The Electricity Journal 33 (2020) 106833

Contents lists available at ScienceDirect

The Electricity Journal

journal homepage: www.elsevier.com/locate/tej

Electricity system resilience in a world of increased climate change and cybersecurity risk

Elizabeth L. Ratnam[a,*,1], Kenneth G.H. Baldwin[a,2], Pierluigi Mancarella[b,3], Mark Howden[a,4], Lesley Seebeck[a,5]

[a] The Australian National University, Canberra, ACT, 2600, Australia
[b] The University of Melbourne, Victoria, 3010, Australia

ARTICLE INFO

Keywords:
Electricity
Resilience
Climate change
Cybersecurity
Distributed energy resources
Renewable energy

ABSTRACT

The shift to widely distributed forms of energy generation and storage, requiring increased interconnectivity to geographically balance supply with distributed demand for electricity, creates a more complex electrical network – the 'Internet of Energy'. A growing array of threats now impact the resilience of the electrical network including digitalisation, cybersecurity, technological changes of the power system, and the potential for climate change to expose the system to more extreme weather events. Whether distributed and renewable electricity systems will be more resilient through multiple pathways and redundancy, or less resilient due to greater cybersecurity risks than a conventional centralised electricity system, is the key focus of this paper.

1. Introduction

On the 18 November 2019, with a backdrop of smoke from the Australian bushfire crisis, both research and industry leaders from around the globe gathered in Australia to discuss the future of electricity markets, including key challenges for future grids and potential solutions. With a focus on the energy transition from mostly large centralised generators to cost-effective renewable and distributed energy technologies, discussions spanned equitable solutions, policy needs, and the underlying physics of the grid (MacGill and Esplin, 2020; Brear et al., 2020; Leslie et al., 2020; Blackhall et al., 2020; Skinner et al., 2020; Nelson, 2020; Dodd et al., 2020). Here we focus on the planetary topic of resilience, identifying emerging considerations and opportunities for future power grid design and operation.

Australia is at the vanguard of the energy transition with increasing adoption of Distributed Energy Resources (DER) such as rooftop solar, small-scale energy storage, demand control mechanisms and electric vehicles (Blackhall et al., 2020; Bloomberg New Energy Finance New Energy Outlook, 2020). Residential energy customers are leading the way with a recent rapid uptake in rooftop solar and battery storage. As we accelerate towards the DER energy transition, the opportunity arises to replace the small set of existing coal-powered generators (many of which are approaching retirement (AEMO, Draft, 2020)), with potentially millions of internet-connected DER resources. If Australia can successfully navigate the energy transition with challenges and opportunities including (1) a carbon-intensive electricity sector, (2) the world's fastest wind and solar adoption rates, (3) the longest and skinniest national grid, (4) no support from neighbouring countries, and (5) the potential for electricity exports that would dwarf the National Electricity Market (NEM) (MacGill and Esplin, 2020), then perhaps others can too. However, the more complicated cyber-physical power system must be resilient to a world of increased cybersecurity risk and climate change.

The range and frequency of threats impacting the resilience of

* Corresponding author.
E-mail addresses: elizabeth.ratnam@anu.edu.au (E.L. Ratnam), kenneth.baldwin@anu.edu.au (K.G.H. Baldwin), pierluigi.mancarella@unimelb.edu.au (P. Mancarella), mark.howden@anu.edu.au (M. Howden), lesley.seebeck@anu.edu.au (L. Seebeck).
[1] Future Engineering Research Leader, Research School of Electrical, Energy and Materials Engineering, College of Engineering and Computer Science, Brian Anderson Building, 115 North Road, Australian National University, Canberra ACT 2600.
[2] Director, Energy Change Institute, Australian National University, Canberra ACT 2600.
[3] Chair Professor of Electrical Power Systems, veski Innovation Fellow, Department of Electrical and Electronic Engineering, Parkville Campus, The University of Melbourne, Victoria 3010 Australia.
[4] Director, Climate Change Institute, Australian National University, Canberra ACT 2600.
[5] CEO, Cyber Institute, Australian National University, Canberra ACT 2600.

https://doi.org/10.1016/j.tej.2020.106833

Available online 28 September 2020

electrical power networks are growing. We consider a few important examples of widespread and sustained power outages, with the respective outage duration spanning hours to days.

- The North American power grid blackout of 2003 affected 50 million people across the USA and Canada, leaving some customers without power for two days, with an estimated cost of $6 billion to the economy (Minkel, 2020).
- In December 2015, a synchronised and coordinated cyberattack compromised three Ukrainian regional electric power distribution companies, resulting in power outages affecting 225, 000 customers for several hours (Liang et al., 2017).
- On 28 September 2016, a tornado-like wind-storm triggered a cascading power outage that impacted 850, 000 customers across South Australia (SA). Power to the impacted customers in SA was gradually restored in the hours that followed, however, some customers were left without supply until 11 October 2016 (13 days later) (AEMC, 2019; AEMO, 2020).
- Across the month of October in 2019, California's largest utility company PG&E cut off power to approximately 2 million people in an attempt to avoid sparking wildfires (MacMilliam et al., 2020).
- The 2019/2020 Australian bushfire crisis cut-off power transmission corridors and isolated communities— the electricity supply to 30,000 customers in a regional community alone was cut on consecutive days (Toscano, 2020).

Each power outage significantly impacted communities, businesses, the economy, and in the case of Ukraine, deliberately destabilised the affected region.

As a consequence of climate change, low probability grid blackouts are expected to become more frequent as reported in the power systems literature (AEMC, 2019; Panteli and Mancarella, 2017, 2015a). However, the rise of DER presents opportunities to reduce power outages and their duration with distributed generation supporting microgrid operation (Habib et al., 2016; Lasseter, 2011; von Meier et al., 2020). Specifically, DER unlocks the ability to operate segments of the distribution grid as a microgrid (von Meier et al., 2020; von Meier et al., 2017; Sankur et al., 2018), improving resilience during contingency events and accelerating grid restoration during black-sky events (i.e. a widespread power outage sustained over several hours or days). Future DER operated grids are potentially less vulnerable to cyber threats at the transmission level, however, make way for a vast number of new entry points (e.g., rooftop solar inverters) which are often beyond the utilities reach.

In this paper, we consider electricity system resilience in a world of increased climate change and cybersecurity risk, exploring if it will be more resilient through multiple pathways and redundancy, or less resilient due to greater complexity than a conventional centralised electricity system. In Section 2, we discuss climate change-induced extreme weather events and the impact on the resilience of the future grid. In Section 3 we focus on ways to improve resilience with power system planning, design and operation. In Section 4 we provide an overview of credible cyber threats and attacks, and we include a discussion on how to remove a single point of failure. A discussion on Future Grids: Key Challenges and Opportunities concludes the paper.

2. Climate change

The modal temperature of the earth has increased by 1 degree Celsius, temperature ranges have effectively doubled over the past 120 years (IPCC, 2014), and the increasing scale of climate impacts are bringing urgency to addressing the resilience of future grid operation and design. Since 1980, the frequency of storms with winds stronger than 250 km has more than tripled. Heat stress days—where the temperature exceeds a threshold that causes impacts to both wildlife and humans—are becoming more frequent. In scenarios with a modal temperature increase of 3 degrees Celsius, in the top-end of Australia, it is expected that every day will be a heat-stress day. Warmer temperatures, dry summers, and below-average winter precipitation have spurred more frequent and extensive wildfires across the globe (LeRoy, 2016). Clearly, future grid design must ensure resilience to more frequent extreme weather events, spurred by a more dangerous climate in which we must consider paths for adaptation (Fazey et al., 2018; van Oldenborgh et al., 2020). Importantly, to adapt well to a more dangerous climate, we must be creative in building new resilience equipment, measures, and with our planning processes, rather than upgrading legacy techniques (Colvin et al., 2020; Fleming and Howden, 2016).

Climate change increases the range and the level of risks we must respond to in order to support critical services that rely on electrical infrastructure, including hospitals, water infrastructure, communication networks and the finance sector. The increasing disruption from wildfires, storms and hail, is correlated and related to climate change resulting in increased and non-stochastic co-occurrence of events. As the temperature rises, the availability of water becomes more scarce as water runoff that fills creeks and dams evaporates, elevating the risk of wildfires. Today, the important Murray Darling river system in Australia has one-third less water, with projections for Western Australia indicating it will have 25 % less water availability per degree Celsius of warming. With increased water evaporation, the ground is dryer elevating the risk of wildfires that can create their own electrical storms. The Australian 2019/2020 bushfire crisis is a case in point, driven by drought conditions, and world-record heat, the intense wildfires were further exacerbated by low atmospheric moisture conditions and self-generated electrical storms.

Increasing the complexity of the power system, by expanding the electrical infrastructure (e.g. installing additional poles and wires) helps, but does not eliminate the resilience risk associated with an increase in heat-stress days. For hydro-electric power plants, water scarcity resulting from an increase in heat-stress days will limit their ability to serve increases in electricity demand. Specifically, with lower rainfall and increased evaporation, there will be lower inflows into dams, and at the same time, there will be an increase in electricity demand arising from an increase in heat-stress days. Another increased resilience risk was observed during the Australian wildfire crisis, where power transmission corridors were cut, fragmenting the electrical grid, leading to power outages across the south-east coast of Australia and a call to reduce power use to essential devices. Numerous communities were isolated, with the electricity supply cut for prolonged periods as the extensive fires damaged surrounding power infrastructure (Toscano, 2020).

Heat stress days increase the demand for air-conditioning, in addition to irrigation pumping and desalination as water requirements increase. Studies have shown that a 2 degree Celsius warming, in Sydney, increases energy consumption by 100 percent, and a 4 degree Celsius warming increases energy consumption by 300 percent. With the increase in energy demand, power flows become congested along electrical wires which in turn impacts the stability of the system. Furthermore, as the temperature rises the cooling in ponds decreases, which impacts the effectiveness of power plant cooling. At the same time, electrical infrastructure such as overhead conductors and transformers are de-rated, as the solar irradiance on heat-stress days increases conductor sagging between pole spans, reduces ambient cooling of transformers and decreases the efficiency of electric power transmission. Adaption to heat-stress days, consequently, will require more distributed forms of generation to reduce congestion along critical power infrastructure, or otherwise, will motivate further costly grid expansion. However, on really hot days solar photovoltaics (PV) lose approximately 25 % of their efficiency creating further challenges for adaptation technology. It follows that supply chain robustness becomes another issue as climate change progresses.

The literature on climate change adaptation is limited in the area of electrical power systems and their resilience. The authors (Panteli and Mancarella, 2015a) provide a comprehensive overview of the topic, including a full view of the potential challenges and technical solutions. Clearly, there are many pathways to consider, including moving overhead conductors underground to protect them against more frequent storms or wildfires—however the expense is often considered prohibitive. Alternately, we could consider increasing pole height to reduce the occurrence of conductor sag (that can potentially spark a wildfire) and we could consider pole design for higher wind speeds to adapt to more frequent storm events. However, upgrading existing infrastructure to manage the climate risk is potentially cost-prohibitive when compared with building new components that potentially spread the risk across the system. In scenarios that optimise adaption to a world of increased climate change, is it possible to lessen the greater risk climate change imposes on the system here in Australia?

3. Power system resilience

On the definition of power system resilience, the CIGRE Working Group C4.47 (Ciapessoni et al., 2019) have proposed resilience as the ability to limit the extent, severity and duration of system degradation following an extreme event. Resilience in the design and operation of future power grids is becoming increasingly important as high-impact, low probability events become more frequent as a direct consequence of climate change (Panteli and Mancarella, 2017). A bigger and stronger electrical network is costly, and considerable cost-effective improvements can be made to the security of the electricity supply with 'smart' measures facilitated by advances in sensing, computing and the rise of internet-connected distributed energy resources (DER) (Panteli and Mancarella, 2015b). The cost of enhancing the resilience of power grids must balance the cost of bigger, stronger and smarter measures (Panteli and Mancarella, 2015a; Panteli et al., 2017a, b).

We define a high level of grid resilience as the ability to maintain the electricity supply in the face of a high-impact, low probability disturbances; reducing the area of the resilience trapezoid in Fig. 1 (Panteli et al., 2017c). When operating at a low level of resilience (phase 2 in Fig. 1), where the grid does not maintain the bulk electricity supply, suitable measures potentially reduce the duration of the outage and accelerate the grid restoration process. That is, by reducing the time (duration) of a power outage, and by accelerating the restoration process, we can increase the overall resilience of the grid by reducing the area of the resilience trapezoid in Fig. 1.

Methods for enhancing the resilience of the power grid include: (1) strengthening the infrastructure e.g., by designing overhead circuits for higher wind speed, (2) building more infrastructure to cater for a greater number of outage conditions e.g., consider designing for $N-X$ conditions,[6] and (3) improve the intelligence of the power grid by investing in advanced sensors, enhanced communication networks, and energy storage to support DER control and coordination to make the grid smarter. Such methods have prompted the formulation of a *Resilience Trilemma* for power systems (Panteli and Mancarella, 2015b), where solutions must consider approaches that make the system

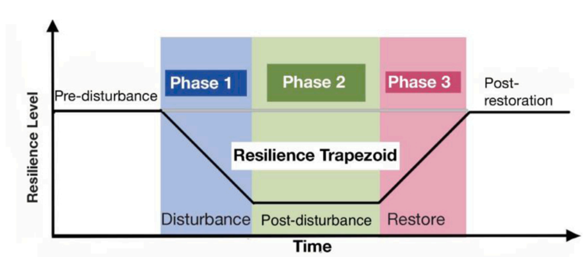

Fig. 1. Resilience trapezoid, showing each phase of a major power outage (Panteli et al., 2017c). Enhancing resilience can be visualized as reducing the area of the trapezoid. That is, we reduce the area of the resilience trapezoid by: (1) improving disturbance rejection to high-impact, low probability events, (2) reducing the time (duration) of a power outage, and (3) accelerating the grid restoration process.

1. *stronger*: to withstand stronger and more extreme events,
2. *bigger*: to reroute supply under $N-X$ conditions,
3. *smarter:* leveraging advanced sensing, computing and control to improve disturbance rejection and to accelerate the revival of the grid after a natural disaster.

Ahead of solving the Resilience Trilemma, new metrics for resilience are needed, supported by standards and market design.

To discuss the term resilience more fully, we will contrast it to the more well-defined concept of *reliability* presently used for power grid expansion decisions and operating practices. It is common practice to build redundancy into the electrical grid to accommodate cases where one or more pieces of electrical equipment fail during normal operation so that the electricity supply is not interrupted, otherwise known as $N-1$ and (for two items out of service) $N-2$. In locations where reliability requirements are higher (e.g., locations with large population centres) it is common to use the $N-2$ planning criteria in both transmission and distribution networks. To gauge the effectiveness of this planning criteria in terms of reliability, metrics such as System Average Interruption Duration Index (SAIDI), System Average Interruption Frequency Index (SAIFI), Customer Average Interruption Duration Index (CAIDI), Momentary Average Interruption Frequency Index (MAIFI), etc., are reported annually. If these indexes exceed set thresholds for reliability, it will potentially trigger a study to improve reliability in the impacted population region.

Power outages as a result of extreme climatic events may fall into the category of resilience. In general, the economics of resilience calls for different considerations from the economics of reliability, as it must incorporate complex nonlinearities from both the physics and markets. This is well-argued in (Moreno et al., 2020), with a techno-economic illustration of the implications of making resilient as opposed to reliable-only investment. Consideration for who will pay the additional cost of resilience must be addressed, otherwise widespread and sustained blackouts potentially become the new normal. As high-impact, low probability events become more frequent, we require a practical engineering approach to the concept of resilience across all spheres of electrical grid design and operation, including a definition of new frameworks and suitable metrics to quantify resilience as opposed to reliability (Panteli et al., 2017d).

4. Cyber security

Advanced sensing, wireless communication networks and sophisticated computing are all needed to control and coordinate DER operated electric power grids—requiring the secure transfer of information between network nodes. With millions of cyber-physical DER systems throughout the grid, the number of access points vulnerable to a cyberattack dramatically increases, particularly when DER such as rooftop solar, battery storage and demand response (e.g. controllable thermostatically coupled loads) are connected behind the meter outside the reach of a utility. To secure the transfer of information in DER operated power grids, and to detect malicious agents who might break classically encrypted data codes, we need to think outside the box and over the horizon as to what are the new cyber threats and vulnerabilities of the future power grid.

[6] N is the normal operating state of the grid, and X denotes the number of critical electrical components out of service—where $X >> 2$.

There are 30 billion Internet of Things (IoT) devices with Secure Sockets Layer (SSL) encrypted communications connected to the internet right now, the sheer volume alone makes protecting such systems nontrivial. With 90 percent of cyberattacks today starting with phishing emails that may not require even a mouse click, it is plausible that an internet-connected fridge might be the next target for the electricity sector, or perhaps your smart meter—both with privacy and economic implications. At scale, cyberattacks that break classically encrypted data codes have serious implications for future electricity market design and the resilient operation of electric power networks. For example, if the fridges of a million residential customers are all switched off at the same time, as instructed by a malicious actor, the frequency of the grid will potentially deviate outside set tolerances disturbing the normal operating state, and customers will potentially experience food spoilage resulting in further economic implications.

New threats and vulnerabilities for cyberattacks must be explored beyond the December 2015 Ukrainian incident that resulted in power outages affecting 225,000 customers for several hours (Liang et al., 2017). The more we rely on real-time data within the electricity sector, the more vulnerable we are to cyberattacks that shut down communication systems that support power grid operations including DER control and coordination. With state actors weaponising their cyber capabilities, it is not unexpected to see an increased frequency of attacks in the energy sector—particularly in cases where state actors deploy malware opening it up for others to reproduce. It may take about 15 hours for someone to get into a cyber system, from which the intruder may build its presence. The intruder may dwell in the systems for months; identification of the intrusion depends on the cyber capability of the organisation, but typically is many months. From there, remediation and redress—if not replacement—may take years and considerable cost. Consequently, by the time the system is protected against the known threat, the technology has moved on. To be certain that future cyber-physical energy systems are secure, we need to accelerate the pace for detection and change.

Within the next 10 years, it is expected that significant breakthroughs in quantum computing will occur. With quantum computing, malicious actors will be able to break every public encryption key within 3 minutes polynomial time,[7] a task that would take approximately 100 years with existing technology. The massive power of quantum computing enhances the aforementioned cybersecurity threats, creating significant uncertainty on how to protect the systems of today knowing the advancements to come—especially with the present pace of change within the IT sector (in the order of years). However, it is reassuring that quantum cryptography has been developed ahead of significant quantum computing breakthroughs, in particular quantum key distribution which can detect communication signals that are being eavesdropped. With advances in quantum cryptography to: (1) make codes unbreakable, (2) secure quantum communications so as to observe if someone is eavesdropping, and (3) securely encrypt and decrypt messages with quantum key distribution—we could see widespread applications in data transfer resilience for future electricity systems.

Central to any system supporting societal benefits is trust. Both accountability and transparency support the building of trust, as does protecting against cyber threats via insurance. With greater trust both society and the economy prosper, especially as the need to secure individual systems is balanced with securing shared services. Principals for cyber technology design must therefore span: (1) integrity while limiting opportunities for subversion; (2) confidentiality while limiting opportunities for espionage; and (3) accessibility while limiting opportunities for sabotage. To defend systems against cyber threats, the key is to identify the scenarios that make us most uncomfortable, that are the most extreme, and then to work through such problems. That is, zero tolerance implies an infinite cost, and so ways to build trust include knowing: (1) your data, (2) your players, (3) the drivers, and identifying a finite, acceptable risk. Importantly, an increase in cyber complexity has been strongly correlated with an erosion in societal trust, which further drives the challenges of creating a resilient electrical power system into the foreseeable future.

5. Future grids: key challenges and opportunities

Resilience is defined by the degree of the disruption and timescales for collapse and recovery. Exact probabilities for disruptive events are unknown, creating uncertainty for how we might design a system for a range of events driven by climate change or cybersecurity risks. Future electricity markets must consider significant uncertainty on the topic of system resilience, where a zero tolerance approach to resilience events implies an infinite cost. The challenge is to identify a finite risk to support market design and its evolution.

As power systems become more complex, calculating and understanding uncertainty is expected to become increasingly difficult. Counterfactuals in delivering a more resilient system will potentially support the judgement of future successes. As knowledge of probability distributions of future disruptive events improves, we will have greater clarity on the framework needed to support economic decisions. Financial decisions on resilience investments ought to be taken at a societal level, where providing a resilient system is about providing insurance against uncertainty. Customers will have a role in societal decision, supported by access to technology that potentially enhances their individual resiliency requirements. The decision to go off-grid due to resilience issues would reflect a problem in customer knowledge, as even their own system is unlikely to be perfect. Approaches to quantify and manage resiliency risks is challenging, and future electricity market design must strike a balance in societal and individual customer requirements.

The industry is responsible for improving communication with consumers on choice, providing tools to support customers with decisions on resilience. However, presently there is a lack of communication between the consumer and the industry, as no individual entity is responsible for the messaging. By enhancing communication channels, arguments supporting the developing of a budget for providing resilience, or an approach that minimises risk, might be supported and endorsed by both industry and consumers.

The concept of consumer tolerance to particular forms and timescales of grid disruption has emerged as an important topic for research ahead of characterising resilience metrics. Expectations from consumers on the level of resilience required are potentially diverse. There is a sliding scale of willingness to pay for disruption, acknowledging that zero tolerance of disruption implies infinite cost. Research on the topic of tolerance must also acknowledge that there are certain situations where we need to guarantee electricity supply (e.g., medical equipment). Consideration of how to fund such a safety net is prudent, with many customers already investing in their own technology to enhance their resilience to a loss in electricity supply from the bulk grid.

Consumer tolerance to the many forms and timescales of grid disruption is the main driver in determining resilience targets. The importance of consumer engagement, both with managing their own risk or their willingness to pay for the grid to manage the risk, is key to future market design. Open questions that remain include: (1) do consumers have enough information to make resilience decisions; (2) do consumers want to make resilience decisions; and (3) are consumer-driven resilience decisions going to confuse market design? Importantly, future electricity markets must be as dynamic and evolutionary as the power system, and what influences it to change. It follows that there is a necessary role for both government and customers in determining the optimal level of resilience, with consumers being able to retain choice, and at the same time guarding the system against self-interest actions that do not capture the broader community benefits.

[7] The amount of time required for a computer to solve a problem, expressed as a polynomial function in terms of the size of the input of the given problem.

Declaration of Competing Interest

The authors report no declarations of interest.

Acknowledgements

The authors would like to thank Andreas Baumhof who presented at the summit, for reading the manuscript and for his thoughtful presentation. We also acknowledge the summit participants who contributed to the discussion of the topic, which informed the composition of items in Section 5. Specifically, we the authors have borrowed freely, added our own perspectives and make no claim to be presenting consensus views on Summit outcomes.

References

AEMC, 2019. New Mechanisms to Enhance Resilience in the Power System: Final Report. Available: (Accessed 21 Sept. 2020). https://www.aemc.gov.au/news-centre/media-releases/new-mechanisms-enhance-resilience-power-system-final-report.

AEMO, 2020. Potential Loss of Multiple Generators in South Australia [Online]. Available: (Accessed 10 Jan. 2020). https://www.aemo.com.au.

AEMO, 2020. Draft 2020 Integrated System Plan [Online] [12 December 2019]. Available: (Accessed 3 Jan. 2020). https://www.aemo.com.au.

Blackhall, L., Kuiper, G., Nicholls, L., Scott, P., 2020. Optimising the value of distributed energy resources. Electr. J. [Accepted].

Bloomberg New Energy Finance New Energy Outlook 2017 [Online], Available: https://data.bloomberglp.com (Accessed 7 Mar. 2020).

Brear, M., Baldick, R., Cronshaw, I., Olofsson, M., 2020. Sector coupling: supporting decarbonisation of the global energy system. Electr. J. [Accepted].

E. Ciapessoni, D. Cirio, A. Pitto, M. Panteli, M. V. Harte, C. Mak, on behalf of C4.47 WG Members, Defining power system resilience [No. 306 - ELECTRA], Available: https://e-cigre.org (October 2019).

Colvin, R., Crimp, S., Lewis, S., Howden, M., 2020. Implications of climate change for future disasters. In: Lukasiewicz, A., Baldwin, C. (Eds.), Natural Hazards and Disaster Justice. Palgrave Macmillan, Singapore.

Dodd, T., Rai, A., Caught, K., 2020. Electricity markets in flux — the importance of a just transition. Electr. J. [Accepted].

Fazey, I., Schäpke, N., Caniglia, G., Patterson, J., Hultman, J., van Mierlo, B., Säwe, F., Wiek, A., Wittmayer, J., Aldunce, P., Waer], H.A., Battacharya, N., Bradbury, H., Carmen, E., Colvin, J., Cvitanovic, C., D'Souza, M., Gopel, M., Goldstein, B., Hamäläinen, T., Harper, G., Henfry, T., Hodgson, A., Howden, M.S., Kerr, A., Klaes, M., Lyon, C., Midgley, G., Moser, S., Mukherjee, N., Muller, K., O'Brien, K., O'Connell, D.A., Olsson, P., Page, G., Reed, M.S., Searle, B., Silvestri, G., Spaiser, V., Strasser, T., Tschakert, P., Uribe-Calvo, N., Waddell, S., Rao-Williams, J., Wise, R., Wolstenholme, R., Woods, M., Wyborn, C., 2018. Ten essentials for action-oriented and second order energy transitions, transformations and climate change research. Energy Res. Soc. Sci. 40 (2018), 54–70.

Fleming, A., Howden, S.M., 2016. Ambiguity: a new way of thinking about responses to climate change. Sci. Total Environ. 571 (2016), 1271–1274.

Habib, A.H., Ratnam, E.L., Disfani, V.R., Kleissl, J., de Callafon, R.A., 2016. Optimization-based residential load scheduling to improve reliability in the distribution grid. Proc. IEEE Conf. on Decision and Control (CDC 2016) 2419–2424 (Dec. 2016).

IPCC, 2014. Climate Change 2014: Synthesis Report. In: Core Writing Team, Pachauri, R. K., Meyer, L.A. (Eds.), Contribution of Working Groups I, II and III to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. IPCC, Geneva, Switzerland, 151 pp.

Lasseter, R.H., 2011. Smart distribution: coupled microgrids. Proc. IEEE 99 (6), 1074–1082 (2011).

LeRoy, W.A., 2016. Increasing western us forest wildfire activity: sensitivity to changes in the timing of spring. Phil. Trans. R. Soc. B 371, 670–673 (Dec. 2016).

Leslie, G.W., Stern, D.I., Shanker, A., Hogan, M.T., 2020. Designing electricity markets for high penetrations of zero or low marginal cost intermittent energy sources. Electr. J. [Accepted].

Liang, G., Weller, S.R., Zhao, J., Luo, F., Dong, Z.Y., 2017. The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE Trans. Power Syst. 32 (4), 3317–3318 (2017).

MacGill, I., Esplin, R., 2020. End-to-end electricity market design – lessons from the Australian National Electricity Market. Electr. J. [Accepted].

MacMilliam, D., Siddliqui, F., Kelly, H., 2020. PG&E's Role in Sonoma fire Questioned As Power Outage Frustrations Grow (Accessed 21 Sept. 2020). https://www.washingtonpost.com/business/2019/10/29/pges-role-sonoma-fire-questioned-anger-around-power-outages-spreads/.

von Meier, A., Ratnam, E.L., Brady, K., Moffat, K., Swartz, J., 2020. Phasor-based control for scalable integration of variable energy resources. Energies 13 (190), 1–14 (2020).

Minkel, J.R., 2020. The 2003 Northeast Blackout—Five Years Later: Tougher Regulatory Measures Are in Place, but We're Still a Long Way From a Smart Power Grid [Online]. https://www.scientificamerican.com/article/2003-blackout-five-years-later/.

Moreno, R., Panteli, M., Mancarella, P., et al., 2020. From reliability to resilience: Planning the grid against the extremes. IEEE Power Energ. Mag. 18 (4), 41–53. July-Aug. 2020.

Nelson, J., 2020. Australia's national electricity market: financing the transition. Electr. J. [Accepted].

Panteli, M., Mancarella, P., 2015a. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. Electr. Power Syst. Res. 127 (2015), 259–270.

Panteli, M., Mancarella, P., 2015b. The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. IEEE Power Energ. Mag. 13 (3), 58–66 (May 2015).

Panteli, M., Mancarella, P., 2017. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. IEEE Syst. J. 11 (3), 1733–1742 (Sep. 2017).

Panteli, M., Pickering, C., Wilkinson, S., Dawson, R., Mancarella, P., 2017a. Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures. IEEE Trans. Power Syst. 32 (5), 3747–3757 (Sep. 2017).

Panteli, M., Trakas, D.N., Mancarella, P., Hatziargyriou, N.D., 2017b. Power systems resilience assessment: hardening and smart operational enhancement strategies. Proc. IEEE 105 (7), 1202–1213 (Jul. 2017).

Panteli, M., Mancarella, P., Trakas, D.N., Kyriakides, E., Hatziargyriou, N.D., 2017c. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Trans. Power Syst. 32 (6), 4732–4742 (Nov. 2017).

Panteli, M., Mancarella, P., Trakas, D.N., Kyriakides, E., Hatziargyriou, N.D., 2017d. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Trans. Power Syst. 32 (6), 4732–4742 (Nov. 2017).

Sankur, M.D., Dobbe, R., von Meier, A., Stewart, E.M., Arnold, D.B., 2018. Optimal Voltage Phasor Regulation for Switching Actions in Unbalanced Distribution Systems, 1804.02080, arXiv, math.OC [online].

Skinner, B., Mancarella, P., Vrakopoulou, M., Hiskens, I., 2020. Incorporating new power system security paradigms into low-carbon electricity markets. Electricity J. [Accepted].

Toscano, N., 2020. 'Like New York After Sandy': Bushfires a 'wake-up Call' for Power Grid (Accessed 21 Sept. 2020). https://www.smh.com.au.

van Oldenborgh, G.J., Krikken, F., Lewis, S., Leach, N.J., Lehner, F., Saunders, K.R., van Weele, M., Haustein, K., Li, S., Wallom, D., Sparrow, S., Arrighi, J., Singh, R.P., van Aalst, M.K., Philip, S.Y., Vautard, R., Otto, F.E.L., 2020. Attribution of the Australian bushfire risk to anthropogenic climate change. Nat. Hazards Earth Syst. Sci. Discuss. 2020 (2020), 1–46.

von Meier, A., Stewart, E., McEachern, A., Andersen, M., Mehrmanesh, L., 2017. Precision micro-synchrophasors for distribution systems: a summary of applications. IEEE Trans. Smart Grid 8 (6), 2926–2936 (Nov. 2017).

Dr Elizabeth Ratnam, Lecturer and FERL Fellow at the Australian National University. Dr Ratnam earned the BEng (Hons I) degree in Electrical Engineering in 2006, and the PhD degree in Electrical Engineering in 2016, from the University of Newcastle, Australia. She subsequently held postdoctoral research positions with the Center for Energy Research at the University of California San Diego, and at the University of California Berkeley in the California Institute for Energy and Environment (CIEE). During 2001–2012 she held various positions at Ausgrid, a utility that operates one of the largest electricity distribution networks in Australia. Dr Ratnam currently holds a Future Engineering Research Leader (FERL) Fellowship from the Australian National University (ANU) and she joined the Research School of Electrical, Energy and Materials Engineering at ANU as a research fellow and lecturer in 2018. Her research interests are in developing new paradigms to control distribution networks with a strong focus on creating a resilient carbon neutral power grid.

Prof. Ken Baldwin, Director of the Energy Change Institute at the Australian National University. Professor Baldwin has held the following appointments: Project Steering Committee for the Australian Energy Technology Assessment (AETA) of the former Bureau of Resources and Energy Economics (BREE, 2011–2013); Board of the South East Region of Renewable Energy Excellence (SERREE, from 2014); Socio-Economic Modelling Advisory Committee of the South Australian Nuclear Fuel Cycle Royal Commission (2015–2017); Chair, Energy Cluster of the Australia-Indonesia Centre (2015–2018); Chair, Energy Research Institutes Council for Australia (ERICA, 2018–2019); Steering Committee for the CSIRO Hydrogen Research, Development and Demonstration Report (2019). Professor Baldwin is an inaugural ANU Public Policy Fellow, and winner of the 2004 Australian Government Eureka Prize for Promoting Understanding of Science, for his role in initiating and championing "Science meets Parliament". In 2007, Professor Baldwin was awarded the W.H. Beattie Steele Medal, the highest honour of the Australian Optical Society. In 2010 he was awarded the Barry Inglis Medal by the National Measurement Institute for excellence in precision measurement. Professor Baldwin is a Fellow of the American Physical Society, the Institute of Physics (UK), the Optical Society of America and the Australian Institute of Physics.

Prof. Pierluigi Mancarella, Chair of Electrical Power Systems at the University of Melbourne. Prof. Pierluigi Mancarella is Chair Professor of Electrical Power Systems at the University of Melbourne and Professor of Smart Energy Systems at the University of Manchester, UK. His research interests include techno-economic modelling of integrated energy systems, low-carbon network planning under uncertainty, and risk and resilience assessment of energy systems. Pierluigi is the 2017 Victorian Government veski innovation fellow and the recipient of a 2018 International Newton Prize for his work on resilience-based Power System planning in Chile.

Prof. Mark Howden, Director of the Climate Change Institute at the Australian National University. Prof. Mark Howden is Director of the Climate Change Institute at the Australian National University, an Honorary Professor at Melbourne University, a Vice-Chair of the Intergovernmental Panel on Climate Change (IPCC) and a member of the ACT Climate Change Council. He contributes to several major national and international science and policy advisory bodies. Mark has worked on climate variability, climate change, innovation and adoption issues for over 30 years in partnership with many industries, community and policy groups via both research and science-policy roles. Issues he has addressed include agriculture and food security, the natural resource base, ecosystems and biodiversity, energy, water and urban systems. He helped develop both the national and international greenhouse gas inventories that are a fundamental part of the Paris Agreement and has assessed sustainable ways to reduce emissions. He has been a major contributor to the IPCC since 1991, sharing the 2007 Nobel Peace Prize.

Prof. Lesley Seebeck CEO of the Cyber Institute at the Australian National University. Dr Lesley Seebeck started as the CEO of the Cyber Institute, Australian National University, on 30 July 2018. Most recently, she was Chief Investment and Advisory Officer at the Digital Transformation Agency, arriving there from the Bureau of Meteorology where she served as Chief Information Officer from mid 2014 to late 2017. She was recognised as Federal Government CIO of the Year in 2017 and in February 2019 she was appointed to the Naval Shipbuilding Advisory Board. Dr Seebeck has extensive experience in strategy, policy, management, budget, information technology and research roles in the Australian Public Service, industry and academia. She has worked in the Departments of Finance, Defence, and the Prime Minister and Cabinet, the Office of National Assessments, and as an IT and management consultant in private industry, and at two universities. Dr Seebeck has a PhD in information technology, an MBA, a Masters in Defence Studies and a Bachelor's degree in Applied Science (Physics). http://linkedin.com/in/lesley-seebeck-346542a