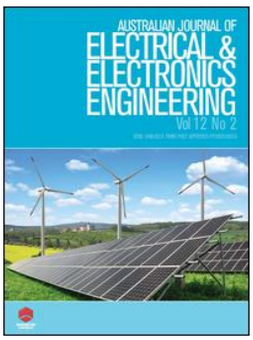

Taylor & Francis
Taylor & Francis Group

Australian Journal of Electrical and Electronics Engineering

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tele20

The concept of vulnerability and resilience in electric power systems

Umair Shahzad

To cite this article: Umair Shahzad (2021): The concept of vulnerability and resilience in electric power systems, Australian Journal of Electrical and Electronics Engineering, DOI: 10.1080/1448837X.2021.1943861

To link to this article: https://doi.org/10.1080/1448837X.2021.1943861

AUSTRALIAN JOURNAL OF ELECTRICAL AND ELECTRONICS ENGINEERING
https://doi.org/10.1080/1448837X.2021.1943861

Taylor & Francis
Taylor & Francis Group

ARTICLE

The concept of vulnerability and resilience in electric power systems

Umair Shahzad

Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE, USA

ABSTRACT

The electric power system is one of the most vital infrastructures, and its security is necessary for the proper functioning of society. The main goal for the electric power system has traditionally been continuity of the electrical power supply. However, in addition to this requirement, power systems must follow the requirements associated with vulnerability and resilience. Vulnerability deals with the assessment of risk, as it relates to physical and economic consequences, arising from the capability of the network to handle an undesirable incident. Resilience deals with the network capability to withstand unknown disturbances, and consequently, the ability to restore stable operating conditions. Despite some research on power system resilience and vulnerability, their basic concepts are still unexplored. This paper aims to discuss the essential concepts of vulnerability and resilience in electric power systems. Their assessment frameworks and quantification metrics are also described. Case studies, on standard test systems, to demonstrate the assessment of power system vulnerability and resilience, are also part of this research.

ARTICLE HISTORY
Received 23 June 2020
Accepted 11 June 2021

KEYWORDS
Disturbances; power system resilience; power system vulnerability; risk; security

1. Introduction

In the recent past, electric power systems have operated quite near to their operating limits. This is due to many factors including lack of investment, deregulation of electricity markets, and various other technical reasons. Under such situations, sudden network disturbances can cause system blackouts (Kerin et al. 2009). Traditionally, these systems have been secured against low-impact, high-probability (LIHP) events caused by component failures, man-made errors, or minor exterior interferences (Panteli and Mancarella 2015a; Chang and Wu 2011). On the contrary, high-impact, low- probability (HILP) events can cause sporadic power outages, which can cause tremendous social and economic damage. Such outages can spread to unpredictable portions of the power system (Amirioun, Aminifar, and Lesani 2018). These events can be precipitated by natural events, such as tornados, cyclones, snowstorms, inundations, and earthquakes, or by deliberate cyber or physical attacks (Li et al. 2017; Chanda and Srivastava 2016; Gholami, Aminifar, and Shahidehpour 2016; Gao et al. 2016; Manshadi and Khodayar 2015). Thus, in addition to power systems being reliable when confronted by credible threats, they should also be able to withstand unforeseen extreme incidents. Recently, various natural disasters and deliberate human attacks have caused unparalleled challenges for power systems, which emphasises that power systems are still unprepared to tackle extreme events. For instance, the 2008 snowstorm in South China resulted in over 129 faults on transmission lines. This caused power outages to 14.66 million homes. In 2012, Hurricane Sandy resulted in chaos on the east coast of the U.S. It is projected that such disasters will continue to rise, due to climate change and the ageing energy infrastructure (Schneider et al. 2016; Bie et al. 2017). Thus, it is imperative that power systems be able to endure events with huge negative impact. Therefore, it is important to define and debate the concepts of vulnerability and resilience in relation to electric power systems. This paper is organised as follows. Sections 2 and 3 discuss the definitions, conceptual frameworks, and metrics, for vulnerability and resilience in electric power systems, respectively. Sections 4 and 5 demonstrate case studies for assessing power system vulnerability and resilience, respectively. Section 6 concludes the paper with a proposed direction for research.

2. Power system vulnerability

Power system vulnerability does not have a standard definition, but (Doorman et al. 2006) defines it as the insufficient ability of the system to endure an unwanted event. Vulnerability analysis plays a significant role in aiding transmission network operators, and identifying vulnerable components, whose protection will result in a system, that is resilient against HILP events (Trakas et al. 2016). Generally, these events are a result of weather- related hazards, such as snowstorms, landslides, tornadoes,

CONTACT Umair Shahzad umairshahzada@hotmail.com Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, Lincoln, NE, USA

and floods (Bompard, Pons, and Wu 2012). Reference (Baldick et al. 2009) defines a vulnerable system as a system that functions with a 'reduced level of security that renders it vulnerable to the cumulative effects of a series of moderate disturbances.' Reference (Fouad, Zhou, and Vittal 1994) describes the notion of vulnerability connecting the system security level with the inclination to alter its operating conditions to a critical state, which (McGillis et al. 2006) calls the 'Verge of Collapse' state. Similarly, (Proag 2014) defines power system vulnerability as 'a measure of risk associated with the physical, social, and economic aspects and implications, resulting from the system's ability to cope with the resulting event.'

The vulnerability of power systems can be categorised into five broad dimensions to formulate a generic background for vulnerability assessment (Abedia, Gaudard, and Romerio 2019; Hofmann, Kjølle, and Gjerde 2012). These dimensions are: threat/hazard, exposure, susceptibility, coping capacity, and criticality. Using these dimensions, a generic vulnerability framework can be formulated, as shown in Figure 1.

Threats and hazards are often used interchangeably, since hazards are included in threats. According to (Proag 2014), a threat is any indication or unforeseen event capable of interrupting a system, in part or in whole. This definition incorporates all likely causes of threats, i.e. natural hazards, technical errors, human mistakes, and deliberate acts of disruption. As evident from Figure 1, system vulnerability is categorised into susceptibility and coping capacity. The susceptibility of the infrastructure is the extent to which a threat can cause a disturbance in the system. This broadly depends on the operational limits of the system. According to (Hofmann, Kjølle, and Gjerde 2012), a system is considered susceptible to a threat if that threat causes an undesirable system event. The coping capacity is the ability of the system operator and the system itself to deal with an undesirable situation, minimise adverse consequences, and reinstate the normal operation of the system. The best manner to evaluate the criticality of an infrastructure is in terms of the reliance of society on that infrastructure. Criticality is the degree to which the infrastructure customers will be affected, when a system fails to perform its planned operation, the severity of which can be evaluated by numerous aspects, such as disturbance duration, financial consequences, social consequences, and technical consequences (Hofmann, Kjølle, and Gjerde 2012). Reference (Kjølle, Gjerde, and Nybø 2010) uses the conventional bow-tie approach to describe the concept of vulnerability in power systems, as shown in Figure 2. The major undesirable events affecting a power system are power system failures due to natural events (e.g. a strong snowstorm), operational/technical errors, human mistakes, and intentional acts of terror. The consequences are quantified in terms of blackouts. The threats might cause power system failures due to a chain of events culminating in severe consequences. As shown in Figure 2, various barriers (labelled B1, B2, etc.) are present to avert threats from forming into unwanted circumstances and to decrease the possibility of extreme consequences. A system is more vulnerable towards these threats if these barriers do not function properly.

According to (Akdeniz and Bagriyanik 2016), power system vulnerability indices can be divided into two main classes: operational and non- operational. These are outlined in Figure 3.

The operational performance indices deal with internal and, usually, electrical performance measures and non- operational indices focus on possible and probable risks, linked with external factors, over which transmission system operators (TSOs) have no control. Depending on the kind of disturbance, the risks which can be assessed using historical data are termed as probable risks; and those for which any statistical data is not available are known as possible risks (Akdeniz and Bagriyanik 2016).

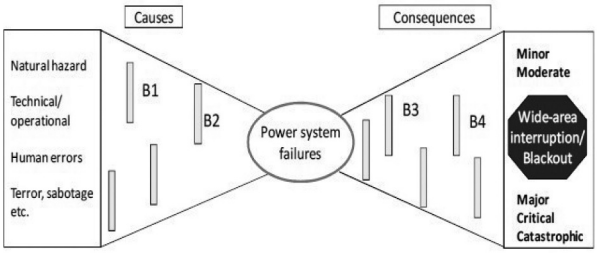

Figure 2. Threats, unwanted event, consequences, and barriers.

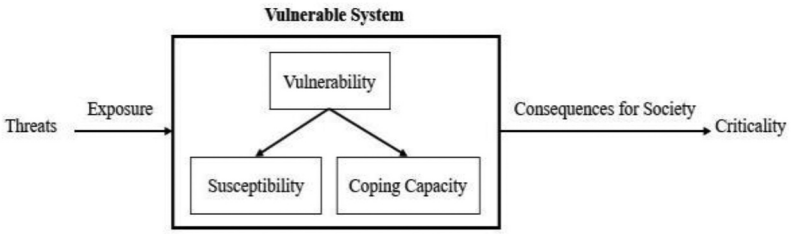

Figure 1. General vulnerability framework.

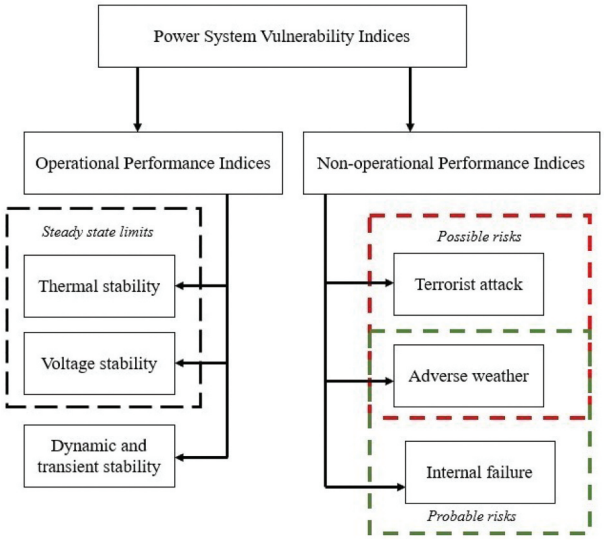

Figure 3. Power system vulnerability indices.

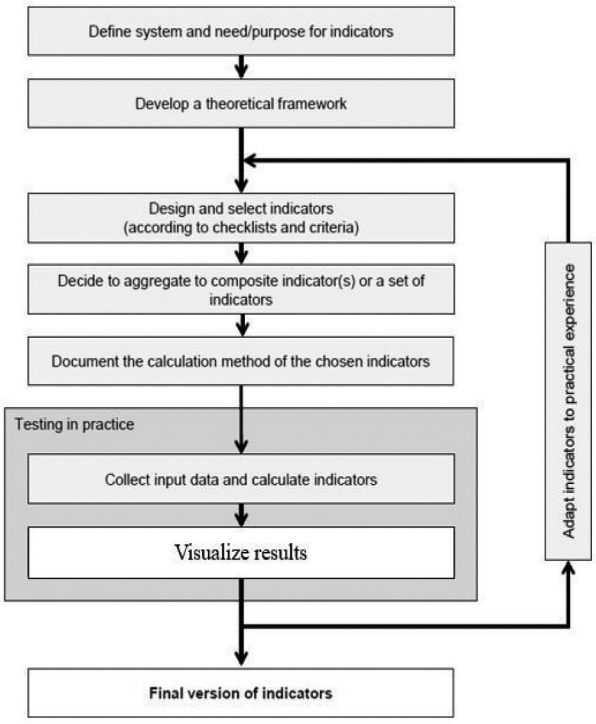

Figure 4. Procedure for development of vulnerability indicators.

Power system vulnerability should be quantified using appropriate indictors or indices. The conceptual procedure for developing these indices is shown in Figure 4 (Hofmann, Kjølle, and Gjerde 2012). Outlining the scope of the vulnerability indicator is the first step in its development. The purpose of the indicator should be concise. The second step focuses on the creation of a theoretical framework where all of those aspects which affect vulnerability should be well-defined with a nested structure of sub aspects of vulnerability. Moreover, the kinds of indicators required to elaborate on various features of vulnerability should be elucidated.

The third step consists of designing appropriate indicators. This is done to ensure pertinent aspects are considered. This step also incorporates the definition of scales and the provision of suitable computation approaches to report the selected indicators in a uniform way. It is recommended that each indicator be defined based on a standard template. If the number of indicators is large or the aim is to analyse multiple dimensional aspects, an aggregation of indicators is required to form a composite indicator or a set of indicators. After choosing the indicators, they need to be tested in real scenarios to get feedback on their performance from potential users. Therefore, data must be gathered to formulate the indicators. A visual display of results aids the user in capturing trends. The design, computation methods, scales, aggregation principles, and the visualisation of the indicators should further be adapted based on practical testing experience. This process of enhancing and testing the indicators is iterated many times until a final version of the indicators is achieved. Some existing power system vulnerability indices, together with the factors considered for their evaluation, are shown in Table 1 (Wei et al. 2018).

Table 1. Some existing power system vulnerability indices.

Vulnerability Indices	Factors Considered
Extended Betweenness (Bompard, Pons, and Wu 2012)	Admittance, Power Transfer Distribution, Line Flow Limits
Hybrid Flow Betweenness (Bai and Miao 2015)	Power Flow, Line Flow Limits, Generation Capacity, Admittance, Load
Electric Betweenness (Wang et al. 2011)	Current, Generation Capacity, Admittance, Load
Maximum Flow (Fang et al. 2018)	Admittance, Power Flow, Line Flow Limits
Load Redistribution (Wenli et al. 2016)	Load, Node Capacity
Bus Dependency Matrix (Nasiruzzaman, Pota, and Akter 2014)	Power Flow, Admittance
Structural Vulnerability Index (Li et al. 2012)	Generation Capacity, Load, Admittance
Grid Coupling Degree (Hu and Li 2016)	Current

3. Power system resilience

Like power system vulnerability, power system resilience systems to such disastrous events has fascinated many researchers lately (Wang et al. 2016; Panteli and Mancarella 2015b). According to (Amirioun, Aminifar, and Lesani 2018; Li et al. 2017; Chanda and Srivastava 2016), power system resilience is the ability of a power system to respond to HILP events; and it emphasises how quickly and resourcefully the power system can be reinstated to its pre-event

operational state. However, it must be noted that the idea of resilience differs from the idea of reliability; reliability focuses on high- probability events, while resilience puts stress on high-impact events. The notion of resilience in power systems can be explained with the help of a resilience curve versus time, as shown in Figure 5 (Tabatabaei, Ravadanegh, and Bizon 2018).

This curve aids power system planners in assessing the power system resilience. Robustness and resistance are the salient characteristics of the system to make it able to deal with events before time *te*' i.e. the time before an event occurs. In Figure 5, *R* denotes the resilience level; and ^{R}o denotes the operational state of the power system. The capability of operational flexibility allows effective conditions for system planners to enhance system resilience.

After the event has occurred, the resilience level decreases drastically to the point R_{pe}. Moreover, the main characteristics of this system stare are resourcefulness, redundancy, and adaptive self-organisation. These features enable the system to deal with the new conditions that never occurred before. The resilience level at time t_r is reduced to R_o-R_{pe}. The third state is called restorative state which is categorised by quick response and recovery of system. After this state, the system goes into post-restoration stage with a resilience level of $R_{pr.}$

In general, power system resilience consists of the following main elements (Li et al. 2017).

(A) *Continuous situational awareness*. Using the operating conditions and external factors (weather conditions etc.), situational awareness allows the conception of the present conditions and the prediction of upcoming disturbances. Consequently, the extreme event can be actively coped with.

(B) *Robustness and readiness prior to any extreme event*. To minimise the negative effects of any upcoming system disruptions, both infrastructural and operational measures are organised before the occurrence of severe events. The electricity infrastructure is strengthened so that it will be invulnerable to hypothesised commotions. Moreover, power system operations must be flexible to tolerate substantial commotions. These resilience measures must self-adapt to embryonic extreme events.

(C) *Receptiveness and survivability during any extreme event*. Power system operators must be ready to take appropriate actions in an appropriate fashion to preserve the system operating conditions and control any deterioration in the performance of the system. Moreover, power system must be able to endure any extreme events by upholding a minimum functionality level.

(D) *Recoverability and rapidity after any extreme event*. System performance must be recoverable and restored swiftly to the level prior to the incidence of extreme incident.

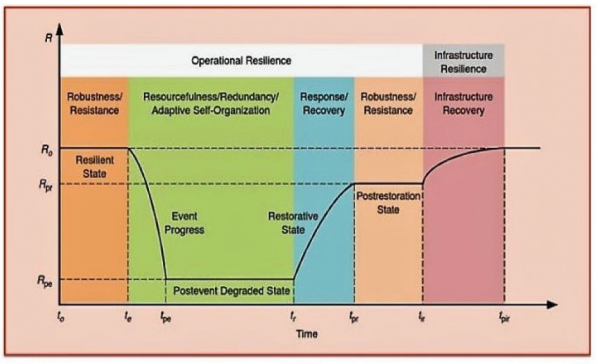

Figure 5. General resilience curve for a power system.

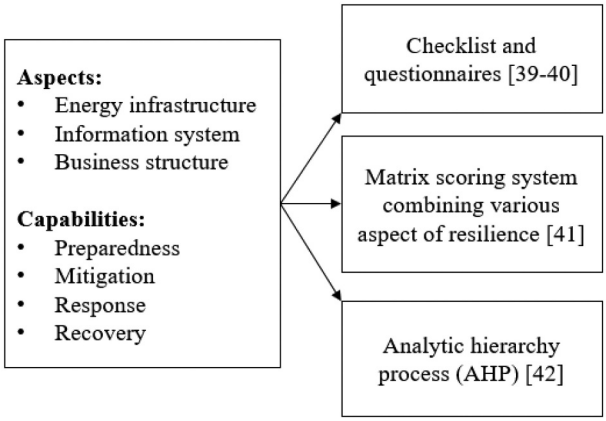

Figure 6. Qualitative evaluation of resilience metrics.

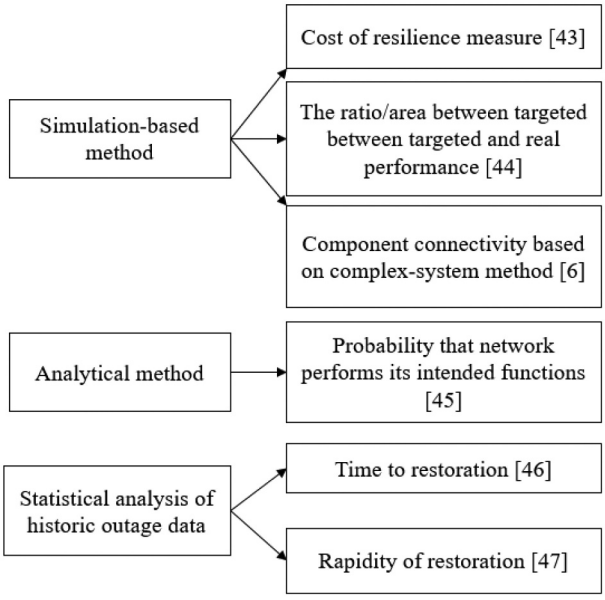

Figure 7. Quantitative evaluation of resilience metrics.

According to (Bie et al. 2017), power system resilience metrics can be evaluated using two approaches: qualitative and quantitative. These approaches are shown in Figures 6 and 7, respectively.

In the qualitative evaluation of resilience metrics, the aspects and resilience capabilities are considered. The aspects usually incorporated in the qualitative evaluation include the power system and other co-dependent systems, such as, information system, fuel supply chain, etc. Capabilities incorporate preparedness, mitigation, response, and recovery, e.g. the existence of a backup plan, personnel training, and availability of repair team (Carlson et al. 2012; McManus et al. 2007; Roege et al. 2014; Orencio and Fujii 2013). On the contrary, quantitative methods are founded on quantifying the performances of the system.

Quantitative metrics are used to assess the efficiency of specific resilience measures or to contrast the resilience values for various systems. Such metrics are performance-based and event specific. Moreover, they can incorporate network uncertainties and aid in accurate decision-making process. Methods for quantitative resilience metrics evaluations are classified into three kinds: the simulation-based method, the analytic method, and the statistical analysis. The simulation-based method is most commonly used as it can be effortlessly merged with disastrous situations and resulting consequences can be easily computed. The analytical method uses the probability of system failure in a specific situation. Historic outage and restoration records can be used to analyse data for those networks which have sufficient data on disasters due to natural events (Chanda and Srivastava 2016; Watson et al. 2015; Shinozuka et al. 2003; Whitson and Ramirez-Marquez 2009; Maliszewski and Perrings 2012; Reed, Kapur, and Christie 2009).

4. Power system vulnerability assessment: a case study

Vulnerability can take place in any part of the power system: lines, buses, generators, etc. Here, only generator vulnerability is considered to demonstrate the assessment of vulnerability. For this purpose, active and reactive powers of generators are considered. Let *Gv* denote the generator vulnerability index, i.e.

$$Gv = \sum_{i=1}^{N} GPi + GQi \tag{1}$$

Where *GPi*and*GQi*denotes the vulnerability index for active and reactive powers of i^{th} generator. *N* denotes total number of generators in the system.

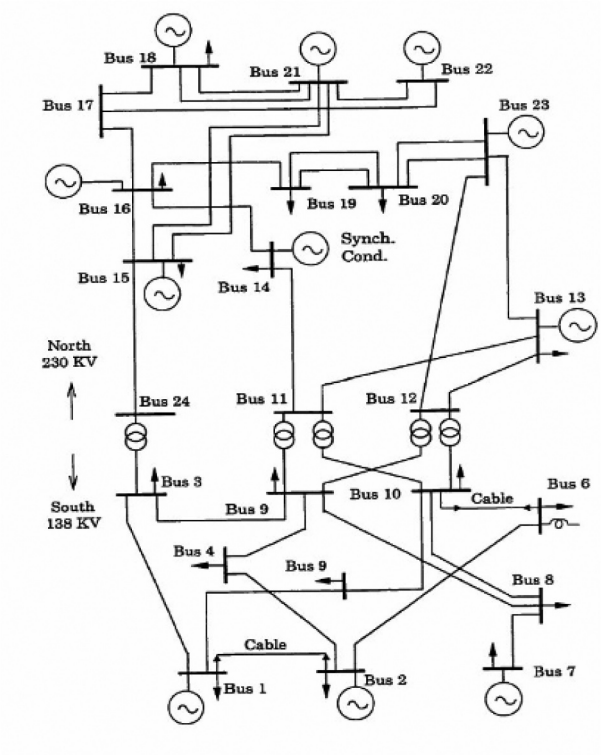

Figure 8. IEEE 24-bus test system.

Table 2. Value of *Gv*for various generator contingencies.

Contingency type	*Gv*
Base case	5.65
G1	5.79
G13	5.85
G14	5.04
G15	4.84
G18	4.39
G23	6.85

All simulations are conducted with the help of DIgSILENT PowerFactory commercial software. The first step is to analyse the system in the base case i.e. without any disturbances/contingencies. In the next step, various generator contingencies are considered. If the value of *Gv*is higher than that of base case, this indicates system is 'more' vulnerable. IEEE 24 bus test system, as shown in Figure 8, was used to conduct the required simulations. The data for the system is taken from (IEEE 24-bus Test System). The weights for *GQi*and *GPi*are assumed to be equal for reducing complexity. The values of *Gv* for various generator contingences are shown in Table 2. The contingencies column indicates the generator which is taken out.

From the Table, it is evident that outage of generators G1, G13 and G23 make the system more vulnerable as their associated *Gv* values are higher than base case value of 5.65. On the contrary, outage of generators G14, G15 and G18 reduce the system vulnerability. As a possible future extension, additional faults on

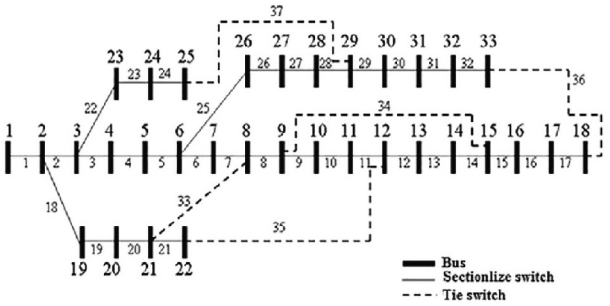

Figure 9. IEEE 33-bus test system.

Table 3. Value of lost load (MW) for various faults.

Bus Fault Location(s)	Lost load (MW)
8–26	2.7
1–13	2.5
4–15	2.9
6–19	3.1
8–13	3.2

other system components, such as lines, transformers, etc. can be incorporate in the assessment procedure.

5. Power system resilience assessment: a case study

To demonstrate an assessment methodology for power system resilience, IEEE 33-bus radial test system was used. The single line diagram is shown in Figure 9. The associated system data can be found in (33-bus radial distribution system) and (Baran and Wu 1989). Various bus faults were considered. The total system active load is 3.72 MW. Two distinct cases are considered: case 1 and case 2. Case 1 contains no distributed generation (DG) and no tie switches. Case 2 contains no DG but has tie switches. Assuming a simultaneous fault at Buses 8 and 26, the resulting lost load (MW) for both cases is computed. The steps were repeated for other fault locations. It is assumed that system operators have enough past statistical data regarding fault location, thus, these specific faults are considered for resilience assessment. The results are shown in Table 3.

From the Table, it is obvious that the maximum load restoration is possible for a fault at Bus 1 and Bus 13. Thus, system is most resilient for a fault at Bus 1 and Bus 13. For a future work, additional fault locations can be considered, and system resiliency can be computed. Moreover, it is of paramount significance to consider probabilistic risk-based approaches in analysing power system resilience as the conventional power system is transitioning towards smart power system (Shahzad and Asgarpoor 2018, 2019; Shahzad 2020; Dondossola, Garrone, and Szanto 2011; Soonee et al. 2018).

6. Conclusion and future work

This paper described the basic concepts for power system vulnerability and resilience. Definitions, conceptual framework and metrics were discussed. It was emphasised that power systems should be designed, keeping in view, the requirements for enhanced resilience and reduced vulnerability. Two different case studies were conducted to demonstrate the assessment of vulnerability and resilience in power systems. The results comprehensively indicate that there is a strong requirement to incorporate power system resilience and vulnerability in the routine procedure of power system operation and planning. Despite the large body of research analysis, the perceptions of vulnerability and resilience are still immature in the power system. Although, various indices and metrics have been proposed for quantifying vulnerability and resilience in power systems, there is still a need to formulate a consistent and comprehensive platform for applications on real-time systems. There are various challenges to quantify vulnerability and resilience to extreme events. One of the main challenge, which remains to be unravelled, is how power systems can accurately predict and adapt to the approaching extreme events. Research on power system vulnerability and resilience is just the tip of iceberg. Extreme events will always be a daunting challenge to power system researchers. Therefore, future investment, strategies, procedures, and innovative ideas are much desirable to assess vulnerability and resilience requirements in the power system.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Umair Shahzad was born in Faisalabad, Pakistan. He received a B.Sc. Electrical Engineering degree from the University of Engineering and Technology, Lahore, Pakistan, and a M.Sc. Electrical Engineering degree from The University of Nottingham, England, in 2010 and 2012, respectively. He is currently working towards Ph.D. Electrical Engineering from The University of Nebraska-Lincoln, USA. His research interests include power system analysis, power system security assessment, power system stability, machine learning, and probabilistic methods applied to power systems.

ORCID

Umair Shahzad http://orcid.org/0000-0003-2968-5026

References

33-bus radial distribution system. Accessed 20 June 2020. https://egriddata.org/dataset/33-bus-radial-distribution-system

Abedia, A., L. Gaudard, and F. Romerio. 2019. "Review of Major Approaches to Analyze Vulnerability in Power System." *Reliability Engineering and System Safety* 183 (Mar): 153–172. doi:10.1016/j.ress.2018.11.019.

Akdeniz, E., and M. Bagriyanik. 2016. "A Knowledge Based Decision Support Algorithm for Power Transmission System Vulnerability Impact Reduction." *Electrical Power and Energy Systems* 78 (Jun): 436–444. doi:10.1016/j.ijepes.2015.11.041.

Amirioun, M. H., F. Aminifar, and H. Lesani. 2018. "Resilience-oriented Proactive Management of Microgrids against Windstorms." *IEEE Transactions on Smart Grid* 33 (Jul): 4275–4284.

Bai, H., and S. Miao. 2015. "Hybrid Flow Betweenness Approach for Identification of Vulnerable Line in Power System." *IET Generation, Transmission & Distribution* 9 (Jan): 1324–1331. doi:10.1049/iet-gtd.2014.1016.

Baldick, R. et al., 2009. "Vulnerability Assessment for Cascading Failures in Electric Power Systems." In *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, USA, 1–9.

Baran, M. E., and F. F. Wu. 1989. "Network Reconfiguration in Distribution Systems for Loss Reduction and Load Balancing." *IEEE Transactions on Power Delivery* 4 (Apr): 1401–1407. doi:10.1109/61.25627.

Bie, Z., Y. Lin, G. Li, and F. Li. 2017. "Battling the Extreme: A Study on the Power System Resilience." *Proceedings of the IEEE* 105 (Jul): 1253–1266. doi:10.1109/JPROC.2017.2679040.

Bompard, E., E. Pons, and D. Wu. 2012. "Extended Topological Metrics for the Analysis of Power Grid Vulnerability." *IEEE Systems Journal* 6 (Sep): 481–487. doi:10.1109/JSYST.2012.2190688.

Carlson, J. L. et al., 2012. "Resilience: Theory and Applications." Tech. Rep. ANL/DIS-12-1, Argonne, IL, USA, February.

Chanda, S., and A. K. Srivastava. 2016. "Defining and Enabling Resiliency of Electric Distribution Systems with Multiple Microgrids." *IEEE Transactions on Smart Grid* 7 (Nov): 2859–2868. doi:10.1109/TSG.2016.2561303.

Chang, L., and Z. Wu. 2011. "Performance and Reliability of Electrical Power Grids under Cascading Failures." *International Journal of Electrical Power and Energy Systems* 33 (Oct): 1410–1419. doi:10.1016/j.ijepes.2011.06.021.

Dondossola, G., F. Garrone, and J. Szanto. 2011. "Cyber Risk Assessment of Power Control Systems — A Metrics Weighed by Attack Experiments." *2011 IEEE Power and Energy Society General Meeting*, 1–9. Detroit, MI, USA.

Doorman, G. L., K. Uhlen, G. H. Kjolle, and E. S. Huse. 2006. "Vulnerability Analysis of the Nordic Power System." *IEEE Transactions on Power Systems* 21 (Feb): 402–410. doi:10.1109/TPWRS.2005.857849.

Fang, J., C. Su, Z. Chen, H. Sun, and P. Lund. 2018. "Power System Structural Vulnerability Assessment Based on an Improved Maximum Flow Approach." *IEEE Transactions on Smart Grid* 9 (Mar): 777–785. doi:10.1109/TSG.2016.2565619.

Fouad, A., Q. Zhou, and V. Vittal. 1994. "System Vulnerability as a Concept to Assess Power System Dynamic Security." *IEEE Transactions on Power Systems* 9 (May): 1009–1015. doi:10.1109/59.317643.

Gao, H., Y. Chen, Y. Xu, and C. Liu. 2016. "Resilience-oriented Critical Load Restoration Using Microgrids in Distribution Systems." *IEEE Transactions Smart Grid* 7 (Nov): 2837–2848. doi:10.1109/TSG.2016.2550625.

Gholami, A., F. Aminifar, and M. Shahidehpour. 2016. "Front Lines against the Darkness: Enhancing the Resilience of the Electricity Grid through Microgrid Facilities." *IEEE Electrification Magazine* 4 (Mar): 18–24. doi:10.1109/MELE.2015.2509879.

Hofmann, M., G. Kjølle, and O. Gjerde. 2012. "Development of Indicators to Monitor Vulnerabilities in Power Systems." In *2012 International Conference on Probabilistic Safety Assessment and Management*, Stockholm, Sweden, 1–10.

Hu, Z., and X. Li, 2016. "The Degree of Coupling Analysis Method Based on Current Injection," in *2016 International Symposium on Fundamentals of Electrical Engineering*, Bucharest, Romania, 1–4.

IEEE 24-bus Test System. Accessed 20 June 2020. https://electricgrids.engr.tamu.edu/electric-grid-test-cases/ieee-24-bus-system/

Kerin, U., G. Bizjak, E. Lerch, O. Ruhle, and R. Krebs. 2009. "Faster than Real Time: Dynamic Security Assessment for Foresighted Control Action." *IEEE Bucharest PowerTech, Bucharest, Romania,* 1–7.

Kjølle, G., O. Gjerde, and A. Nybø. 2010. "A Framework for Handling High Impact Low Probability (HILP) Events." In *2010 CIRED Workshop*, Lyon, France, 1–4.

Li, C., Q. Shu, Z. Chen, and C. L. Bak. 2012. "Vulnerability Evaluation of Power System Integrated with Large-scale Distributed Generation Based on Complex Network Theory." In *2012 International Universities Power Engineering Conference*, Uxbridge, UK, 1–5.

Li, Z., M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki. 2017. "Networked Microgrids for Enhancing the Power System Resilience." *Proceedings of the IEEE* 105 (Jul): 1289–1310. doi:10.1109/JPROC.2017.2685558.

Maliszewski, P. J., and C. Perrings. 2012. "Factors in the Resilience of Electrical Power Distribution Infrastructures." *Applied Geography* 32 (Mar): 668–679. doi:10.1016/j.apgeog.2011.08.001.

Manshadi, S. D., and M. E. Khodayar. 2015. "Resilient Operation of Multiple Energy Carrier Microgrids." *IEEE Transactions Smart Grid* 6 (Sep): 2283–2292. doi:10.1109/TSG.2015.2397318.

McGillis, D., K. El-Arroudi, R. Brearley, and G. Joos, 2006. "The Process of System Collapse Based on Areas of Vulnerability." In *2006 Large Engineering Systems Conference on Power Engineering*, Halifax, NS, Canada,35–40.

McManus, S., E. Seville, D. Brunsdon, and J. Vargo. 2007. "Resilience Management: A Framework for Assessing and Improving the Resilience of Organizations." *Resilient Organizations Research Report* 1 (Jan): 1–79.

Nasiruzzaman, A. B. M., H. R. Pota, and M. N. Akter. 2014. "Vulnerability of the Large-scale Future Smart Electric Power Grid." *Physica A: Statistical Mechanics and Its Applications* 413 (Jun): 11–24. doi:10.1016/j.physa.2014.06.024.

Orencio, P. M., and M. Fujii. 2013. "A Localized Disaster-resilience Index to Assess Coastal Communities Based on an Analytic Hierarchy Process (AHP)." *International Journal of Disaster Risk Reduction* 3 (Mar): 62–75. doi:10.1016/j.ijdrr.2012.11.006.

Panteli, M., and P. Mancarella, 2015a. "The Grid: Stronger, Bigger, Smarter? Presenting a Conceptual Framework of Power System Resilience," *IEEE Power and Energy Magazine* 13: 58–66, May-Jun.

Panteli, M., and P. Mancarella. 2015b. "Influence of Extreme Weather and Climate Change on the Resilience of Power Systems: Impacts and Possible Mitigation Strategies." *Electric Power Systems Research* 127 (Oct): 259–270. doi:10.1016/j.epsr.2015.06.012.

Proag, V., 2014. "The Concept of Vulnerability and Resilience." In *2014 International Conference on Building Resilience*, Salford Quays, UK, 369–376.

Reed, D. A., K. C. Kapur, and R. D. Christie. 2009. "Methodology for Assessing the Resilience of Networked Infrastructure." *IEEE Systems Journal* 3 (Jun): 174–180. doi:10.1109/JSYST.2009.2017396.

Roege, P. E., Z. A. Collier, J. Mancillas, J. A. McDonagh, and I. Linkov. 2014. "Metrics for Energy Resilience." *Energy Policy* 72 (Sep): 249–256. doi:10.1016/j.enpol.2014.04.012.

Schneider, K. P., F. K. Tuffner; M. A. Elizondo, C. Liu, Y. Xu, and D. Ton. 2016. Evaluating the Feasibility to Use Microgrids as a Resiliency Resource. *IEEE Transactions Smart Grid* 8: 687–696. Mar.

Shahzad, U. 2020. "Significance of Smart Grids in Electric Power Systems: A Brief Overview." *Journal of Electrical Engineering, Electronics, Control and Computer Science* 6: 7–12.

Shahzad, U., and S. Asgarpoor, "Probabilistic Evaluation of Line Loading and Line Active Power in an Active Distribution Network Using Numerical and Analytical Approaches." *2018 North American Power Symposium (NAPS)*, Fargo, ND, 2018, pp. 1–6.

Shahzad, U., and S. Asgarpoor. 2019. "Probabilistic Risk Assessment of an Active Distribution Network Using Monte Carlo Simulation Approach." *2019 North American Power Symposium (NAPS)*, Wichita, KS, USA, 1–6.

Shinozuka, M., S. E. Chang, T. Cheng, M. Feng, T. D. O'Rourke, M. Saadeghvaziri, X. Dong, X. Jin, Y. Wang, and P. Shi 2003. "Resilience of Integrated Power and Water Systems." In *2003 Proceedings of Seismic Evaluation and Retrofit of Lifeline Systems*, Buffalo, NY, USA. 65–86.

Soonee, S. K., S. C. Saxena, K. V. S. Baba, S. R. Narasimhan, K. V. N. P. Kumar, and S. Mukhopadhyay. 2018. "Grid Resilience in Indian Power System." *2018 IEEE 8th Power India International Conference (PIICON)*, Kurukshetra, India, 1–6.

Tabatabaei, N. M., S. N. Ravadanegh, and N. Bizon. 2018. *Power Systems Resilience*. Switzerland: Springer.

Trakas, D. N., N. D. Hatziargyriou, M. Pantelli, and P. Mancarella, 2016. "A Severity Risk Index for High Impact Low Probability Events in Transmission Systems Due to Extreme Weather." In *2016 IEEE PES Innovative Smart Grid Technologies Conference Europe*, Ljubljana, Slovenia,1–6.

Wang, K., B. Zhang, Z. Zhang, X. Yin, and B. Wang. 2011. "An Electrical Betweenness Approach for Vulnerability Assessment of Power Grids considering the Capacity of Generators and Load." *Physica A: Statistical Mechanics and Its Applications* 390 (Nov): 4692–4701. doi:10.1016/j.physa.2011.07.031.

Wang, Y., C. Chen, J. Wang, and R. Baldick. 2016. "Research on Resilience of Power Systems under Natural disasters—A Review." *IEEE Transactions on Power Systems* 31 (Mar): 1604–1613. doi:10.1109/TPWRS.2015.2429656.

Watson, J., R. Guttromson, C. Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley, and L. Walker. et al., 2015. "Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States." Tech. Rep. SAND 2014-18019, September. Albuquerque, NM, USA: Sandia National Laboratory.

Wei, X., J. Zhao, T. Huang, and E Bompard. 2018. ""A Novel Cascading Faults Graph Based Transmission Network Vulnerability Assessment Method." *IEEE Transactions on Power Systems* 33 (3, May): 2995–3000. doi:10.1109/TPWRS.2017.2759782.

Wenli, F., L. Zhigang, H. Ping, and M. Shengwei. 2016. "Cascading Failure Model in Power Grids Using the Complex Network Theory." *IET Generation, Transmission & Distribution* 10 (Nov): 3940–3949. doi:10.1049/iet-gtd.2016.0692.

Whitson, J. C., and J. E. Ramirez-Marquez. 2009. "Resiliency as a Component Importance Measure in Network Reliability." *Reliability Engineering and System Safety* 94 (Oct): 1685–1693. doi:10.1016/j.ress.2009.05.001.