Journal of Electrical Engineering, Electronics, Control and Computer Science – JEEECCS, Volume 7, Issue 26, pages 17-24, 2021

Vulnerability Assessment in Power Systems: A Review

Umair Shahzad
Department of Electrical and Computer Engineering,
University of Nebraska-Lincoln,
Lincoln, NE, USA
umair.shahzad@huskers.unl.edu

Abstract – **Power systems are one of the most multifaceted systems and have a large significance in present society. For stable and continuous operation of such systems, numerous protection methods are compulsory. Although, modern power systems are fortified with numerous protection schemes with the goal of evading the unexpected events, they are still impacted by various emergency and mal-operation conditions. The most severe disturbances put the entire or at least a part of the network at the risk of blackout. If the emergency is not dealt with timely and accurately, the power system is probable to have cascading failures, which ultimately lead to a blackout. Due to the severe impacts, many nations around the world have research teams whose main task is to circumvent blackouts on their systems. Moreover, due to ecological concerns and expensive system expansion, power systems generally operate closer to their limits, which upsurges their vulnerability and possibility of blackouts. With the continuous development of power systems, rise in grid intricacy, and the drift towards deregulated market, vulnerability assessment is critical. It is of great significance to include vulnerability in power system planning and operating procedures, as it is the key to accurate assessment of power system security and stability. Thus, this paper aims to review the concept of vulnerability assessment in power systems and the associated research. This review can be a great starting point for researchers in the domain of power system security and vulnerability.**

Keywords-Blackout; cascading failure; security; stability; vulnerability

I. Introduction

The power system is one of the most critical infrastructures of society, and therefore, any failure to this system can drastically impact the security of the associated consumers. Numerous systems such as transportation, education, trade, banking, etc., heavily rely on reliable and continuous operation of power systems. Regrettably, the unforeseen climate changes and alarming number of natural disasters may radically increase the vulnerability of power systems, causing substantial outages, thereby disrupting power supply to critical loads for days and sometimes for weeks [1]. During the years 2003 to 2012, severe weather-related events contributed to roughly 58% outages in the USA, which is estimated to have an average burden of 18-33 billion $ annually to the economy of USA [2]. The swelling dependency on power systems coupled with an increased number of natural disasters has drawn the attention of both the research community and industry to reduce the system vulnerability [3-6]. One of the stimulating difficulties faced by power system operators nowadays is enhancing the vulnerability level in the system.

Recently, various natural disasters and deliberate human attacks have caused unparalleled challenges for power systems, which emphasizes 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 aging energy infrastructure. Thus, it is imperative that power systems can endure events with huge negative impact. Therefore, it is important to define and debate the concepts of vulnerability in relation to electric power systems.

The rest of the paper is organized as follows. Section II discusses about power system vulnerability. Section III presents a review of major works related to vulnerability assessment in power systems, Section IV mentions some significant research gaps. Finally, Section V concludes the paper with a proposed direction for future research.

II. Power System Vulnerability

Power system vulnerability does not have a standard definition, but [7] 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 high impact low probability (HILP) events [8]. Generally, these events are a result of weather- related hazards, such as snowstorms, landslides, tornadoes, and floods [9]. Reference [10] 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 [11] describes the notion of vulnerability connecting the system security level with the inclination to alter its operating conditions to a critical state, which [12] calls the “Verge of Collapse” state. Similarly, [13] 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.". In a nutshell, the main aim of vulnerability assessment is to determine the ability of a power system to continue to provide service when an unexpected catastrophic contingency occurs.

The vulnerability of power systems can be categorized into five broad dimensions to formulate a generic background for vulnerability assessment [14-15]. These dimensions are: threat/hazard, exposure, susceptibility, coping capacity, and criticality. Using these dimensions, a generic vulnerability framework can be formulated, as shown in Fig. 1.

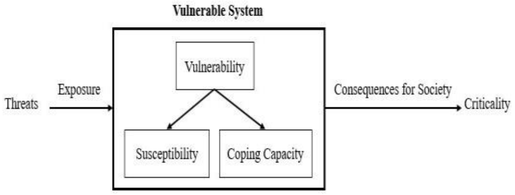


Fig. 1. General vulnerability framework

Threats and hazards are often used interchangeably, since hazards are included in threats. According to [13], 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 Fig. 1, system vulnerability is categorized 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 [15], 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, minimize 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 [15]. Reference [16] uses the conventional bow-tie approach to describe the concept of vulnerability in power systems, as shown in Fig. 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 Fig. 2, various barriers (labeled 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.

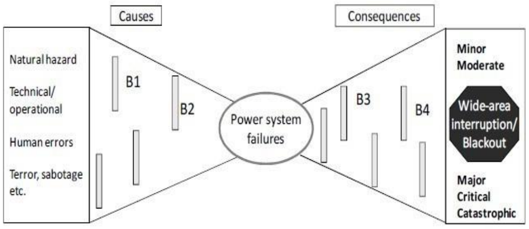


Fig. 2. Threats, unwanted event, consequences, and barriers

According to [17], power system vulnerability indices can be divided into two main classes: operational and non- operational. These are outlined in Fig. 3.

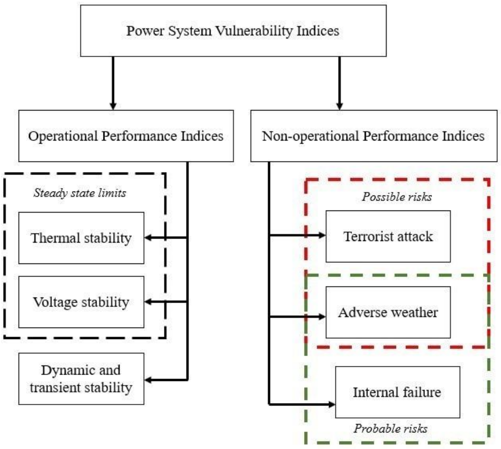

Power System Vulnerability Indices
Operational Performance Indices
Non-operational Performance Indices
Steady state limits
Thermal stability
Voltage stability
Dynamic and transient stability
Possible risks
Terrorist attack
Adverse weather
Internal failure
Probable risks

Fig. 3. Power system vulnerability indices

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 [17].

Power system vulnerability should be quantified using appropriate indictors or indices. The conceptual procedure for developing these indices is shown in Fig. 4 [15]. 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 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.

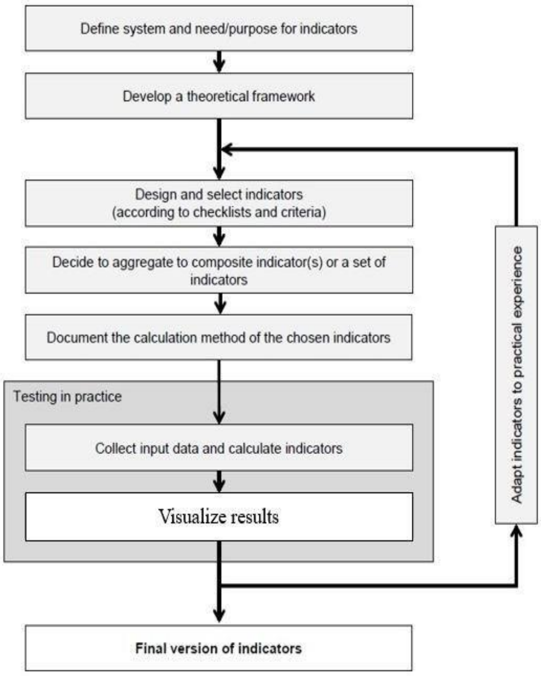

Define system and need/purpose for indicators
Develop a theoretical framework
Design and select indicators (according to checklists and criteria)
Decide to aggregate to composite indicator(s) or a set of indicators
Document the calculation method of the chosen indicators
Testing in practice
Collect input data and calculate indicators
Visualize results
Adapt indicators to practical experience
Final version of indicators

Fig. 4. Procedure for development of vulnerability indicators

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 analyze 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 visualization 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 [18].

III. Literature Review

The method proposed in [19] evaluated voltage stability status efficiently in both pre-contingency and post contingency states using two outstanding techniques, adapting the continuation method and the local analysis of contingency effect. The suggested approach was also able to determine vulnerable buses of the power system from the viewpoint of voltage security by determining the best candidates for the start point of the voltage collapse phenomenon. Results of testing the proposed techniques on two practical systems confirmed the validity of established approaches.

Reference [20] proposed a scheme to study power system vulnerability considering the failures of protection system. The power system vulnerability was assessed by adequacy indices, such as Bus Isolation Probability (BIP), Loss of Load Probability (LOLP) and Expected Power Loss (EPL), and the security index Probability of Stability (POS). A novel vulnerability index, Integrated System Vulnerability (ISV), was also presented to provide comprehensive description of the network vulnerability.

In [21], two new vulnerability evaluation approaches were proposed. One is based on the distance of the current operating point from the vulnerability border of the system. The other is based on the anticipated loss of load. These two methods are fully applicable to cascading events. The proposed method was tested on the WSCC 179 bus test system. A comprehensive procedure was developed in [22] for assessing power system vulnerability with respect to energy shortage, capacity shortage, and power system failures. The goal was to identify medium- and high-risk situations that necessitate corrective actions. The Nordic power system was used for conducting simulations. The results indicated that the system is in a medium-risk state, suggesting the need to consider numerous measures.

Reference [23] attempted to assess the effect of line outage, generation outage and amount of load disconnected on the transmission network losses of a large size power system. These were evaluated using vulnerability index of power system loss. The goals of this work were to assess and compare the efficiency of the proposed vulnerability index in assessing the vulnerability of a large size power system with other known vulnerability indices based on anticipated loss of load and generation vulnerability index. Reference [24] presented a novel index to determine the vulnerability of a power system. The process combined stochastic and probabilistic methods to determine the likelihood of a line overloading in a power system. A case study was performed to examine the ability of such an index in computing operational aspect of power system vulnerability.

Reference [25] described a framework for vulnerability analysis including extraordinary events in power systems. The framework was based on a bow-tie structure and identified threats, unwanted events, barriers, and penalties. The results indicated that one of the most stimulating parts of a vulnerability analysis is the identification of the vulnerable operational states and extraordinary events. An extended topological technique was suggested in [26] by incorporating several electrical features, such as electrical distance, power transfer distribution, and line flow limits, into the pure topological metrics. The paper defined an extended betweenness centrality which considers the features of power grids and can measure the local importance of the components in power grids. The results demonstrated that the extended betweenness is superior to topological betweenness in the identification of critical elements in power grids.

Reference [27] presented a novel method for measuring vulnerability of a power system. For attaining this goal, several indices, that replicate the health of the system, were calculated. The indices allow assessing four different symptoms of system stress such as voltage instability, poorly damped power oscillations, frequency deviations outside limits, and overloads. The procedure was tested on the IEEE New England test system using time domain simulations. The results showed that vulnerability starts to develop in a specific region of the network, thereby, its evaluation can be used to coordinate control actions that alleviate the penalties of the disturbances and decrease the risk of cascading events. A vulnerability assessment was suggested in [28] to calculate the impact factors for power systems based on generator and line outages. A Bus Impact Severity (BIS) analysis was then designed and used to determine the vulnerable buses. The buses with larger BIS values can be considered as the better locations for ESS (energy storage system) placement. Test results showed that the ESS placement in the vulnerable buses can effectively alleviate system vulnerability.

In [29], the static strategy, dynamic strategy, and space-pruning searching strategy were presented for more effectively identifying the critical lines in the multiple line attack scenarios. Moreover, the optimal selection of critical lines in the multiple lines attack was determined, based on the criticality of the lines. The efficacy of the suggested attack strategies was tested using three different bulk IEEE test systems. In [30], a model based on risk-based decision-making process was proposed for extreme weather events. The presented method was tested on the IEEE 118-bus system. According to the simulation results obtained, the suggested risk-based model is a flexible decision-making tool, which can help decision makers make a tradeoff between economy and security.

In [31], an Optimal Performance Index (OPI) was presented considering the real and reactive power output from distributed generation (DG) units. This suggested OPI considered multi-objective indices, namely real and reactive power loss, fault current and voltage, voltage deviation, harmonic distortion, vulnerability for DG and bus with Vulnerability Index (VI). The test system was modeled as a directed graph network formed using power flow method in Backward-Forward-Sweep algorithm. The topological significance of each node was derived from betweenness centrality to represent the weights. The results were analyzed to validate the presented model using OPAL-RT 5600 Real-time digital Simulator in MATLAB/Simulink environment.

A method to identify vulnerable lines based on the weighted entropy analysis technique was presented in [32]. In this method, an assessment index, namely the incremental power flow entropy, was first developed, which was used to define impacts caused by variation of the lines' capability of carrying power flow transfers on the vulnerability of the lines themselves at the same aggregation level. A second assessment index, namely structural importance, described the structural changes of a power grid that are caused by the integration of wind generation. Reference [33] proposed a mathematical model based on graph theory notions to quantify the criticality of transmission lines and substations. The capabilities and effectiveness of the topological characterization was demonstrated using the IEEE 39-bus network. These results provided useful intuitions on the association between critical sets of transmission lines and critical substations.

In [34], a mixed optimal power flow (OPF) stochastic approach was proposed to simulate cascading failures in a power system and to assess the impact of wind generation in terms of its penetration and uncertainty level. The presented method combined both thermal stability model for transmission line outage and power balance algorithms. Numerical simulation results on the IEEE 300 bus system indicated that uncertainty of wind energy has severe influences on grid vulnerability in terms of cascading overload failures under different contingency scenarios. Results also suggested that higher penetration levels of wind energy, if not controlled suitably, will upsurge this severity because higher uncertainties may be injected into weaker lines in a grid. Reference [35] discussed the vulnerability analysis and identification of key nodes in power grids from the viewpoint of complex network. Based on the AC Power Flow (PF) model and the network topology weighted with admittance, the cascading failure model was formed first. The node electrical centrality was further elaborated, using complex network centrality theory, to classify the key nodes in the network. To efficiently examine the behavior and verify the correctness of node electrical centrality, the net-ability and vulnerability index were introduced to define the transfer ability and performance under normal operation and consequently, assess the vulnerability of the power system under cascading failures, respectively. Simulation results of IEEE 30-bus and IEEE 57-bus test cases showed that the key nodes can be efficiently recognized with high electrical centrality, verifying the effectiveness of the analysis.

Reference [36] proposed a maximum flow-based complex network method to classify the critical lines in a system. The presented approach consists of two main steps. First, the power network was modeled as a graph with edges (transmission lines, transformers, etc.) and nodes (buses, substations, etc.). The critical scenarios were recognized using the principal component analysis and convex hull. In the second step, an improved maximum flow-based complex network method was used for topology analysis. The proposed approach was validated using the western Danish power system. Consequently, the vulnerable lines in the network were ranked. Simulation results demonstrated the effectiveness of the approach by intentional attacks and comparison with the planning strategy from the system operator. In [37], the vulnerability assessment was conducted using two different indices: active power performance index and voltage performance index. These indices provide a means of comparing the relative severity of the different line outages on the system loads and voltage profiles. It was found that the most severe line outages are those lines that interconnect the high load centered with the rest of the regional power systems. Moreover, the most vulnerable buses of the network in respect of voltage limit violations were majorly found at the high load centers.

Reference [38] proposed a bilevel optimization-based model to assess the vulnerability of a power system, which is geographic-cyber interdependent with communication network. The presented research modeled simultaneous physical attacks on the power system and communication network, while considering the effects of communication network disruption on the corrective actions taken by the power system operator. Numerical results showed that the vulnerability of a power system under physical attacks likely upsurges when considering the geographic-cyber interdependence. Based on the equal area criterion, [39] proposed the weak line vulnerability index of a two-area grid connected by multiple lines in parallel or in series. Using the index, the weak lines can be identified and the failures with the most serious effect on them can be determined. Simulation analysis of actual power grid examples verified the effectiveness of the proposed indicators.

Reference [40] demonstrated that power systems increase their vulnerability against cascading failure events when they are weakly interconnected, such as by a single power line. In these cases, the results obtained indicated that it is better to interconnect isolated systems with at least two or more transmission lines. To validate this, the IEEE 24-bus RTS test system network was used. The results obtained can aid in comprehending the vulnerability of interconnected power systems. In [41], grid vulnerability identification was conducted by combined use of grid network topology and centrality measures along with real and physical characteristics of power grid. The presented approach was validated by execution over a section of Iranian 400 kV and 230 kV power grids. The accuracy of the results obtained was confirmed by comparison against results that obtained through computations by Iran’s national dispatching body.

In [42], a method for vulnerable node identification was suggested based on dynamic regional electrical coupling. Considering mutual impact of operational states of the nodes, regional electrical coupling, and interdependency relations between nodes were adopted to reflect the ability of the node to affect the transient stability of its neighboring nodes. Also, a coupling algorithm was suggested to recognize the vulnerable nodes that will decline the system stability most when they fail. Reference [43] proposed an adjacent graph based on the spontaneous faults of an electrical network to evaluate the electrical network vulnerabilities from the standpoint of the overload mechanism. Fault probability, load shedding, and topological structure-based indices were presented to define the weights of the directed edges in the adjacent graph. Based on the physical features of the graph mapped to the electrical network, the improved betweenness based on the complex network theory was suggested to recognize the critical branches of the electrical network. Numerical results on an IEEE 118-bus system demonstrated the efficiency of the proposed technique.

The hidden geometry of current flow path was proposed in [44] for analysis of vulnerability in power system. Various metrics were defined to measure the impact of line tripping on load flow and identified the critical line in a perturbed grid. The presented method allows to focus on the power grid vulnerable areas and can help the control system operator to examine the variations in power flow on transmission lines and execute the essential corrective actions. In [45], a vulnerability assessment method was presented based on total power system loss which considered power generation loss due to generation outage, power line loss due to line outage, increase in total load and amount of load disconnected. The aim of this study was to examine the effectiveness of the presented technique in assessing the vulnerability of power system when subjected to various contingencies.

Reference [46] attempted to conduct a more accurate approach of urban power grid vulnerability assessment. To achieve this, firstly, the evaluation index system was conducted through four aspects: composition of power supply, grid structure, grid operation and important power transmission channel. Secondly, the basic indices and their weights were determined through artificial neural network (ANN) evaluation method. Lastly, the input data were nondimensionalized and the evaluation index system was formed. The objective of [47] was to create a methodological basis for vulnerability analysis that is complementary to traditional risk and reliability analysis of power systems. It presented a comprehensive framework of definitions, indicators and approaches that can be used to classify, analyze and monitor vulnerabilities in power transmission and distribution networks.

IV. Research Gaps

From the extensive literature review of major works in power system vulnerability, the following gaps were identified. Firstly, there is a lack of a generalized vulnerability index. Several indices have been proposed in the literature. However, most of them offer ranking methods based on some performance indices which consider bus voltages, active and reactive powers of generating units, and transmission lines. Also, in some references, effective vulnerability mitigation approaches focused on ensuring resiliency and reliability of the grid, are mandatory [6]. To the best of author’s knowledge, there is a lack of a generalized index for both steady state and dynamic vulnerability assessment. There is a lack of precise information about how vulnerable an element is following a contingency while vulnerability assessment is done for all generating units, transmission lines, and buses. Any proposed index must consider a wider range of operation to cover both dynamic and steady-state security regions [6].

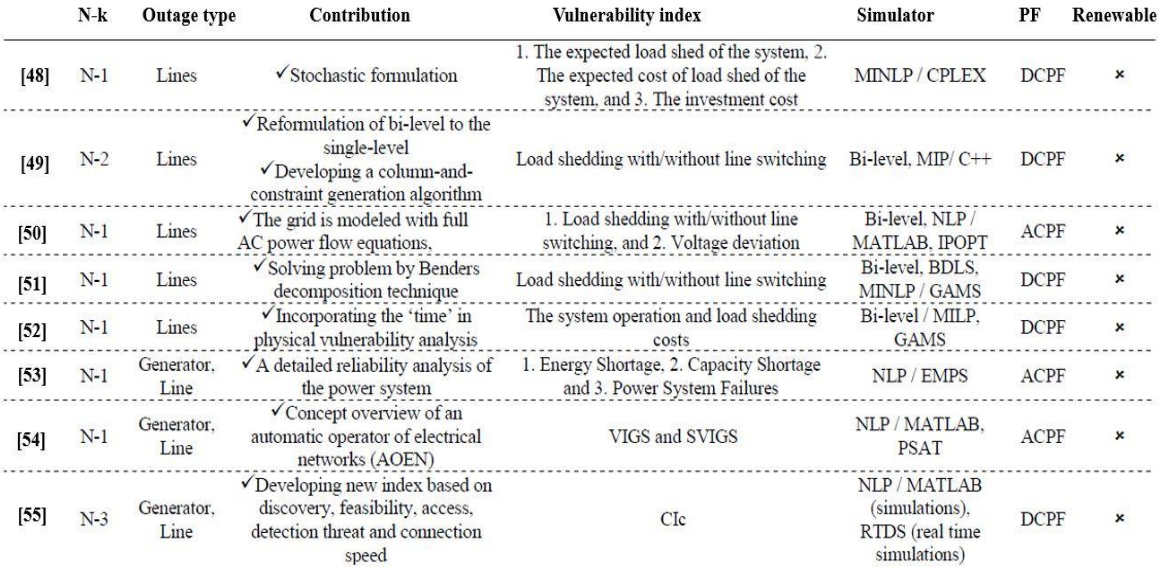
No standard metrics exist for vulnerability assessment. Most of proposed metrics often underestimate the consequences of high impact events and deal majorly with normal operating scenarios, i.e., these metrics cannot entirely address the impacts caused by cyber-attacks and extreme weather events.

Although modeling extreme events, especially weather-related events, have been under widespread research and development, there are still numerous research gaps that need further research. First, in most of the available weather-related forecasting methods, numerous assumptions have been made which reduces the accuracy of results' accuracy. The meteorological data used in forecasting weather-related events depend on local historic datasets capturing the propagation of a single event in a specific geographical location.

Facing the increasing penetration of distributed energy resources (DERs) in the emerging power systems, the uncertain nature of these energy resources should be properly handled in vulnerability assessment. Based on Table I, current references ignore DERs and their volatile nature in vulnerability analysis.

Moreover, nearly all works focus only on a specific aspect (operational failures, weather impact, cyber attack, natural disaster, etc.) of vulnerability. There is a need to formulate an integrated framework for power system vulnerability which considers more than one variable. Thus, it is important to model and include these variables, in addition to operational failures, while assessing power system vulnerability.

TABLE I. SUMMARY OF RECENT RESEARCH ON STATIC/DYNAMIC VULNERABILITY ASSESSMENT



	N-k	Outage type	Contribution	Vulnerability index	Simulator	PF	Renewable
[48]	N-1	Lines	✓Stochastic formulation	1. The expected load shed of the system, 2. The expected cost of load shed of the system, and 3. The investment cost	MINLP / CPLEX	DCPF	×
[49]	N-2	Lines	✓Reformulation of bi-level to the single-level ✓Developing a column-and-constraint generation algorithm	Load shedding with/without line switching	Bi-level, MIP/ C++	DCPF	×
[50]	N-1	Lines	✓The grid is modeled with full AC power flow equations,	1. Load shedding with/without line switching, and 2. Voltage deviation	Bi-level, NLP / MATLAB, IPOPT	ACPF	×
[51]	N-1	Lines	✓Solving problem by Benders decomposition technique	Load shedding with/without line switching	Bi-level, BDLS, MINLP / GAMS	DCPF	×
[52]	N-1	Lines	✓Incorporating the 'time' in physical vulnerability analysis	The system operation and load shedding costs	Bi-level / MILP, GAMS	DCPF	×
[53]	N-1	Generator, Line	✓A detailed reliability analysis of the power system	1. Energy Shortage, 2. Capacity Shortage and 3. Power System Failures	NLP / EMPS	ACPF	×
[54]	N-1	Generator, Line	✓Concept overview of an automatic operator of electrical networks (AOEN)	VIGS and SVIGS	NLP / MATLAB, PSAT	ACPF	×
[55]	N-3	Generator, Line	✓Developing new index based on discovery, feasibility, access, detection threat and connection speed	CIc	NLP / MATLAB (simulations), RTDS (real time simulations)	DCPF	×

This study reviewed some major works in vulnerability assessment. This can be an exceptional starting point for researchers in the field of power system security. Recent research [56-63] indicates that the full potential of vulnerability analysis is yet to be utilized in modern power systems.

V. CONCLUSION AND FUTURE WORK

The power system is a cornerstone of modern society. Efficient operation of power system is the key to providing power to consumers at all times. However, vulnerability has also been brought in to the picture in recent years. Therefore, a great effort is necessary to deeply understand the vulnerability, to protect the power systems from various unwanted events and threats. Therefore, this paper reviewed some pertinent literature in this regard, and consequently, pointed out some research gaps.

There are various challenges in assessing the vulnerability of a power system. One of the main challenges, which remains to be unraveled, is how power systems can accurately predict and adapt to the approaching extreme events. The expansion of innovative technologies, frameworks, and strategies constitute a significant step toward a less vulnerable power system in the face of a changing natural, social, and economic environment with uncertain and incompletely understood influences.

This paper provides the foundation for a more comprehensive research roadmap to reduce power system vulnerability. Research on power system vulnerability is just the tip of iceberg. Extreme events will always be a daunting challenge to power system researchers. Thus, as a future work, it is important to research and devise reasonable solutions to these challenges. It is believed that this review would provide a good starting point for any research in the domain of power system security and stability, and would certainly be helpful for further research in the significant area of power system planning under security constraints.

REFERENCES

[1] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Transactions on Power Systems,* vol. 31, no. 2, pp. 1604-1613, 2016.

[2] W. House, "Economic benefits of increasing electric grid resilience to weather outages," *Washington, DC: Executive Office of the President,* 2013.

[3] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electric Power Systems Research,* vol.127, pp. 259-270, 2015.

[4] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," *IEEE Transactions on Smart Grid,* vol. 7, no. 2, pp. 958-966, 2016.

[5] H. Gao, Y. Chen, Y. Xu, and C.-C. Liu, “Resilience-oriented critical load restoration using microgrids in distribution systems,” *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2837-2848, 2016.

[6] S. M. Mohseni-Bonab, I. Kamwa, A. Moeini and A. Rabiee, “Vulnerability Assessment in Power Systems: A Review and Representing Novel Perspectives,” *IEEE Power & Energy Society General Meeting (PESGM)*, 2020, pp. 1-5.

[7] G. L. Doorman, K. Uhlen, G. H. Kjolle, and E. S. Huse, “Vulnerability analysis of the Nordic Power System,” *IEEE Transactions on Power Systems*, vol. 21, pp. 402-410, Feb. 2006.

[8] D. N. Trakas, N. D. Hatziargyriou, M. Pantelli, and P. Mancarella, “A severity risk index for high impact low probability events in transmission systems due to extreme weather,” *IEEE PES Innovative Smart Grid Technologies Conference*, 2016, pp. 1-6.

[9] E. Bompard, E. Pons, and D. Wu, “Extended topological metrics for the analysis of power grid vulnerability,” *IEEE Systems Journal*, vol. 6, pp. 481- 487, Sep. 2012.

[10] R. Baldick et al., “Vulnerability assessment for cascading failures in electric power systems,” *IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1-9.

[11] A. Fouad, Q. Zhou, and V. Vittal, “System vulnerability as a concept to assess power system dynamic security,” *IEEE Transactions on Power Systems*, vol. 9, pp. 1009-1015, May 1994.

[12] D. McGillis, K. El-Arroudi, R. Brearley, and G. Joos, “The process of system collapse based on areas of vulnerability,” *Large Engineering Systems Conference on Power Engineering*, 2006, pp. 35 – 40.

[13] V. Proag, “The concept of vulnerability and resilience,” *International Conference on Building Resilience*, 2014, pp. 369-376.

[14] A. Abedia, L. Gaudard, and F. Romerio, “Review of major approaches to analyze vulnerability in power system,” *Reliability Engineering and System Safety*, vol. 183, pp. 153-172, Mar. 2019.

[15] M. Hofmann, G. Kjølle, and O. Gjerde, “Development of indicators to monitor vulnerabilities in power systems,” *International Conference on Probabilistic Safety Assessment and Management*, 2012, pp. 1-10.

[16] G. Kjølle, O. Gjerde, and A. Nybø, “A framework for handling high impact low probability (HILP) events,” *CIRED Workshop*, 2010, pp. 1-4.

[17] E. Akdeniz and M. Bagriyanik, “A knowledge based decision support algorithm for power transmission system vulnerability impact reduction,” *Electrical Power and Energy Systems*, vol. 78, pp. 436-444, Jun. 2016.

[18] X. Wei, J. Zhao, T. Huang, and E, Bompard, “A novel cascading faults graph based transmission network vulnerability assessment method,” *IEEE Transactions on Power Systems*, vol. 33, pp. 2995-3000, May 2018.

[19] N. Amjady, “Voltage security assessment and vulnerable bus ranking of power systems,” *Electric Power Systems Research*, vol. 64, no. 3, pp. 227-237, Mar. 2003.

[20] X. Yu and C. Singh, “A practical approach for integrated power system vulnerability analysis with protection failures,” *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1811-1820, Nov. 2004.

[21] M. Kim, “Vulnerability indices for power systems,” Proceedings of the 13th International Conference on Intelligent Systems Application to Power Systems, 2005, pp. 1-7.

[22] G. L. Doorman, K. Uhlen, G. H. Kjolle, and E. S. Huse, “Vulnerability analysis of the Nordic Power System,” *IEEE Transactions on Power Systems*, vol. 21, pp. 402-410, Feb. 2006.

[23] A. M. Haidar and A. Hussain, “Vulnerability assessment of a large sized power system considering a new index based on power system loss,” *European Journal of Scientific Research*, vol. 17, no. 1, pp. 61-72, 2007.

[24] J. Rossmaeir, “Development of a new system vulnerability index – the overload risk index,” *40th North American Power Symposium*, 2008, pp. 1-8.

[25] O. Gjerde, “Risk and vulnerability analysis of power systems including extraordinary events,” *IEEE Trondheim Power Tech*, 2011, pp. 1-5.

[26] E. Bompard, E. Pons and D. Wu, “Extended topological metrics for the analysis of power grid vulnerability,” *IEEE Systems Journal*, vol. 6, no. 3, pp. 481-487, Sep. 2012.

[27] J. Cepeda, “Vulnerability assessment of electric power systems through identification and ranking of vulnerable areas,” *International Journal of Emerging Electric Power Systems*, vol. 13, no. 1, pp. 1-23, 2012.

[28] J. Teng, “Power system vulnerability assessment considering energy storage systems,” *IEEE 10th International Conference on Power Electronics and Drive Systems (PEDS*), 2013, pp. 1-5.

[29] M. Wang, “Critical line identification for hypothesized multiple line attacks against power systems”, *IEEE/PES Transmission and Distribution Conference and Exposition (T&D*), 2016, pp. 1-5.

[30] J. Qiu, “A probabilistic transmission planning framework for reducing network vulnerability to extreme events,” *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3829-3839, Sep. 2016.

[31] K.Sarkar, “Optimal location for single and multiple DG based on vulnerability index in smart distribution system, *IEEE Power & Energy Society General Meeting*, 2017, pp. 1-5.

[32] R. Fang, “Identification of vulnerable lines in power grids with wind power integration based on a weighted entropy analysis method,” *International Journal of Hydrogen Energy*, vol. 42, no. 31, pp. 20269-20276, Aug. 2017.

[33] R. Moreno, “Identification of topological vulnerabilities for power systems networks,” *IEEE Power & Energy Society General Meeting (PESGM)*, 2018, pp. 1-5.

[34] M. H. Athari and Z. Wang, “Impacts of wind power uncertainty on grid vulnerability to cascading overload failures,” *IEEE Transactions on Sustainable Energy*, vol. 9, no. 1, pp. 128-137, Jan. 2018.

[35] B. Liu, Z. Li, X. Chen, Y. Huang and X. Liu, “Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 3, pp. 346-350, Mar. 2018.

[36] J. Fang, C. Su, Z. Chen, H. Sun and P. Lund, “Power system structural vulnerability assessment based on an improved maximum flow approach,” *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 777-785, Mar. 2018.

[37] M. A. Tekuneh, “Identification of system vulnerabilities in the Ethiopian electric power system,” *Global Energy Interconnection*, vol. 1, no. 3, Aug. 2018.

[38] M. Zeerati, “Vulnerability analysis of power systems under physical deliberate attacks considering geographic-cyber interdependence of the power system and communication network,” *IEEE Systems* Journal, vol. 12, no. 4, Dec. 2018.

[39] Y. Sun, “Study on the transmission line vulnerability index and its application based on the transient power angle stability mechanism,” *IEEE 2nd International Electrical and Energy Conference (CIEEC)*, 2018, pp. 434-439.

[40] J. Beyza, “Effect of interconnection lines on the vulnerability of power systems,” *IEEE Milan PowerTech*, 2019, pp. 1-6.

[41] A. Shahpari, “Vulnerability analysis of power grid with the network science approach based on actual grid characteristics: A case study in Iran,” *Physica A*, 2019.

[42] M. Zhou, “Vulnerability analysis of power system based on dynamic regional electrical coupling,” *International Transactions on Electr Energ Syst*ems, vol. 513, pp. 14-21, 2019.

[43] T. Zang, S. Gao, T. Huang, X. Wei and T. Wang, “Complex network-based transmission network vulnerability assessment using adjacent graphs,” *IEEE Systems Journal*, vol. 14, no. 1, pp. 572-581, Mar. 2020.

[44] S. Gupta, “Analysis and prediction of vulnerability in smart power transmission system: A geometrical approach,” *International Journal of Electrical Power & Energy Systems*, vol. 94, pp. 77-87, Jan. 2018.

[45] A. Haidar, “New method for vulnerability assessment of power system,” *journal of Applied Sciences*, vol. 7, no. 6, Jun. 2007.

[46] Y. Che, “Vulnerability assessment of urban power grid based on combination Evaluation,” *Safety Science*, vol. 113, pp. 144-153, Mar. 2019.

[47] I. Sperstad, “A comprehensive framework for vulnerability analysis of extraordinary events in power systems,” *Reliability Engineering & System Safety*, vol. 196, Apr. 2020.

[48] M. Carrión, J. M. Arroyo, and N. Alguacil, “Vulnerability-constrained transmission expansion planning: A stochastic programming approach,” *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1436-1445, 2007.

[49] L. Zhao and B. Zeng, “Vulnerability analysis of power grids with line switching,” *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2727-2736, 2013.

[50] T. Kim, S. J. Wright, D. Bienstock, and S. Harnett, “Analyzing vulnerability of power systems with continuous optimization formulations,” *IEEE Transactions on Network Science and Engineering*, vol. 3, no. 3, pp. 132-146, 2016.

[51] A. Delgadillo, J. M. Arroyo, and N. Alguacil, “Analysis of electric grid interdiction with line switching,” *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 633-641, 2010.

[52] S. Sayyadipour, G. R. Yousefi, and M. A. Latify, “Mid-term vulnerability analysis of power systems under intentional attacks,” *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3745-3755, 2016.

[53] G. L. Doorman, K. Uhlen, G. H. Kjolle, and E. S. Huse, “Vulnerability analysis of the Nordic Power System,” *IEEE Transactions on Power Systems*, vol. 21, pp. 402-410, Feb. 2006.

[54] L. Lenoir, I. Kamwa, and L.-A. Dessaint, “Overload alleviation with preventive-corrective static security using fuzzy logic,” *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 134-145, 2009.

[55] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U.Adhikari, “Modeling cyber-physical vulnerability of the smart grid within complete information,” *IEEE Transactions on Smart Grid*, vol. 4, no.1, pp. 235-244, 2013.

[56] A. Albarakati, “Modeling power systems vulnerability under targeted attacks considering hidden failures,” *SoutheastCon*, 2020, pp. 1-6.

[57] H. Pan, H. Lian, C. Na and X. Li, “Modeling and vulnerability analysis of cyber-physical power systems based on community theory,” *IEEE Systems Journal*, vol. 14, no. 3, pp. 3938-3948, Sep. 2020.

[58] W. Xu, “Vulnerability assessment of distributed load shedding algorithm for active distribution power system under denial of service attack,” *CSEE Journal of Power and Energy Systems*, Aug. 2020.

[59] R. S. Biswas, A. Pal, T. Werho, and V. Vittal, “A graph theoretic approach to power system vulnerability identification,” *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 923-935, Mar. 2021.

[60] U. Shahzad, “Significance of smart grids in electric power systems: a brief overview,” *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 6, no. 1, pp. 7-12, 2020.

[61] U. Shahzad, “Resilience in electric power systems,” *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, no. 2, pp. 1-6, 2021.

[62] U. Shahzad, “A review of challenges for security-constrained transmission expansion planning,” *Journal of Electrical Engineering, Electronics, Control and Computer Science*, vol. 7, no. 2, pp. 21-30, 2021.

[63] U. Shahzad, “The need for renewable energy sources,” *Information Technology and Electrical Engineering Journal*, vol. 4, pp. 16-18, Aug. 2015.