On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review

Shuva Paul, *Member, IEEE*, Fei Ding, *Senior Member, IEEE*, Kumar Utkarsh, *Member, IEEE*, Weijia Liu, *Member, IEEE*, Mark J. O'Malley, *Fellow, IEEE*, and John Barnett

***Abstract*—Power systems have been transformed into cyber-physical systems that integrate electric grids with advanced information technology and operational technology. To ensure reliable and resilient operations of such systems, it is important to understand the system vulnerability and quantify system resilience. This article provides an overview of existing work on vulnerability assessment and resilience quantification related to cyber-physical power systems, and it identifies research gaps and opportunities to enhance resilience. Specifically, we first review the definition and architecture of cyber-physical power systems, and then, summarize existing approaches to assess vulnerability and resilience. Later, we identify several research gaps that have not been well addressed yet and point out possible future work to fill the gap. Although this article focuses on cyber-physical power systems, the research can also benefit stakeholders of other critical infrastructures.**

***Index Terms*—Cyber-physical power systems, cybersecurity, resilience, resilience metrics, vulnerability, vulnerability metrics.**

I. Introduction

BOTH the frequency and intensity of power outages have been increasing in recent years. In the United States, approximately 3526 events were reported in 2017, affecting almost 36.7 million people [1]. Power outages are caused by different reasons, and weather is the one that has caused the majority [2]. In early March 2018, two back-to-back winter storms pummeled the East Coast. More than one million customers residing in New Jersey, New York, Massachusetts, and Connecticut were left without electricity after the second storm [3]. On the other hand, power systems have been transformed into cyber-physical systems that integrate electric grids with sensors, measurement devices, smart automation systems, industrial control systems, and communications devices. As interconnected networks of heterogeneous devices and elements, cyber-physical power systems (CPPSs) demonstrate advanced monitoring, communication, optimization, and control capabilities that are crucial for providing flexible, efficient, and reliable electricity to customers. The interconnectivity and complex nature of CPPSs, however, make them more exposed and vulnerable to threats. Besides of the vulnerability to extreme weather events, CPPSs depend on both information technology (IT) and operation technology (OT) systems, and thus, they are vulnerable to malicious cyber-physical attacks. The number of cyber threats per year, as shown in Fig. 1, has been increasing rapidly, and the energy sector has been recognized as one of the most critical infrastructures attracting the attentions of adversaries.

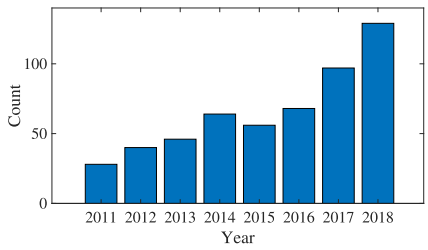

Fig. 1. Number of cybersecurity breaches disclosed per year [4].

Vulnerability can be considered as the measure of a system's weakness [5]. Resilience is the ability of a system to anticipate, prepare for, and adapt to changing conditions and to withstand, respond to, and recover rapidly from disruptions [6]. To mitigate the impact of power outages, it is indispensable to understand the vulnerability of the CPPS and to identify promising solutions to enhancing grid resilience. In [7], several methods were reviewed to identify and address the weaknesses of power systems caused by three types of events including natural events, intentional attacks, and random failures. These methods were classified into analytical approaches, functional methods, and Monte Carlo simulations. Multiple review studies exist focusing on the vulnerability of the CPPS related to cyberattacks. The authors in [8] reviewed the critical attack threats and defense strategies in the CPPS. They provided an overview of the CPPS security, focusing on prominent attack schemes with critical impacts on grid operations and the corresponding defense strategies. The authors in [9] reviewed recent research on cyberattack modeling, security evaluation, attack detection, and defense methods. A comprehensive review about false data injection attacks against the CPPS was provided in [10], which also discussed about physical and economic impacts of the attack on power systems. Man-in-the-middle attack, distributed denial-of-service attack, jamming attack, and false data injection attack were identified as four major cyberattacks in smart grids in [11], and two mitigation methods were summarized for addressing these four types of attacks. A comprehensive study has been conducted on the

Manuscript received October 12, 2020; revised April 10, 2021 and September 11, 2021; accepted October 19, 2021. Date of publication November 25, 2021; date of current version June 13, 2022. This work was supported in part by the National Renewable Energy Laboratory (NREL), Operated by Alliance for Sustainable Energy, LLC for the U.S. Department of Energy (DOE) under Grant DE-AC36-08GO28308. *(Corresponding author: Fei Ding.)*

Shuva Paul is with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332-0250 USA (e-mail: spaul94@gatech.edu).

Fei Ding, Kumar Utkarsh, Weijia Liu, and John Barnett are with the National Renewable Energy Laboratory, Golden, CO 80401 USA (e-mail: fei.ding@nrel.gov; utkarsh.kumar@nrel.gov; weijia.liu@nrel.gov; john.barnett@nrel.gov).

Mark J. O'Malley is with the University of College Dublin, 4 Belfield, Dublin, Ireland (e-mail: mark.omalley@ucd.ie).

Digital Object Identifier 10.1109/JSYST.2021.3123904

data-driven monitoring and safety control of industrial cyber-physical systems [12]. On a different study, real-time monitoring and control aspects of industrial cyber-physical systems were reviewed with an integrated plant-wide monitoring and control framework [13]. On the other hand, resilience is an emerging research topic. The authors in [14] and [15] discussed about the concept of resilience for general engineering systems. Focusing on power systems, the definitions of resilience were discussed in [16] and [17]. These two references aimed at providing a converged and commonly accepted definition of cyber-physical resilience of power systems, and the differences between robustness/reliability and resilience were differentiated.

Although there have been multiple related review papers, many of them neglect the cross-domain interdependencies of the CPPS and do not comprehensively study system vulnerabilities and resilience strategies from the architectural viewpoint of the CPPS. To fill the gap, this article first provides an overview of the definition, architecture, and elements of the CPPS. Then, the definitions of vulnerability and resilience are discussed. Also, a thorough review of state-of-the-art approaches to assess the vulnerability and to quantify the resilience of the CPPS is provided. Additionally, some research gaps in the existing approaches are identified and potential solutions to overcome these gaps are introduced.

The rest of this article is organized as follows: Section II discusses the definition, framework, and elements of the CPPS. Sections III and IV present cyber, physical, and cyber-physical vulnerabilities and resilience, state-of-the-art approaches to assess the vulnerabilities and resilience in the CPPS, and their assessment metrics from the perspectives of different methodologies and applications. Section V identifies the research gaps and introduces possible future research opportunities. Finally, Section VI concludes this article.

II. Cyber-Physical Power Systems

To identify the vulnerabilities of the CPPS, it is indispensable to first understand what a CPPS is, how the CPPS is operating, and where the CPPS could be exposed to threats. Accordingly, this section provides a summary of CPPS definitions and the key elements that constitute the CPPS.

A. Definition

The CPPS integrate advanced sensors, intelligent automation systems, and communication networks into power systems. The CPPS have been elaborated in the literature from different perspectives. The authors in [18]–[20] defined the CPPS from the perspective of embedded systems focusing on the integration of computing systems with the physical systems under monitoring and control. The authors in [21] and [22] defined the CPPS as the integration of information and communications systems into physical systems, whereas [23] defined the CPPS as representatives of penetrations of new technologies, such as cloud computing and the Internet of Things. In our opinion, CPPSs are complex automated systems comprising interdependent, multidimensional, heterogeneous networks that use collaborative computation, communications, and control technologies to fulfill different power system applications and aim to deliver efficient, reliable, secure, and resilient electricity.

B. Architectural Framework of the CPPS

Inspired by the smart grid architecture model (SGAM) [24], which was proposed by the National Institute of Standards and Technology, we consider that the CPPS consists of multiple domains, and each domain has its own roles and entities. Roles can be considered as the services that a domain should be capable of providing by using one entity or multiple entities within the same domain. The roles in one domain often interact with roles in other domains to achieve a complex function for providing reliable, secure, and resilient electricity. Communications occur within the same domain and across multiple domains, and these communications need to meet the requirements of data modeling and protocols to achieve interoperability. Accordingly, the architectural framework of the CPPS can be depicted as Fig. 2. The following five domains are identified: markets, generation, transmission, distribution, and customers. The SGAM has two additional domains: service providers and operations; however, we think these two domains can be merged with others, so only five domains are defined. The roles in the markets domain are the operators and participants in electricity markets. The generator domain refers to the generators of electricity, and it includes traditional fossil-fueled generators, hydropower, wind power plants, and other large-scale renewable energy resources. The transmission domain refers to the carriers of bulk electricity over long distances, and the distribution domain includes the distributors of electricity to and from customers. The customer domain deals with the end-user process of the electrical process. It involves loads, distributed energy resources, meters, and customer-side control systems. The customer domain also includes retail energy providers and aggregators that manage a group of grid-edge resources to provide grid services. These five domains interact with each other and support a variety of grid planning and operation functions. These five domains involve different components and elements that exchange information and collaborate with each other, described as those blocks shown in Fig. 2. Detailed information about these elements and their functions can refer to [24].

C. Interactions Between Domains and CPPS Threat Surfaces

To maintain a fully functioning CPPS, all the devices inside each domain need to keep working correctly, i.e., strengthening physical security. In addition, because massive data exchanges and communications exist inside each domain and across multiple domains, ensuring interoperability and enhancing cybersecurity for the CPPS are of great significance. As described in Fig. 2, the market domain involves external communications with the generation, transmission, distribution, and customer domains. Internal communications exist among market management, market operations, wholesales, trading, ancillary operations, retailing, and distributed energy resource aggregation. The customer domain has internal communications links among different components—such as houses, meters, appliances, automation processes, and thermostats—and it involves external communications and electrical flows with markets and distribution domains. Both the transmission and distribution domains have highly interconnected communications and electricity flows inside their own domains.

In sum, the elements of CPPS include software and devices, computer systems, and individuals from different organizations participating in grid planning and operations. CPPS elements and their associated connectivity are the areas where CPPS are

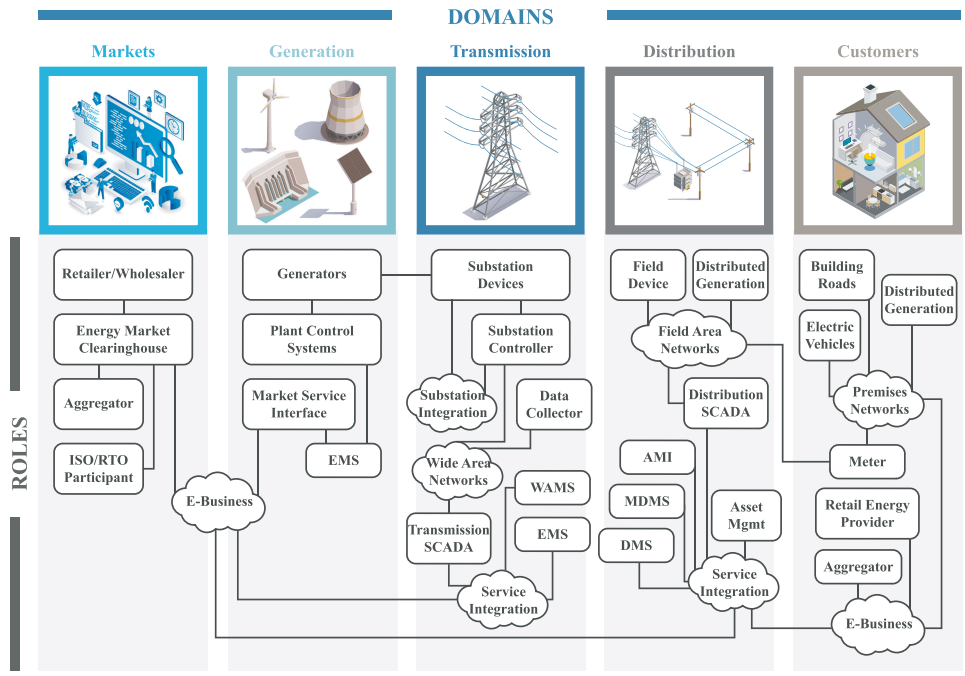

Fig. 2. Architectural framework of the CPPS consisting of multiple domains and providing different functions.

vulnerable to security threats, and thus, need attention. In the next section, we will provide an overview of CPPS vulnerabilities and the methods to assess them.

III. Vulnerabilities of CPPS

According to [5], vulnerability refers to "a measure of the system's weakness concerning a sequence of cascading events that may include a line or generator outages, malfunctions or undesirable operations of protection relays, information or communication system failures." In [25], vulnerability is defined as a measure of the extent to which a power system has low reliability. In our opinion, vulnerability measures the weakness of a system to failures, threats, disasters, and attacks, and the vulnerability of the CPPS can be divided into three groups.

A. Types of Vulnerabilities

1) Cyber Vulnerability: Modern power systems are controlled by computer networks on a large scale. The integration of IT and OT broadens threat surfaces for threat actors. Several choking points of the CPPS are responsible for allowing cyberattacks to happen in power systems.

a) Networks: Networks form one of the most attractive entry points for threat actors because they are vulnerable to misconfiguration, poor administration, lack of perimeter awareness, and communications shortcomings [26], [27]. A determined threat actor continuously looks for potential entry points to the network by searching for electronic holes in firewalls, routers, and switches, and uses those to break the defense.

b) Communications: There are multiple existing and frequently used industrial control system protocols, such as Distributed Network Protocol 3 [28], Modbus [29], International Electrotechnical Commission (IEC) 60870-5-104 [30], IEC 61850 [31], and IEC 61400-25 [32]. However, many of these communications protocols lack enough authentication, authorization, and encryption, and transmitted messages can be easily intercepted and manipulated [33].

c) Devices: With rapid technological advancements, increasing numbers of heterogeneous devices are being connected to the physical power system. This also increases attack surfaces for threat actors.

d) Remote access: To manage widespread assets, reduce costs, and make system processes convenient, utility operators usually rely on remote accessible equipment and devices. Because of weak passwords and authentication, however, a remote access point could lead to an unauthorized intrusion and cause catastrophic damage.

e) Third-party services and supply chains: In some cases, vendors, system integrators, and other third-party services and product providers unintentionally create cybersecurity problems in industrial control system equipment. These unintentionally created backdoors could lead to cyber threats, such as changing passwords or installing unauthorized security packages, which make it challenging to ensure supply chain integrity [34], [35].

f) Human error: Human error, which generally refers to unintentional actions or lack of action, by employees and users is one major reason causing a cybersecurity breach to happen.

2) Physical vulnerabilities: Although physical and cybersecurity schemes are established as two separate sectors, in practice, these two are related. Optimal protection against cyber vulnerabilities is achievable if the CPPSs are physically less vulnerable and managed through physical and operational control. CPPSs are vulnerable physically in many aspects. For instance, sensors or measurement devices can be damaged, and protection relays can be destroyed in many ways.

One major concern of power systems is the transmission network. It is extremely challenging to protect transmission networks because the lines usually extend several thousands of miles. Notably, high-capacity transmission line cables are more vulnerable because they have a large diameter, which

makes them easy targets [36]. On the other hand, towers and transformers are also among the primary concerns. Damages to towers and transformers could create widespread power outages, which could last for days or even longer. And coordinated and simultaneous attacks on high-voltage transformers could create severe damage, leading to social and economic consequences [37].

3) Cyber-physical vulnerabilities: With advanced information and communication technologies embedded in physical systems and grid controls, CPPSs are facing new vulnerabilities. Coordinated attacks can be conducted to compromise monitoring systems and control frameworks by unauthorized intrusion, data theft, privacy and policy violation, etc. The damage to the grid can be amplified to a significant level by targeting physical systems in coordination with cyberattacks. Cyber-physical coordinated vulnerability has been studied rarely in the existing literature, but it should be brought under critical consideration to prevent massive damages to the grid. For instance, the connecting links among cyber-physical components in advanced grid infrastructures make the whole system vulnerable to physical damage to the grid [38]. Additionally, the digitization of the operation leaves OT networks exposed critically. Since the IT and OT are merging together, concerned authorities must enhance their security tools to protect the cyber-physical systems [39].

Cyber-physical vulnerability is different from cyber vulnerability. The former considers the correlation between cyber and physical elements of the CPPS network, and studies the impact of cyber damages on the physical network operations, and vice versa. Cyber vulnerability mainly focuses on the IT elements and devices but cyber-physical vulnerability also studies control and monitoring systems, communication links, etc. Thus, the study of cyber-physical inter-dependencies is necessary in order to investigate and mitigate cyber-physical vulnerabilities.

B. Analytic Approaches to Assessing Vulnerability

Many research activities have been conducted to analyze the vulnerabilities of power systems. In [40], a framework was proposed to identify vulnerable and critical components of the power system. It considered the interactions among power system components and modeled the dynamic process of cascading failures. System vulnerability was quantified in terms of the cost to the power system. The authors of [41] studied vulnerability assessment considering stochastic loads and model imprecision. They proposed a framework for uncertainty quantification and vulnerability assessment of power systems. The developed algorithm analyzed the drops in performance as a result of single and multiple contingencies.

Based on the complex network theory, the authors in [42] assessed the nodal vulnerability of the grid by creating different nodal-attack scenarios based on the centrality measures. Similarly, the authors in [43] also studied power system vulnerability and identified critical nodes of a grid using the complex network theory, and a cascading failure model based on the ac power flow model and network topology weighted admittance was developed.

In [44]–[47], the vulnerability of the grid was analyzed using the machine learning and game theory. The authors identified the critical elements of the grid as sequences of action strategies from the attacker's viewpoints. In [48], the electric grid was modeled as a graph network and the vulnerability of the grid was evaluated according to topological/structural characteristics. The structural vulnerability/attack tolerance of the grid caused by line removal was also studied. In [49], the authors mentioned different performance indices and evaluation metrics for assessing the grid vulnerability. Later, they provided a correlation analysis of the metrics by measuring the failure probability caused by a single or multiple nodes or edge failures.

TABLE I
EXISTING ANALYTICAL APPROACHES FOR ASSESSING VULNERABILITY

Reference	Strategy	Evaluation Index
[49]–[51]	Complex Network Theory	Efficiency
[48], [52]–[55]		Error and attack tolerance
[56]–[58]		Betweenness
[42], [43], [59]–[61]		Centrality measures
[62]		Electrical and operational features
[63]		Line voltage stability
[64]		Impactability, Susceptibility
[65], [66]	Machine Learning	Voltage Security
[67]		Grid Exposure, Line Outage
[68], [69]		Transient Stability
[70]		Security Metric
[71], [72]		Grid Disturbances
[73]		Line overload and voltage deviation index
[74]		Correlation between data flows
[44]–[47], [75], [76]		Line outages, time to reach blackout
[5], [77], [78]	Simulation Based	Cascading Failure
[79]		Maximum power supply
[80]		Loss of load
[81]		Link-centrality measures
[82], [83]	Optimization Based	Load shedding
[84]		Line switching
[85]		Failure and recovery probabilities

Additionally, Table I summarizes more analytical approaches for assessing the vulnerabilities of power systems. The first column in Table I refers to the associated references, the second column represents the associated strategies applied/followed while doing vulnerability assessment, and the third/last column represents the associated evaluation indices. An evaluation index indicates a standard to measure the vulnerability of the concerned system.

C. Vulnerability Metrics

In addition to the analytic approaches summarized in Table I, a suite of metrics has been proposed in the literature to quantify vulnerability. These metrics can be divided into two major categories: those based on system characteristics and those determined by evaluating the holistic system impact.

1) Metrics Defined by System Characteristics: The authors in[52] defined vulnerability of a network as follows:

$$V = \frac{1}{N_T} \sum_{i=1}^{N_T} V(i) \tag{1}$$

Where N_T is the total number of terminal nodes in the grid, and $V(i)$ is the vulnerability of the node i, which is defined as

$$V(i) = \frac{g_i}{g_T} \tag{2}$$

Where g_i is the number of generators connected to the terminal node i, and g_T is the total number of generation nodes.

In [43], grid vulnerability was calculated based on $net-ability$, which is a function of the electrical distance. The electrical distance can be defined as the equivalent impedance Z_{ij} between the ith and jth nodes. Net-ability evaluates the

transferability and performance of the grid under normal operating conditions. It is affected by network structure, transmission line impedance, rated power of generators, and load demands. The net-ability (NA) is formulated as

$$\mathrm{NA} = \frac{1}{N_G N_L} \sum_{i \in G} \sum_{j \in L} \frac{P_i}{L_j |e^{Z_{ij}}|} \tag{3}$$

Where N_G and N_L represent the nodes with generation sources and the nodes with loads, respectively. P_i stands for generation power, and L_j stands for maximum load. Then, the vulnerability of the network when the node i is removed from the network, denoted as $V_{NA}(i)$, can be calculated as follows:

$$V_{\mathrm{NA}}(i) = \frac{\mathrm{NA}_{\mathrm{init}} - \mathrm{NA}_i}{\mathrm{NA}_{\mathrm{init}}} \tag{4}$$

Where $\mathrm{NA}_{\mathrm{init}}$ represents the net-ability of the initial network, and NA_i represents the net-ability of the network after the cascading failure caused by removing the node i.

Similarly, in [86], the authors computed system vulnerability caused by the removal of lines. They first defined $V_E(l)$ as the reduction of performance caused by line removal, as

$$V_E(l) = \frac{E_{\mathrm{init}} - E_l}{E_{\mathrm{init}}} \tag{5}$$

Where E_{init} is the network's initial global efficiency, and E_l is the network's global efficiency after the line removal.

Then, network vulnerability is expressed as the maximum vulnerability of all of the network's nodes.

2) Metrics Defined by the Holistic System Impact: In [87], vulnerability was quantified as the conditional probability of a damaged grid given an extreme weather event. Grid vulnerability, V, is defined as $V = P(D|I_{EW})$, where V is expressed in percentage (%), $P(D|I_{EW})$ is a conditional probability (cumulative) of damage (D), and I_{EW} represents the intensity of the extreme weather event.

In [88], the authors defined the vulnerability of a critical infrastructure resulting from a set of possible damages as

$$V[S, D] = \frac{\phi[S] - W[S, D]}{\phi[S]} \tag{6}$$

Where $W[S, D] = \phi[D(S, d^*)]$ is the worst performance of the infrastructure S associated with a class of damages, D. The vulnerability is defined with a range [0, 1].

Impactibility and susceptibility were introduced in [64] as two features to evaluate the vulnerability of complex network infrastructures, such as power systems. The impactibility metric (IM) can be defined as follows:

$$\mathrm{IM}_j = \frac{1}{N_Q} E_j \tag{7}$$

Where j is the index of the vertex; N_Q is the total number of affected vertices in the set of affected vertices Q; and E_j is the entropy that measures load change in the graph.

Also, security index (SI) was introduced in [73] to evaluate the vulnerability of a power system. The security index is a function of the line overload index and voltage deviation index, and it is formulated as

$$\mathrm{LOI}_{km} = \begin{cases} \frac{S_{km} - S_{\mathrm{lim}}}{S_{km}}.100, & \text{if } S_{km} > S_{\mathrm{lim}} \\ 0, & \text{if } S_{km} < S_{lim} \end{cases} \tag{8}$$

$$\mathrm{VDI}_k = \begin{cases} \frac{|U_k^{\min}| - |U_k|}{|U_k^{\min}|}.100 & \text{if } |U_k| < |U_k^{\min}| \\ 0 & \text{if } |U_k^{\min}| \le |U_k| \le |U_k^m| \\ \frac{|U_k| - |U_k^{\max}|}{|U_k^{\max}|}.100 & \text{if } |U_k| > |U_k^{\max}| \end{cases} \tag{9}$$

$$\mathrm{SI} = \frac{w_1 . \sum_{i=1}^{n_L} LOI_i + w_2 . \sum_{i=1}^{n_B} VDI_i}{n_L + n_B} \tag{10}$$

where S_{km} and S_{lim} stand for the MVA flow and MVA limit of branch $k - m$; and $|U_k^{\min}|$, $|U_k^{\max}|$, and U_k are the minimum voltage limit, maximum voltage limit, and bus-k voltage, respectively.

In addition, a scoring system, called the cyber vulnerability scoring system (CVSS), was proposed by the National Institute of Standards and Technology to measure the vulnerability of computer systems. We believe CVVS can be extended to quantify the vulnerability for cyber systems, physical systems, and cyber-physical systems. The CVSS can be expressed as a function of base metric group, temporal metric group, and environmental group. Details about how these groups are defined can be found in [89].

The vulnerabilities in the CPPS have been studied extensively in the existing literature. However, advancement and convergence of the OT/IT platforms are exposing in such ways that elaborated, collaborative/joint, and more sophisticated researches are required to reduce the vulnerabilities of the CPPS from root level to edge levels.

IV. Resilience in CPPS

Resilience defines a system's ability to survive while experiencing extreme events, and recover to its operating state after experiencing the disruption. Resilient CPPS should be capable of not only identifying their vulnerabilities and taking appropriate actions to stand for the vulnerabilities caused by extreme events, but also recovering fast to operational state after experiencing the extreme disturbances.

A. Types of Resilience

1) Cyber Resilience: Cyber resilience in modern cyber-physical systems generally denotes the integration of cybersecurity that emphasizes preventing failures and cyber risk management that maintains critical functions in the event of cyberattacks [90]. In terms of CPPS, cyber networks such as supervisory control and data acquisition system, energy management system, and wide-area monitoring system collect, transmit, process, and store power system operation information [91]. Thus, cyber resilience of CPPS relies on information availability and accessibility, data integrity and accuracy, and data confidentiality. To safeguard power system operations, the following two questions should be solved.

1) How should a cyber network be designed to avoid and prevent severe failures?
2) If the cyber system is attacked, how can the damage be minimized to recover system functionality and how can the recovery be achieved as quickly as possible?

To answer the first question, a resilient communication network design on the device level was studied in [92], and a named data networking approach was introduced in [93] to guarantee the security of communications content and to identify cyberattacks. To answer the second question, defense strategies

against false data injections were studied in [94]–[96]. Quick recovery relies on intelligent and robust controls. Software-defined networking was employed in [97] to achieve cyber network self-healing. A resilient control under denial-of-service attacks was developed in [98] to improve the stability. These techniques can help recover cyber network.

2) Physical Resilience: An essential objective of power systems is to absorb and recover from high-consequence events [99]. Per the report provided by the U.S. National Academy of Sciences [100], resilience can be defined as "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events." According to this definition, resilience can be categorized further as short- and long-term resilience [101]. Short-term resilience defines the features a system should have before, during, and after an event, and it relates to the system's ability to resist and adapt dynamically to such events. Long-term resilience, on the other hand, deals with the system's ability to adapt to future damaging events considering learning from past events. It typically involves comprehensive system planning and physical infrastructure hardening.

Multihazard risk assessment for high-impact low-frequency power grid events is also critical for power grid physical resilience. A two-stage hybrid risk estimation model was developed as a multihazard approach for extreme weather-induced power outage risk assessment [102]. It is important to note here that power systems are usually operated in order to satisfy $N-1$ contingencies, implying that the failure of any one component at any given time should not result in any unserved loads. Therefore, considering single component failures will not produce conclusive results demonstrating increase or decrease in physical resilience. Further evaluating the effects of $N-k(k>1)$ order contingencies entails calculating their probability of occurrence based on events causing simultaneous k failures or interdependent k failures. However, full contingency evaluation is almost impossible for real-world systems for reasonable values of k due to the combinatorial nature of possible contingency states [103].

3) Cyber-Physical Resilience: A cyber-physical resilient power system should respond to cyber-physical disturbances in real time and mitigate major interruptions of critical services. The evaluation of cyber-physical resilience and proper infrastructure, network, and control designs of general cyber-physical systems were studied in [104]–[106]. For CPPS, a framework for power system cyber-physical resilience was proposed in [16], which consisted of three parts: system identification, vulnerability analysis before, during, and postdisturbance, and resilient operation considering absorbing disturbances and recovering from failures. The resilience assessment framework considering distributed energy resources and wide-area monitoring systems were discussed in [107] and [108], respectively. The implementations of cyber-physical resilience in different power system areas could be found, such as power system stability [109], [110], power system restoration [111], [112], power system protection [113], microgrids [114], [115], and voltage control [116].

B. Analytic Approaches to Assess Resilience

Different approaches have been implemented to study the short-term resilience of the CPPS, such as evaluation and decision making, the Markov process, and optimization. Security assessment metric for cyber-physical systems can be developed considering microgrids, where the cyber-physical model is established based on the graph theory, and the resilience impact factors are integrated by a fuzzy Choquet integral approach [115]. Device-level resilience against cyberattacks in the microgrid environment can be modeled analyzing the communication networks and cyber vulnerabilities, leading to a development of a device resilience framework [92].

For the interdependent critical infrastructures, such as for combined power and water supply systems, the cyber-physical resilience can be studied where the infrastructural metrics and operational metrics are integrated through a weighted sum method [117]. The cyber resilience can be evaluated and the assessment metrics can be formulated by using a systemic impact index and a targeted system performance index [118]. Markov decision processes and Q-learning can be beneficial while assessing the resilience of cyber-physical control systems against attacks. The optimal attack sequence can be modeled and employed to simulate the attacker's problem. The defender's strategies of attack detection and mitigation were designed accordingly [116]. Cyber-physical intrusion resilience based on a new hybrid cyber-physical resilience metric can be developed consisting of physical resilience and cyber resilience [110]. Cyber-physical systems were modeled as linear systems, and methodologies were discussed to synthesize the controllers to guarantee resilience. Hierarchical games and Markovian cyber defense policies can be adopted to maximize system resilience considering the cost of recovery [116]. The resilience analysis framework of dc microgrids against denial-of-service cyberattacks can be established based on a stability analysis considering the influences of time-varying denial-of-service incidents. A resilience measure is defined to stand for the input-to-state stability and was quantified by convex optimization techniques [94]. Additionally, resilience curve is widely used to assess the smart grid resilience and develop generic resilience metric evaluating the performance of the power system after a severe disturbance [111].

To sum up, Table II provides different analytic approaches proposed in the literature in 11 application areas as well the methodologies used in each application area.

C. Resilience Metrics

Several resilience metrics have been proposed along with the aforementioned analytic approaches. Also, note that resilience is still an emerging research topic, and many researchers are currently working on defining resilience metrics. In [125], the resilience of power systems under extreme events was defined as

$$\theta = \{K, \text{LOLP}, \text{EDNS}, G\} \tag{11}$$

Where index K represents the number of line outages during the event. LOLP is the loss of load probability and it measures the probability of load not being fully supplied. EDNS measures the amount of expected demand not being supplied. G is the measurement of the difficulty level to recover the grid. Here, K can be defined as

$$K = \int_0^\infty k f(k) dk \tag{12}$$

TABLE II
APPLICATION AREAS AND METHODOLOGIES OF ASSESSING RESILIENCE IN CPPS

Reference	Application Area	Methodology
[115]	Microgrid	Communications failure with distributed event-triggered secondary control
[116]		Integration of Choquet integral
[92]		CVSS method, weighted sum approach
[94]		Optimization approach to assess resilience (stability) against cyber incidents
[91]		Establish frameworks to improve cybersecurity
[97]		Software-defined networking technique
[113]		Collaborative restoration of cyber and physical system
[121]		Cyber network is modeled as a constraint and integrated into OPF
[16]	Distributed energy resources	Framework to assess vulnerability and resilience of power system
[108]		Establish framework to assess resilience against attacks
[117]	Power grid control	Markov process, Q-learning, attacker-defender
[122]		Hierarchical architecture with automatic generation of contracts
[123]		Cyber resilience assessment proposed and assessed in a hierarchy
[90]		Scoring system is used to grade vulnerability and impact
[114]	Power system stability, monitoring, and protection	Game-theoretic analysis
[95]		Bayesian approach to improve resilience against data injection attacks
[110]		Robust and resilient control system design
[109]		Establish general frameworks to improve resilience against cyberattacks
[124]	Networked systems	Hardware-in-the-loop test bed to evaluate impacts of cyberattacks
[125]		An epidemic spreading approach is used to assess cyber resilience
[126]		Network design solved by multi-objective optimization
[111]	Power system generator dynamics	A hybrid cyber-physical resilience assessment approach is proposed combining physical stability and cyberattack impact

where f is the fragility function characterizing the probability of line outages caused by an event, and it is defined as

$$f = P_d(k|V) \tag{13}$$

where V stands for the severity measurement of the event, and P_d is the probability of line outages in V. LOLP and EDNS are two reliability indices that can be defined as

$$\text{LOLP} = \sum_{e_i \in S_e} P_{e_i} \tag{14}$$

$$\text{EDNS} = \sum_{e_i \in S_e} P_{e_i} C_{e_i} \tag{15}$$

where e_i stands for the ith extreme weather event, P_{e_i} represents the probability of the event e_i happening in the grid, S_e stands for the set of extreme events, and C_{e_i} stands for the load curtailment in event e_i.

In [115], the authors discussed cyber-physical resilience and quantified it using a physical metric and a cyber-physical metric. The physical metric represents the forced outage rate of a generator i, FOR_i as follows:

$$\text{FOR}_i = \frac{\text{FOH}_i}{\text{SH}_i + \text{FOH}_i + \text{MOH}_i} \tag{16}$$

where SH_i is the normal operating hours of generator per year, FOH_i is the forced outage hours for generator per year, and MOH_i is the maintenance outage hours for generator per year. The cyber-physical metric provides an exploit-ability and vulnerability ratio. The integrated resilience metric is provided by the Choquet integral. The exploit ability is the average value of the common vulnerability scoring system exploit-ability score. Furthermore, the vulnerability ratio is the ratio of reachable devices (RD) across all domains in both reachable and non-reachable devices (NRD), and formulated as

$$\text{Vulnerability ratio} = \frac{10 \times \text{RD}}{\text{RD} + \text{NRD}}. \tag{17}$$

In [126], while assessing the resilience, the authors discussed critical disconnecting probability (ϕ_{cr}), which represents the maximum intensity of initial failure that the system can survive; and cascade length (τ_{cf}), which represents the time when the random failure stops. ϕ_{cr} is defined as

$$\phi_{cr} = \sup\{0 \le \phi \le 1 | Y_n(\phi) > 0\}. \tag{18}$$

Here, ϕ stands for physical edge disconnecting probability, and Y_ϕ denotes the node yield. And τ_{cf} is defined as

$$\tau_{\text{cf}} := \max\left\{ t \ge 0 | E(R_t^{p'}) - E(R_{t-1}^{p'}) \ge \frac{1}{n_p} \right\} \tag{19}$$

where n_p is the physical graph size, and $R_t^{p'}$ is the ratio of the remaining physical nodes.

Additionally, the authors of [111] provided a general resilience metric to measure the difference between actual post-disturbance performance and the ideal response:

$$\text{RM} = \int_{t_{\text{start}}}^{t_{\text{end}}} [H_3(t) - H^*(t)] dt \tag{20}$$

where RM is the resilience metric, t_{start} and t_{end} are the restoration horizon, and $H_3(t)$ and H^* are the ideal and post-event operation mode, respectively.

In [118], cyber resilience was evaluated by combining a systemic impact index and a targeted system performance index

$$\text{CR} = \frac{\text{SI} + \alpha \text{TRE}}{N} \tag{21}$$

TABLE III
KEY PARAMETERS AFFECTING CPPS RESILIENCE

Category	Parameters	Description
Network Graph Parameters	Path redundancy	Path combinations possible from a generator to a load node
	Branch count effect	Number of branches leading up to a load node
	Overlapping branches	Critical branches used several times in path combinations
	Switching operations	Switching operations needed to connect to all the loads
	Repetition of sources	Number of generators compared to the number of loads
	Aggregated central point dominance	Centrality (or importance) of each node for the connectivity of the network
Resource Inputs	Energy resource availability	Accessibility of energy resources for generators (like diesel for DGs)
	Energy not supplied	Energy not supplied to critical loads during/after an extreme event
	Energy storage availability	Availability of sufficient capacity storage systems to supply critical loads under an extreme event
	Probability of generation resource availability/ Equipment hardening capability	Environmental rating of generators to be able to operate under extreme events
	Redundant power lines	Extra power lines to add redundancy to critical branches
System Capacities	Communications/control systems	Whether generators or controllable loads can be operated in a centralized, distributed or decentralized manner
	Power flow paths, line flow limits	Availability of sufficient power margins in especially critical branches
	Generator and load distribution	Geographical distribution of generators and loads (clustered versus distributed)
	Reserve capacity	Availability of sufficient power margins in generators
	Overhead lines versus underground cables	Depends on proneness to certain types of natural events
System Capabilities	Ancillary service capability	Ability to ensure customers and third-party assets can provide resilience benefits to the utility
	Component failure rate	Related to the environmental rating and overall reliability of a component
	Efficiency of power supply/ power losses	Efficiency of power generation and power distribution will ensure minimal energy wastage during extreme events
	Protective and switching devices	Ability of the distribution system to isolate into multiple microgrids or enable microgrids to form new connections to ensure load supply

where CR, SI, TRE, N, and α stand for cyber resilience, system impact, total recovery effort, the normalized quantity for comparison between systems with different sizes, and weighting parameter of SI relative to TRE, respectively.

Furthermore, resilience was measured as the speed of restoration in [112], where the calculation is similar to [111].

$$R = \frac{Q_0 - \min Q(t)}{t_5 - t_3} = \frac{1 - Q_2}{t_5 - t_3}. \tag{22}$$

Here, $t_5 - t_3$ denotes the system restoration period, and Q_2 is the normalized system performance before restoration. R indicates the speed of restoration.

Finally, [127] and [128] present two risk-based resilience metrics, VaR_α (value at risk) and $CVaR_\alpha$ (conditional value at risk). These metrics are calculated by utilizing the system performance loss function *U(I)* by randomly sampling events from the event probability distribution function *p(I)*, where *I* is a variable representing an event. First, the probability ψ that the system performance loss is limited within a threshold τ is calculated as: $\psi(\tau) = \int_{U(I)\leq\tau} p(I)dI$. Then, VaR_α, which refers to the lowest value τ not exceeded by the loss function with a probability α, is calculated as: $VaR_\alpha = \min\{\tau : \psi(\tau) \geq \alpha\}$. And, $CVaR_\alpha$, which measures the anticipated loss function due to top $(1-\alpha)$ percent of the high impact events, is calculated as

$$CVaR_\alpha = (1-\alpha)^{-1} \int_{U(I)\geq VaR_\alpha} U(I)p(I)dI. \tag{23}$$

Based on the review on existing resilience metrics, we summarize the key parameters that affect system resilience in Table III, and these parameters could be considered by utility operators or technology developers to enhance resilience for the CPPS. Although resilience has been widely studied, there still lacks constructive research work of resilience for the CPPS, especially in terms of quantifying system resilience from a cyber-physical coordinated perspective. The interdependencies between cyber and physical domains need to be brought into consideration.

V. RESEARCH GAPS AND OPPORTUNITIES

This article has provided an overview of existing studies on the CPPS vulnerability and resilience. Although many approaches have been proposed to assess the system vulnerability and quantify resilience, research gaps still exist. Thus, this section will discuss the identified research gaps and propose potential future work to advance the state of the art. Several research gaps and opportunities are summarized as follows.

1) Most power networks satisfy the $N-1$ security criterion. Real-world systems comprise more than thousands of elements and it is important to study $N-k$ contingency analysis, where $k \geq 2$. However, the existing CPPS models are not capable of considering all the combinations of contingencies. Also, the computational complexities become huge while considering higher order contingencies. The development of advanced models is required to

reduce the computational complexities for assessing the vulnerability of the CPPS.

2) Multihazard modeling of threat/vulnerability is significant in assessing the risk and vulnerability in different domain of critical infrastructures. Modeling and assessment of an external threat imposed simultaneously on both cyber and physical power systems carries high importance. However, it is rarely addressed, and this gap should be filled by developing appropriate models and introduce these models for evaluating CPPS resilience.
3) The current research work generally limits the scope to either cyber or physical vulnerability. Advancements in the CPPS have increased the interdependencies between cyber networks and physical systems. Vulnerabilities in cyber networks can trigger, propagate, and accelerate vulnerabilities in physical systems, and the damages in physical systems could also lead to misfunctions in cyber networks. Thus, new research work is required to investigate the cross-domain vulnerability for cyber-physical coupled networks. Moreover, new modeling techniques for interdependent CPPS infrastructures and applications of cutting-edge artificial intelligence techniques could be leveraged.
4) The development of a general resilience metric or metrics to quantify CPPS resilience is required. Because of the diverse characteristics of different cyber-physical systems (e.g., microgrids, vehicular systems, and industrial control systems), researchers have proposed metrics and evaluation methods that fit the specific system they have worked on. Although it is reasonable and beneficial to build these specific metrics, the establishment of a more general (set of) resilience metric(s) that reveals the level of resilience of any domain in the CPPS will significantly improve the awareness of cyber-physical resilience in modern industries and prompt the standardization of CPPS resilience. In addition, resilience is affected by the control decisions taken by the system operator during an ongoing event. Thus, the impact of time-varying control decisions on system resilience should be considered, and this could actually yield the resilience of a system as a time-varying value.
5) Existing resilience metrics are generally approached from the points of view of traditional reliability, stability, or security, leading to inconsistent definitions and perceptions. Moreover, most metrics are vaguely evaluated without providing a clear and detailed quantification method. Thus, it is crucial to integrate the definition of CPPS resilience with a reasonable quantification method presented. The comparability of the resilience metrics should also be guaranteed to enforce the effectiveness across different systems and sectors. Besides, the establishment of simulation test beds will verify the feasibility and efficiency of existing resilience metrics and test the strategies for resilience enhancement. In addition, benchmark use cases can be developed to prompt CPPS resilience standardization.
6) Quantifying the vulnerability and resilience of the CPPS is not the ultimate goal. It is more important to develop countermeasures and enhancement guidelines to safeguard CPPS operations and mitigate the influences of cyber and physical attacks based on the evaluated metrics. Hence, the resilience metrics should be able to illustrate the vulnerable parts of a system so that proper improvement strategies can be developed.

VI. Conclusion

Assessing system vulnerability and measuring resilience are crucial for making proactive actions to safeguard CPPS operations. This article provides an overview of the state of the art, and it could help both researchers and system operators enhance their understandings of CPPS vulnerability and resilience, and thus, advance the state of the art by identifying potential future pathways. The contribution of this article consists of the following.

First, this article reviews the definitions of the CPPS from the existing literature, and then, provides our understanding of the CPPS with a new definition and a holistic architectural framework. The domains and their associated roles are defined in the architectural framework to demonstrate the complex interconnectivities inside CPPS. The vulnerabilities and resilience of the CPPS are explained from three different aspects including cyber, physical, and cyber-physical.

Second, this article provides a comprehensive study of existing approaches that have been used to assess CPPS vulnerabilities and quantify resilience. The reviewed approaches can be divided into several major categories, such as game theory, graph theory, machine learning, and power-flow-based approaches. Table I provides strategy-wise evaluation indices of assessing the vulnerability in the CPPS. Table II summarizes the methodologies and the application areas for measuring CPPS resilience. Assessment indices and metrics are studied and summarized for both CPPS vulnerabilities and resilience. Additionally, the key parameters affecting CPPS resilience are identified in Table III.

Third, through the study of existing literature, this article also identifies several research gaps in vulnerability assessment and resilience quantification related to the CPPS. Specifically, the in-depth study of $N - k$ contingency analysis, extensive cyber-physical vulnerability analysis, generic metric development for cyber-physical vulnerability and resilience assessment, etc., are some important sectors where new developments can be made to secure the CPPS. Also, potential research works that can be conducted in the future to overcome these gaps are introduced.

Acknowledgment

The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes. The views expressed in this article do not necessarily represent the views of the U.S. Department of Energy or the U.S. Government.

References

[1] EATON, *Blackout Tracker*, 2017. Accessed: Dec. 2, 2019. [Online]. Available: http://electricalsector.eaton.com/forms/BlackoutTrackerAnnualReport

[2] V. Sultan and B. Hilton, "A spatial analytics framework to investigate electric power-failure events and their causes," *ISPRS Int. J. of Geo- Inf.*, vol. 9, no. 1, pp. 1–22. 2020.

[3] R. Rojas, *Snowstorm Pummels Eastern Seaboard*, Mar. 2018. Accessed: Dec. 2, 2019. [Online]. Available: https://www.nytimes.com/2018/03/21/nyregion/snow-storm-winter-weather.html

[4] N. Hallas, *Trends in Cybersecurity Breaches Continue in 2019*, Oct. 2019. Accessed: Feb. 12, 2020. [Online]. Available: https://blog.auditanalytics.com/trends-in-cybersecurity-breaches-continue-in-2019/

[5] R. Baldick *et al.*, "Vulnerability assessment for cascading failures in electric power systems," in *Proc. IEEE/PES Power Syst. Conf. Expo.*, 2009, pp. 1–9.

[6] B. Obama, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, Feb. 2013, [Online]. Available: https://www.hsdl.org/?viewdid=731087

[7] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power system," *Rel. Eng. Syst. Saf.*, vol. 183, pp. 153–172, 2019.

[8] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber- Phys. Syst.: Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[9] X. Cai, Q. Wang, Y. Tang, and L. Zhu, "Review of cyber-attacks and defense research on cyber physical power system," in *Proc. IEEE Sustain. Power Energy Conf.*, 2019, pp. 487–492.

[10] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[11] M. M. Pour, A. Anzalchi, and A. Sarwat, "A review on cyber security issues and mitigation methods in smart grid systems," in *Proc. SoutheastCon*, 2017, pp. 1–4.

[12] Y. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374–47384, 2018.

[13] S. Yin, J. J. Rodriguez-Andina, and Y. Jiang, "Real-time monitoring and control of industrial cyberphysical systems: With integrated plant-wide monitoring and control framework," *IEEE Ind. Electron. Mag.*, vol. 13, no. 4, pp. 38–47, Dec. 2019.

[14] D. Woods, "Four concepts for resilience and the implications for the future of resilience engineering," *Rel. Eng. System Saf.*, vol. 141, pp. 5–9, Sep. 2015.

[15] S. Hosseini, K. Barker, and J. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Jan. 2016.

[16] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable Sustain. Energy Rev.*, vol. 58, pp. 1060–1069, 2016.

[17] A. Gholami, T. Shekari, M. Amirioun, F. Aminifar, M. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32 035–32 053, 2018.

[18] T. Facchinetti and M. L. Della Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans. Ind. Inform.*, vol. 7, no. 4, pp. 689–698, Nov. 2011.

[19] H. Gharavi, H. Chen, and C. Wietfeld, "Guest editorial special section on cyber-physical systems and security for smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2405–2408, Sep. 2015.

[20] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Automatica Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[21] M. Bessani, "Impact of operators' performance in the reliability of cyber-physical power distribution systems," *IET Gener., Transmiss. Distrib.*, vol. 10, pp. 2640–2646(6), Aug. 2016.

[22] S. Xin, Q. Guo, H. Sun, C. Chen, J. Wang, and B. Zhang, "Information-energy flow computation and cyber-physical sensitivity analysis for power systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 329–341, Jun. 2017.

[23] Q. Li *et al.*, "Safety risk monitoring of cyber-physical power systems based on ensemble learning algorithm," *IEEE Access*, vol. 7, pp. 24788–24805, 2019.

[24] D. Wollman *et al.*, "NIST framework and roadmap for smart grid interoperability standards," Nat. Inst. Standards Technol., NIST Special Publication 1108, release 3.0, Oct. 2014.

[25] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, 2015.

[26] S. Keith, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *NIST 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, May 2015.

[27] Ponemon Institute LLC, "Critical infrastructure: Security preparedness and maturity," Jul. 2014.

[28] I. Darwish, O. Igbe, O. Celebi, T. Saadawi, and J. Soryal, "Smart grid DNP3 vulnerability analysis and experimentation," in *Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, Nov. 2015, pp. 141–147.

[29] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. IEEE Int. Workshop Tech. Committee Commun. Qual. Rel.*, May 2015, pp. 1–6.

[30] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, 2013, pp. 1–5.

[31] X. Niu, Y. Tong, and J. Sun, "Vulnerability assessment for PMU communication networks," in *Smart Computing and Communication*, M. Qiu, Ed. Cham, Switzerland: Springer, 2018, pp. 29–38.

[32] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr.*, Nov. 2017, pp. 1–6.

[33] M. Robinson, "The SCADA threat landscape," in *Proc. 1st Int. Symp. ICS&SCADA Cyber Secur. Res.*, 2013.

[34] S. Papastergiou and N. Polemi, "Mitigate: A dynamic supply chain cyber risk assessment methodology," in *Smart Trends in Systems, Security and Sustainability*, X.-S. Yang, A. K. Nagar, and A. Joshi, Eds. Singapore: Springer, 2018, pp. 1–9.

[35] N. Polatidis, M. Pavlidis, and H. Mouratidis, "Cyber-attack path discovery in a dynamic supply chain maritime risk management system," *Comput. Standards Interfaces*, vol. 56, pp. 74–82, 2018.

[36] [Online]. Available: https://operationcircuitbreaker.wordpress.com/chapter-4-transmission-line-vulnerabilities.

[37] P. W. Parfomak, "Physical security of the U.S. power grid: High-voltage transformer substations," Jun. 17, 2014. [Online]. Available: https://fas.org/sgp/crs/homesec/R43604.pdf

[38] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[39] S. De Dutta and R. Prasad, "Security for smart grid in 5G and beyond networks," *Wireless Pers. Commun.*, vol. 106, no. 1, pp. 261–273, 2019.

[40] M. X. Cheng, M. Crow, and Q. Ye, "A game theory approach to vulnerability analysis: Integrating power flows with topological analysis," *Int. J. Elect. Power Energy Syst.*, vol. 82, pp. 29–36, 2016.

[41] R. Rocchetta and E. Patelli, "Assessment of power grid vulnerabilities accounting for stochastic loads and model imprecision," *Int. J. Elect. Power Energy Syst.*, vol. 98, pp. 219–232, 2018.

[42] H. Cetinay, K. Devriendt, and P. Van Mieghem, "Nodal vulnerability to targeted attacks in power grids," *Appl. Netw. Sci.*, vol. 3, no. 34, pp. 1–19, Aug. 2018.

[43] 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 Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 3, pp. 346–350, Mar. 2018.

[44] S. Paul and Z. Ni, "Vulnerability analysis for simultaneous attack in smart grid security," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf.*, Apr. 2017, pp. 1–5.

[45] Z. Ni, S. Paul, X. Zhong, and Q. Wei, "A reinforcement learning approach for sequential decision-making process of attacks in smart grid," in *Proc. IEEE Symp. Ser. Comput. Intell.*, Nov. 2017, pp. 1–8.

[46] S. Paul and Z. Ni, "A study of linear programming and reinforcement learning for one-shot game in smart grid security," in *Proc. Int. Joint Conf. Neural Netw.*, Jul. 2018, pp. 1–8.

[47] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2684–2695, Sep. 2019.

[48] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Anal.*, vol. 26, no. 4, pp. 955–969, 2006.

[49] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Physica A, Statist. Mechanics Appl.*, vol. 396, pp. 204–211, 2014.

[50] V. Gol'dshtein, G. A. Koganov, and G. I. Surdutovich, "Vulnerability and hierarchy of complex networks," 2004, *arXiv:cond-mat/0409298*.

[51] W. Kang, P. Zhu, J. Zhang, and J. Zhang, "Critical nodes identification of power grids based on network efficiency," *IEICE Trans. Inf. Syst.*, vol. E101.D, no. 11, pp. 2762–2772, 2018.

[52] S. Xu, H. Zhou, C. Li, and X. Yang, "Vulnerability assessment of power grid based on complex network theory," in *Proc. Asia-Pacific Power Energy Eng. Conf.*, Mar. 2009, pp. 1–4.

[53] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A, Statist. Mechanics Appl.*, vol. 389, no. 3, pp. 595–603, 2010.

[54] J. Beyza, E. Garcia-Paricio, and J. M. Yusta, "Applying complex network theory to the vulnerability assessment of interdependent energy infrastructures," *Energies*, vol. 12, no. 3, 2019, Art. no. 421.

[55] D. Deka, S. Vishwanath, and R. Baldick, "Topological vulnerability of power grids to disasters: Bounds, adversarial attacks and reinforcement," in *PLoS One*, vol. 13, no. 10, 2018, Art. no. e0204815.

[56] E. Bompard, D. Wu, and F. Xue, "The concept of betweenness in the analysis of power grid vulnerability," in *Proc. Complexity Eng.*, Mar. 2010, pp. 52–54.

[57] K. Wang, B. H. Zhang, Z. Zhang, X. G, Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A, Statist. Mech. Appl.*, vol. 390, no. 23, pp. 4692–4701, 2011.

[58] D. Wu, F. Ma, M. Javadi, K. Thulasiraman, E. Bompard, and J. N. Jiang, "A study of the impacts of flow direction and electrical constraints on vulnerability assessment of power grid using electrical betweenness measures," *Physica A, Statist. Mechanics Appl.*, vol. 466, pp. 295–309, 2017.

[59] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. 49th IEEE Conf. Decis. Control*, Dec. 2010, pp. 5792–5797.

[60] F. Gutierrez, E. Barocio, F. Uribe, and P. Zuñiga, "Vulnerability analysis of power grids using modified centrality measures," *Discrete Dyn. Nature Soc.*, vol. 2013, Apr. 2013, Art. no. 135731.

[61] T. Verma, W. Ellens, and R. E. Kooij, "Context-independent centrality measures underestimate the vulnerability of power grids," *Int. J. Critical Infrastructures*, vol. 11, no. 1, pp. 62–81, 2015.

[62] Y. Dai, G. Chen, Z. Dong, Y. Xue, D. J. Hill, and Y. Zhao, "An improved framework for power grid vulnerability analysis considering critical system features," *Physica A, Statist. Mechanics Appl.*, vol. 395, pp. 405–415, 2014.

[63] O. Adewuyi, M. S. S. Danish, A. Howlader, T. Senjyu, and M. Lotfy, "Network structure-based critical bus identification for power system considering line voltage stability margin," *J. Power Energy Eng.*, vol. 6, pp. 97–111, Jan. 2018.

[64] X. Wei, S. Gao, T. Huang, T. Wang, and W. Fan, "Identification of two vulnerability features: A new framework for electrical networks based on the load redistribution mechanism of complex networks," *Complexity*, vol. 2019, pp. 3 531 209 2019.

[65] R. Diao *et al.*, "Decision tree-based online voltage security assessment using PMU measurements," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 832–839, May 2009.

[66] H. Mohammadi and M. Dehghani, "PMU based voltage security assessment of power systems exploiting principal component analysis and decision trees," *Int. J. Elect. Power Energy Syst.*, vol. 64, pp. 655–663, 2015.

[67] S. Paul, F. Ding, U. Kumar, W. Liu, and Z. Ni, "Q-learning-based impact assessment of propagating extreme weather on distribution grids," in *Proc. IEEE Power Energy Soc. General Meeting*, 2020, pp. 1–5.

[68] M. Mohammadi and G. Gharehpetian, "On-line transient stability assessment of large-scale power systems by using ball vector machines," *Energy Convers. Manage.*, vol. 51, no. 4, pp. 640–647, 2010.

[69] J. C. Cepeda, D. G. Colomé, and N. J. Castrillón, "Dynamic vulnerability assessment due to transient instability based on data mining analysis for smart grid applications," in *Proc. IEEE PES Conf. Innov. Smart Grid Technol. Latin America*, Oct. 2011, pp. 1–7.

[70] S. Zonouz and P. Haghani, "Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior," *Comput. Secur.*, vol. 39, pp. 190–200, 2013.

[71] R. C. Borges Hink *et al.*, "Machine learning for power system disturbance and cyber-attack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst.*, Aug. 2014, pp. 1–8.

[72] A. Keliris, H. Salehghaffari, B. Cairl, P. Krishnamurthy, M. Maniatakos, and F. Khorrami, "Machine learning-based defense against process-aware attacks on industrial control systems," in *Proc. IEEE Int. Test Conf.*, Nov. 2016, pp. 1–10.

[73] N. V. Tomin, V. G. Kurbatsky, D. N. Sidorov, and A. V. Zhukov, "Machine learning techniques for power system security assessment," *IFAC-PapersOnLine*, vol. 49, no. 27, pp. 445–450, 2016.

[74] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *Proc. Joint Workshop Cyber- Phys. Secur. Resilience Smart Grids*, Apr. 2016, pp. 1–6.

[75] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[76] S. Paul, Z. Ni, and C. Mu, "A learning-based solution for an adversarial repeated game in cyber-physical power systems," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 11, pp. 4512–4523, Nov. 2020.

[77] M. H. Athari and Z. Wang, "Impacts of wind power uncertainty on grid vulnerability to cascading overload failures," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 128–137, Jan. 2018.

[78] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the us power grid," *Saf. Sci.*, vol. 47, no. 10, pp. 1332–1336, 2009.

[79] L. Fu, W. Huang, S. Xiao, Y. Li, and S. Guo, "Vulnerability assessment for power grid based on small-world topological model," in *Proc. Asia-Pacific Power Energy Eng. Conf.*, 2010, pp. 1–4.

[80] K. Wang, B.-H. Zhang, Z. Zhang, X.-g. Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A, Statist. Mechanics Appl.*, vol. 390, no. 23/24, pp. 4692–4701, 2011.

[81] C. Pu, P. Wu, and Y. Xia, "Vulnerability assessment of power grids against link-based attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 10, pp. 2209–2213, Oct. 2020.

[82] J. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Gener., Transmiss. Distrib.*, vol. 4, pp. 178–190, Feb. 2010.

[83] A. Pinar, J. Meza, V. Donde, and B. Lesieutre, "Optimization strategies for the vulnerability analysis of the electric power grid," *SIAM J. Optim.*, vol. 20, no. 4, pp. 1786–1810, 2010.

[84] L. Zhao and B. Zeng, "Vulnerability analysis of power grids with line switching," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2727–2736, Aug. 2013.

[85] Y.-P. Fang, G. Sansavini, and E. Zio, "An optimization-based framework for the identification of vulnerabilities in electric power grids exposed to natural hazards," *Risk Anal.*, vol. 39, no. 9, pp. 1949–1969, 2019.

[86] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos*, vol. 19, no. 1, Mar. 2009, Art. no. 013119.

[87] F. H. Jufri, J.-S. Kim, and J. Jung, "Analysis of determinants of the impact and the grid capability to evaluate and improve grid resilience from extreme weather event," *Energies*, vol. 10, no. 11, 2017, Art. no. 1779.

[88] V. Latora and M. Marchiori, "Vulnerability and protection of infrastructure networks," *Phys. Rev. E*, vol. 71, Jan. 2005, Art. no. 015103.

[89] FiRST, *Common Vulnerability Scoring System 3.1: Specification Document*, 2019. Accessed: Mar. 3, 2020. [Online]. Available: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

[90] N. Jacobs, S. Hossain-McKenzie, and E. Vugrin, "Measurement and analysis of cyber resilience for control systems: An illustrative example," in *Proc. Resilience Week*, Aug. 2018, pp. 38–46.

[91] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proc. IEEE*, vol. 105, no. 7, pp. 1367–1388, Jul. 2017.

[92] V. Venkataramanan, A. K. Srivastava, A. Hahn, and S. Zonouz, "Measuring and enhancing microgrid resiliency against cyber threats," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6303–6312, Nov. 2019.

[93] S. H. Bouk, S. H. Ahmed, R. Hussain, and Y. Eun, "Named data networking's intrinsic cyber-resilience for vehicular CPS," *IEEE Access*, vol. 6, pp. 60570–60585, 2018.

[94] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019.

[95] H. M. Khalid and J. C. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, Jul. 2016.

[96] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[97] D. Jin *et al.*, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[98] A. Lu and G. Yang, "Resilient observer-based control for cyber-physical systems with multiple transmission channels under denial-of-service," *IEEE Trans. Cybern.*, vol. 50, no. 11, pp. 4796–4807, Nov. 2020.

[99] Office of Electricity, "North American energy resilience model," U.S. Dept. Energy, Washington, DC, USA, Jul. 2019.
[100] National Academies of Sciences and Medicine, *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC, USA: The National Academies Press, 2017. [Online]. Available: https://www.nap.edu/catalog/24836/enhancing-the-resilience-of-the-nations-electricity-system
[101] A. Kwasinski, "Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level," *Energies*, vol. 9, no. 2, 2016, Art. no. 93.
[102] S. Mukherjee, R. Nateghi, and M. Hastak, "A multi-hazard approach to assess severe weather-induced major power outage risks in the U.S.," *Rel. Eng. Syst. Saf.*, vol. 175, pp. 283–305, 2018.
[103] A. Bagheri and C. Zhao, "Distributionally robust reliability assessment for transmission system hardening plan under $n-k$ security criterion," *IEEE Trans. Rel.*, vol. 68, no. 2, pp. 653–662, Jun. 2019.
[104] Y. Mussard-Afcari, D. B. Rawat, and M. Garuba, "Data validation and correction for resiliency in mobile cyber-physical systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf.*, Jan. 2019, pp. 1–4.
[105] S. Mouelhi, M. Laarouchi, D. Cancila, and H. Chaouchi, "Predictive formal analysis of resilience in cyber-physical systems," *IEEE Access*, vol. 7, pp. 33741–33758, 2019.
[106] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.
[107] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber- Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016.
[108] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proc. IEEE*, vol. 105, no. 7, pp. 1389–1407, Jul. 2017.
[109] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. 50th IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 4066–4071.
[110] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.
[111] H. Haggi, R. R. nejad, M. Song, and W. Sun, "A review of smart grid restoration to enhance cyber-physical system resilience," in *Proc. IEEE Innov. Smart Grid Technol.—Asia (ISGT Asia)*, May 2019, pp. 4008–4013.
[112] Z. Li, M. Shahidehpour, R. W. Galvin, and Y. Li, "Collaborative cyber-physical restoration for enhancing the resilience of power distribution systems," in *Proc. IEEE Power Energy Soc. General Meeting*, Aug. 2018, pp. 1–5.
[113] A. Sanjab and W. Saad, "On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection," in *Proc. Joint Workshop Cyber Phys. Secur. Resilience Smart Grids*, Apr. 2016, pp. 1–6.
[114] Y. Wang, T. L. Nguyen, Y. Xu, Z. Li, Q. Tran, and R. Caire, "Cyber-physical design and implementation of distributed event-triggered secondary control in islanded microgrids," *IEEE Trans. on Ind. Appl.*, vol. 55, no. 6, pp. 5631–5642, Nov. 2019.
[115] V. Venkataramanan, A. Hahn, and A. Srivastava, "CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1055–1065, Mar. 2020.
[116] S. Lakshminarayana, J. S. Karachiwala, T. Z. Teng, R. Tan, and D. K. Y. Yau, "Performance and resilience of cyber-physical control systems with reactive attack mitigation," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6640–6654, Nov. 2019.
[117] S. Zuloaga, P. Khatavkar, L. Mays, and V. Vittal, "Resilience of cyber-enabled electrical energy and water distribution systems considering infrastructural robustness under conditions of limited water and/or energy availability," *IEEE Trans. Eng. Manage.*, to be published, doi: 10.1109/TEM.2019.2937728.
[118] S. Hossain-McKenzie, C. Lai, A. Chavez, and E. Vugrin, "Performance-based cyber resilience metrics: An applied demonstration toward moving target defense," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2018, pp. 766–773.
[119] G. Huang, J. Wang, C. Chen, and C. Guo, "Cyber-constrained optimal power flow model for smart grid resilience enhancement," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5547–5555, Sep. 2019.
[120] Z. Xu, D. J. X. Ng, and A. Easwaran, "Automatic generation of hierarchical contracts for resilience in cyber-physical systems," in *Proc. IEEE 25th Int. Conf. Embedded Real-Time Comput. Syst. Appl.*, Aug. 2019, pp. 1–11.
[121] M. A. Haque, G. K. De Teyou, S. Shetty, and B. Krishnappa, "Cyber resilience framework for industrial control systems: Concepts, metrics, and insights," in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, 2018, pp. 25–30.
[122] B. Potteiger, W. Emfinger, H. Neema, X. Koutsoukos, C. Tang, and K. Stouffer, "Evaluating the effects of cyber-attacks on cyber physical systems using a hardware-in-the-loop simulation testbed," in *Proc. Resilience Week*, Sep. 2017, pp. 177–183.
[123] E. Bellini, F. Bagnoli, A. A. Ganin, and I. Linkov, "Cyber resilience in IoT network: Methodology and example of assessment through epidemic spreading approach," in *Proc. IEEE World Congr. Serv.*, vol. 2642-939X, 2019, pp. 72–77.
[124] X. Zeng, Z. Liu, and Q. Hui, "Energy equipartition stabilization and cascading resilience optimization for geospatially distributed cyber-physical network systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 1, pp. 25–43, Jan. 2015.
[125] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Bie, "Microgrids for enhancing the power grid resilience in extreme conditions," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 589–597, Mar. 2017.
[126] J. Wang, S. Pambudi, W. Wang, and M. Song, "Resilience of IoT systems against edge-induced cascade-of-failures: A networking perspective," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6952–6963, Aug. 2019.
[127] S. Poudel, A. Dubey, and A. Bose, "Risk-based probabilistic quantification of power distribution system operational resilience," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3506–3517, Sep. 2020.
[128] S. Espinoza, A. Poulos, H. Rudnick, J. C. de la Llera, M. Panteli, and P. Mancarella, "Risk and resilience assessment with component criticality ranking of electric power systems subject to earthquakes," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2837–2848, Jun. 2020.