services available
- Clause 4.4.4 of the NER that provides instructions for AEMO to enable inertia network services to provide inertia to an inertia sub-network at the minimum threshold level of inertia.

These various processes could potentially be included in a GPSR process, with a requirement for AEMO to consider interactions and overlaps between each. Staff will provide further advice as to what this consolidated process may look like in subsequent papers.

F.3 Consideration of risks associated with distributed energy resources

AEMO has identified that high DER penetration, in particular small rooftop PV, may have increasing implications for the secure operation of the system. These include:

- evidence that significant proportions of DER can disconnect or cease operating during power system disturbances (up to 40%), which in the future could translate into the sudden loss of hundreds of megawatts in regions like Queensland, Victoria of New South Wales[77]

75 Clause 5.20B.2 of the NER.

76 Clause 4.4.5 of the NER

77 Ibid.

- under much smaller, localised distribution network voltage and frequency events, between 8-20% of monitored DER was observed to reduced generation to zero over unpredictable periods[78]
- observed behaviour of DER under disturbed system security conditions indicate small percentage of rooftop PV fails to comply with existing standards, posing risks to system security predictability.[79]

observed behaviour of DER under disturbed system security conditions indicate small percentage of rooftop PV fails to comply with existing standards, posing risks to system security predictability.[80] This means that potential system security risks presented by changing DER patterns may not be captured in a single, transparent, integrated review.

The policy team recommends that AEMO collaborate with both TNSPs and DNSPs in developing the GPSR, to evaluate risks arising from uncertain and indistinct non-credible contingency events. In particular, this would include a requirement for consideration of risks related to increased DER, both in terms of how DER might exacerbate events that have occurred on the transmission system, and whether increased DER could itself potentially trigger events on the transmission system. This would provide better visibility of the performance of DER during indisinct contingency events. Further, given that as part of the PSFRR AEMO is already required to consider effective functioning of under-frequency load shedding schemes and over frequency generator shedding schemes, including consideration of DER in the GPSRR would better inform AEMO's understand the effectiveness of these emergency response mechanisms.

78 Ibid.

79 Ibid. p.5

80 See clause 5.20A.2 of the NER.