Renewable and Sustainable Energy Reviews 58 (2016) 1060–1069

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

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

On the definition of cyber-physical resilience in power systems

Reza Arghandeh [a,*], Alexandra von Meier [b], Laura Mehrmanesh [b], Lamine Mili [c]

[a] Center for Advanced Power Systems, Electrical and Computer Engineering Department, Florida State University, Tallahassee, FL, United States
[b] California Institute for Energy and Environment, Electrical Engineering and Computer Science Department, University of California-Berkeley, Berkeley, CA, United States
[c] Bradly Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Falls Church, VA, United States

ARTICLE INFO

Article history:
Received 6 April 2015
Received in revised form
12 October 2015
Accepted 17 December 2015
Available online 15 January 2016

Keywords:
Resilience
Power system
Cyber-physical system
Vulnerabilities
Smart grids
Microgrids

ABSTRACT

Modern society relies heavily upon complex and widespread electric grids. In recent years, advanced sensors, intelligent automation, communication networks, and information technologies (IT) have been integrated into the electric grid to enhance its performance and efficiency. Integrating these new technologies has resulted in more interconnections and interdependencies between the physical and cyber components of the grid. Natural disasters and man-made perturbations have begun to threaten grid integrity more often. Urban infrastructure networks are highly reliant on the electric grid and consequently, the vulnerability of infrastructure networks to electric grid outages is becoming a major global concern. In order to minimize the economic, social, and political impacts of large-scale power system outages, the grid must be resilient in addition of being robust and reliable. The concept of a power system's cyber-physical resilience centers around maintaining critical functionality of the system backbone in the presence of unexpected extreme disturbances. Resilience is a multidimensional property of the electric grid; it requires managing disturbances originating from physical component failures, cyber component malfunctions, and human attacks. In the electric grid community, there is not a clear and universally accepted definition of cyber-physical resilience. This paper focuses on the definition of resilience for the electric grid and reviews key concepts related to system resilience. This paper aims to advance the field not only by adding cyber-physical resilience concepts to power systems vocabulary, but also by proposing a new way of thinking about grid operation with unexpected extreme disturbances and hazards and leveraging distributed energy resources. The concepts of service availability and quality are not new, but many recognize the need of resilience in maintaining essential services to critical loads, for example to allow home refrigerators to operate for food conservation in the aftermath of a hurricane landfall. By providing a comprehensive definition of power system resilience, this paper paves the way for creating appropriate and effective resilience standards and metrics.

Contents

* Corresponding author.
E-mail address: arghandehr@gmail.com (R. Arghandeh).

http://dx.doi.org/10.1016/j.rser.2015.12.193
1364-0321/

1. Introduction

The astounding pace at which the electric grid now experiences energy resource diversification, digitalization, and aging means that critical electrical grids face greater and more frequent risks of intrusion and interruption. This is due to the fact that these electric power systems are merging with cyber systems, resulting in sociotechnical and cyber-physical systems that are creating an infrastructural Internet of Things (IoT) – where all grid components can talk and collaborate – most recently referred to as "smart grids" or "smart cities" for next generation of power systems and cities, respectively. A smart grid can strengthen the connection between information and communication technology (ICT) and advanced control systems. Synergy between the components of physical power, communications and cyber infrastructures may revolutionize grid efficiency and performance, but it also adds new cyber-access points. Increasing the number of access points increases the risk of physical damage by cyber-intruders. A recent report by the University of Cambridge estimates the United States cyber-related electrical grid interruptions to be in the range of $243 billion to $1 trillion [1]. To make matters worse, electrical grids are experiencing increased dynamics and complexity due to the intermittency of renewable energy resources. The interdependencies between electric power transmission and distribution systems create additional vulnerability to the power system as an interconnected entity. Power system vulnerability must therefore be evaluated from the physical, cyber and interdependency perspectives.

It is vital that the power grid can quickly recover with minimum damage after any intentional or unintentional outage. Severe weather is the leading cause of power outages in the United States, accounting for 87% of outages according to the 2013 report of the Executive Office of the U.S. President [2]. A recent congressional study estimates the cost of severe weather-related outages at an annual average of $25 to $70 billion [3]. It has been estimated that 90% of customer outages in the United States are related to distribution networks [4]. Moreover, power distribution systems historically are behind power transmission systems in terms of observability and monitoring system deployment. In the context of defining resilience, both transmission and distribution systems are taken into account. However, distribution systems need more attention in this area due to the future interconnection of a large number of distributed resources and microgrids.

This paper aims to take a step forward not only by clarifying the concept of resilience, but also by proposing a new way of thinking about grid operation during unexpected disturbances, especially in distribution networks. This paper is a follow up to [5]. There is no clear and universally accepted definition of cyber-physical resilience for power systems. The first step in designing, standardizing, and operating resilient power systems is to clarify the definition of resilience. Current literature on power system resilience presents many conflicting and vague descriptions. The following are the contributions of this paper:

1) The definitions of electric grid resilience in different publications do not always converge [6–8]. This paper provides a unified approach to define resilience in power systems. It presents a review of resilience definitions and concepts from related disciplines to ensure a complete and grounded definition of resilience in power systems.
2) Service outages are well-studied in transmission systems, but not in distribution systems. Service outages in the latter have been increasing in recent years due to an aging grid and more frequent natural disasters. The growing presence of distributed energy resources has made the grid more dynamic and complex [9]. Therefore, the relationships between the terms resilience, reliability and stability in power systems requires more careful articulation [10,11]. This paper proposes a time-based framework for defining resilience to extreme events that clearly differentiates it from concepts like reliability, which deals with average, more frequent disturbances.
3) The terms "robustness" and "resilience" are sometimes used interchangeably [12–14]. This is unfortunate, given that these are two different and sometimes mutually exclusive properties. Resilience hinges on flexibility and survivability in the face of unexpected extreme events, while robustness implies resistance to change [4]. This paper clarifies the differences between these two concepts in the context of power systems.
4) This paper clarifies differences between resilience and risk assessment objectives in the context of power systems. Some literature uses risk assessment methodology for system resilience; that may not be a perfect approach for power systems.
5) One major contribution of this paper is defining resilience in a cyber-physical framework. The modern grid is a mixture of information and communication technologies woven into the legacy physical electric grid. Today's grid is the energy Internet of Things. The proposed definition classifies vulnerabilities in three categories: physical, cyber and cyber-physical. To the knowledge of the authors, the proposed resilience definition is the most suitable, given the recent and upcoming changes in the electric grid, especially when taking the holistic view and extending the discussion to "smart cities".
6) This paper highlights the role of distributed energy resources for enhancing grid resilience, especially in distribution networks. The authors of this paper previously have proposed distributed energy resources for enhancing resilience in distribution networks and microgrids in their prior work [15]. As a follow-up, this paper provides a more refined use case to illuminate the importance of DERs in the context of smart grids.
7) This paper doesnot propose specific metrics for electric grid resilience. However, it does provide guidelines for developing power system resilience metrics in future work.
8) As others have noted, cyber-physical network resilience (CPR) must be a temporal, agile, and holistic practice that makes the electric grid less vulnerable to outages and reduces the time of service recovery [16]. This paper defines resilience in power systems and provides a review of key related concepts, including robustness, hazards, vulnerability, risks, capacity and severity, focusing on power distribution systems. It aims to clarify the similarities and differences between these concepts – most notably robustness, a frequently misused word that has a specific and important meaning in the context of power system operating states. These definitional considerations provide the basis for the discussion of cyber and physical threats in power systems, and possible actions to mitigate these threats within a resilient infrastructure.

The paper is organized as follows: Section 2 focuses on the concept of resilience, and Section 3 presents a framework for understanding cyber-physical network resilience (CPR). Cyber-physical vulnerabilities in power systems are addressed in

Section 4. In Section 5, distributed energy resources used for grid resilience enhancement are highlighted. Finally, Section 6 presents our conclusions and ideas for future work.

2. The "Pillars of Resilience" concept

Before defining resilience in power systems, other concepts related to risk, hazard, vulnerability and robustness need to be clarified. They are the most commonly used terms in literature discussing system resilience. For risk concepts, the established analytic approaches for risk assessment can be of use in resilience analysis. For robustness concepts, in system engineering and control theory communities, "system robustness" is another concept used for system response in the presence of disturbances. Section 2.3 is devoted to comparing robustness and resilience concepts explicitly in power systems.

2.1. From risk assessment to resilience

Risk and risk analysis are popular topics for scientists, engineers and politicians. While "risk" has different meanings in economics, business, politics and infrastructure, some common themes emerge. Risk assessment has been matured over the decades to analyze system damage probability following perturbations. This section aims to clarify the concept of risk in power systems to build a framework for a definition of resilience. Some literature uses risk assessment methodology for system resilience; that may not be a perfect approach. In infrastructure engineering, a discipline closely related to power systems, risk is assessed by two factors, the likelihood of an undesirable event and the consequence of that event [17].

Definition 1. Risk is the possibility of an undesired event and its sequenced loss [17].

In risk assessment, an event's occurrence likelihood and its consequences are characterized by probability distribution functions [18,19]. For example, the risk of an overhead conductor line to ground fault is the probability of a line to ground short-circuit and the fault consequences for customers. A common approach for risk quantification is the triplet representation of the risk from Kaplan[19]. It focuses on the scenario, likelihood and consequence of the risk.

Corollary 1. The risk frequency and consequence are expressed in a set of probability distribution functions (PDF)[19]:

$$\text{Risk}_i = \{\langle S_i, f_i(\varphi_i), g_i(\xi_i)\rangle\} \quad ,i = 1, 2, \ldots \tag{1}$$

where S_i, $f_i(\varphi_i)$, and $g_i(\xi_i)$ are risk scenario, likelihood PDF and consequence PDF for hazard i.

The Pressure and Release (PAR) risk model by Wisner [20] is another popular approach for risk modeling. The PAR model views disasters as the intersection of vulnerability and hazards. It has three determinates: hazard, capacity and vulnerability [21].

Definition 2. A hazard is an event or set of events that is the source of potential damage. Hazards cause concerns for system owners and operators [22].

In Corollary 1, the i subscript refers to possible hazards. The properties of hazard-generating sources are usually unknown, so they are represented with probability rules. The behavior of the system subjected to hazardous events can be probabilistic or deterministic. Hazards in power distribution networks can be natural phenomena such as vegetation, lightning, severe weather, and animals. Other types of hazards include malicious and terrorist attacks.

Definition 3. Capacity is the ability of a system to adapt to imposed changes and moderate potential damage [23].

For example in power systems, capacity is part of system planning for reserve capacity, conductor over-sizing and line redundancy. In generation, capacity can be in the form of spinning reserve for frequency droop control.

Definition 4. Vulnerability is a condition or a process resulting from a given (natural or man-made) hazard and is defined as the joint conditional probability distribution of hazard likelihood, hazard potential impact and system capacity [24].

Definition 5. Severity is the statistical likelihood of hazards according to historical data.

Corollary 2. Given the hazard i and $i \subseteq H$ where H is the set of possible hazards for the system, the vulnerability function will be:

$$\text{Vul}_i = f(\varphi|i) \times g(\xi|i) \tag{2}$$

where f is the conditional PDF for the hazard potential impact φ relative to the hazard i, and g is the conditional PDF for the system capacity ξ relative to the hazard i.

Drawing upon the definitions of the PAR model basics in Corollary 1, Corollary 3 describes the PAR mathematical formulation.

Corollary 3. The Pressure and Release (PAR) model of risk [25] is:

$$\text{Risk}_i = \text{Vul}_i \times \text{Severity} \tag{3}$$

where the Vul_i is the vulnerability for hazard i.

Risk assessment based on hazard and vulnerability is a framework that presents risk in both a system behavior context and a physical characteristics context [26]. Wisner [20] provides a conceptual PAR risk framework (see Fig. 1).

As Fig. 1 shows, the damage of a system following the disturbances is a function of four different parameters, probability of the disturbance, severity of the disturbance, system vulnerability, and system capacity to absorb the disturbance (Fig. 2).

Understanding the nature of a risk and its consequences and perturbations in a network is part of risk assessment procedure. While understanding risks is an important first step, the ultimate goal is to build power systems that are both resistant and resilient in the face of average and extreme risks. Resistance refers to robustness to common events, which is opposed to resilience, which requires flexibility and agility in the face of extreme risks. Modern power systems need to adopt mechanisms to cope with risks and recover from outages quickly. The next section is focused on the concept of resilience in the context of the electric grid.

2.2. The meaning of resilience

The electric grid is a socio-ecological system with different spatial, temporal, and organizational parameters that are affected

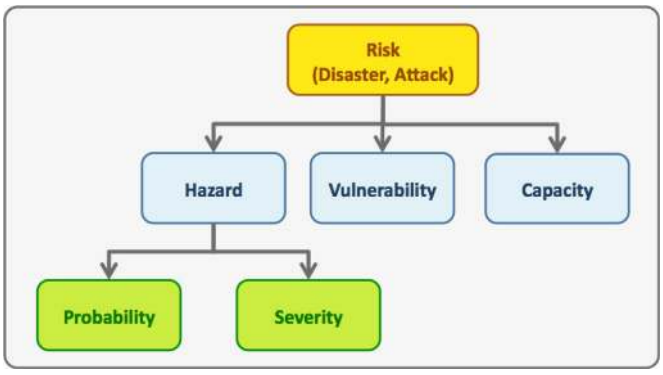

Fig. 1. Conceptual PAR risk framework [20].

by policy, economy and society. Therefore, definitions of resilience in other disciplines can help us build an expressive definition of resilience in power systems. Definitions of resilience have evolved and expanded over the years. In 1973, Holling [27] defined resilience as the ability of a system to maintain its functionality and behavior after a disturbance. Gunderson et al. [28] modified the definition by adding buffer capacity for absorbing perturbations in a timely fashion. Walker et al. [29] extended the definition to include the ability to self-heal during disturbances. Kendra et al. [30] described "bouncing back from a disturbance" as a crucial aspect of resilience. The breadth of and number of definitions for "resilience" has increased significantly over the last decade, making it difficult to find a universal understanding of the term "resilience".

Table 1 presents different definitions for resilience in various disciplines. It shows how resilience definitions share similar concepts from different perspectives. The power systems community needs a tailored resilience definition that includes physical and cyber network characteristics and service outage consequences.

Resilience is especially critical immediately following an event that challenges system performance and functionality. Such events are given various names by different authors from various disciplines. A hazard, Definition 2 in this paper, is one such name for these events. Table 2 lists some of the other labels used. These terms describe consequences of rapid changes both in the environment and in system operation that are caused by system/component failures, attacks and natural disasters. From this point forward in the paper, "disturbing events" will include all of the terms in Table 2 and other similar terms.

Definition 6. The resilience of a system presented with an unexpected set of disturbances is the system's ability to reduce the magnitude and duration of the disruption. A resilient system downgrades its functionality and alters its structure in an agile way.

Cyber-physical resilience assessment is often based on risk assessment [45,46], which may not be the best approach for providing a system with a given degree of resilience. Risk assessment is the likelihood of failures in a probabilistic language. Resilience is about mitigation of unexpected rare extreme failures, whose likelihood cannot be estimated from historical data (i.e., the black swan metaphor). Resilience assessment depends on the temporal dimension of potential disturbances and mitigating actions. Resilient structures find strategies to keep the functionality of the backbone of the system [4] in the face of extreme events. However, risk assessment centers around the probability of hitting a system's weak points.

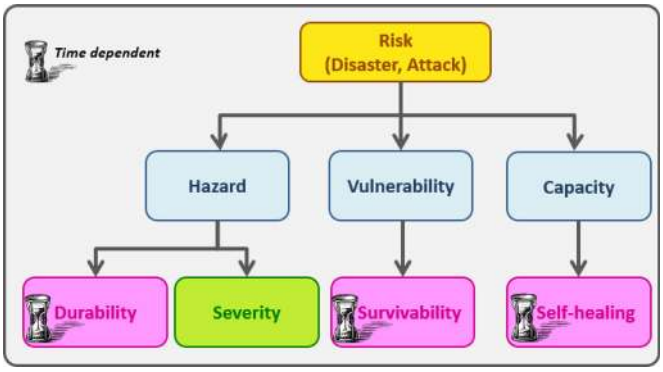

Fig. 2. Comparing a resilience framework to a PAR risk analysis framework.

In terms of a system's response to disasters, attacks and failures, risk assessment is a general framework to evaluate damage to the system performance and functionality. The risk assessment goal is situational awareness and diagnostics. However, resilience is taking one step forward while taking quick actions to maintain critical system functionality via remedial action schemes such as system islanding, generation outages and load shedding [47].

In resilience operations, response time and service availability are key. In the next sections, a more refined definition of resilience for power systems is presented.

2.3. Going beyond robustness

In the wake of unprecedented disasters and attacks, robustness and resilience have become buzzwords in many disciplines, including biology, ecology, sociology, systems engineering and infrastructure engineering. The traditional definition of resilience in systems engineering is the capacity for fast recovery after stress and for enduring greater stress [48]. In systems engineering, resilience includes maintaining system functionality following disturbances. Robustness, on the other hand, refers to the ability of a system to resist change without losing stability [5]. A more generic definition of robustness is:

Definition 7. Robustness is the ability of a system to cope with a given set of disturbances and maintain its functionality.

Robustness and resilience belong to two different design philosophies. Robustness is concerned with strength, whereas resilience is concerned with flexibility. When a robust grid is attacked, it may break like an oak tree in a storm. When a resilient grid is attacked, it can bend and survive like a reed in a storm [5]. From a systems engineering point of view, absolute robustness can actually lead to fragility [49].

Table 2
Different terms for "disturbing events" used in system resilience literature.

Term	Ref	Term	Ref	Term	Ref
Perturbations	[35]	**Losses**	[36]	**Anomalies**	[34]
Disturbances	[34]	**Adversity**	[37]	**Threats**	[38]
Disruptions	[39]	**Emergency**	[40]	**Shocks**	[41]
Events	[42]	**Changes**	[43]	**Hazards**	[44]

Table 1
Different definitions of resilience from different disciplines.

Discipline	Definition of "resilience"	Ref
Infrastructure systems	The ability to reduce the magnitude and duration of disturbances. It depends upon the system's ability to predict, absorb and adapt to disturbances and recover rapidly.	[31]
Economic systems	The response to hazards that enables people and communities to avoid some economic losses at micro–macro market levels. It is the capacity for the enterprise to survive and adapt following market or environmental shocks.	[32]
Social systems	The ability of a community to withstand stresses and disturbances caused by social, political and economic changes.	[33]
Organizational systems	The ability of an organization to identify risks and to handle perturbations that affect its competencies, strategies and coordination.	[34]

In some disciplines like social systems and organizational systems, resilience and robustness are interchangeably used.

Remark 1. The more an infrastructure network is designed to be robust against one set of disturbances, the more fragile it is when faced with a different set of disturbances [49]. Therein lies the fundamental connection and conflict. Extreme robustness actually leads to fragility. High level of robustness leads to system brittleness and, thereby, to vulnerability to large-scale failures via cascading events. Moreover, the term robustness is usually used with specific assumptions for protection system operation under predefined operational ranges for voltage and loading.

Remark 2. Robustness is embedded in the system's design, whereas resilience is typically integrated into the system's operational components like its control system [4]. Robustness is defined against specific threats to the system. For example, distribution poles have to withstand earthquakes and wind speeds up to a certain level of structural stress and strain. System robustness requires stronger coupling between network components, like replacing overhead lines with underground cables. Resilience, on the other hand, demands flexibility, adaptability and agility. Dynamical system components like loads and distributed generation force sudden changes in system behavior. Resilient power systems know how to reroute electricity to customers using alternative paths and alternative local sources during natural disasters.

Robustness in the enterprise world is more focused on asset utilization, whereas resilience centers around service quality. Robustness is embedded in the system architecture design; resilience is more concerned with system operation and control. Robustness can be a passive approach for system security. Distribution pole hardening and putting cables underground are examples of passive system security enhancement. Resilience, on the other hand, is an active approach with real-time reactions to disturbances. Resilience can mean a set of real-time switching and islanding actions. Resilience can involve explicitly partitioning the grid into different sub-systems (for instance, sub-systems of microgrids). Robust electric grids aim at maintaining system functionality via additional component redundancy in transmission and in generation and via transmission line switching (that is, topological changes) and local control actions that convert destabilizing injected kinetic energy by the faults into potential energy resulting from enhanced system stability margins. Resilient networks, on the other hand, rely on agility and flexibility to cope with extreme disturbances. Therefore, segmentation into multiple coupled sub-systems with flexible interties are crucial in resilient systems. Table 3 compares robustness and resilience against different criteria. Only expected failures are in the blueprint of a robust system design. Unexpected failures may lead to catastrophic failures in robust systems. This is the realm of resilience, not robustness.

Reliability and stability are two more explicit power systems concepts that pre-date the terms “robustness” and “resilience” [5]. Reliability and stability are well-studied concepts in power systems. Similarities and dissimilarities between them and the terms robustness and resilience can inform future cyber-physical resilience studies. Reliability in power systems is the ability of grid components to meet all consumers' demand for electricity with acceptable power quality. The concept of reliability is also used in industrial and systems engineering and is accompanied by statistical and probabilistic approaches that characterize system performance following a collection of predicted failures.

Table 3
Robustness vs. resilience in power systems.

Criteria	Robustness	Resilience
Application	Network hardening	Network flexibility
Enterprise focus	Utility assets	Utility services
Value proposition	Design	Operations
Security approach	Passive	Active
Network preference	Isolated	Interdependent
Network segmentation	Few	Multiple

Definition 8. Reliability is the ability of the power system to deliver electricity to customers with acceptable quality and in the amount desired while maintaining grid functionality even when failures occur [50,51].

Discussions of resilience often center around a system survivability that leverages load shedding, generation outages, and other actions. Reliability is a measure of the system's ability to serve all loads. The system's ability to serve loads is traditionally referred to as service availability, which falls under the power systems definition of reliability. Reliability indices are usually expressed in terms of the Loss-of-Load Probability (LOLP) [5,47], which is in fact not a probability, but the expected number of days per year that generation does not meet demand. The basic mathematical definition of reliability is presented in the next corollary. Reliability is primarily concerned with the risk of service interruption or device failure.

Corollary 4. The device failure at a random time $T>0$ has the cumulative failure distribution function $F(t)$, probability density function $f(t)$ and reliability $R(t)$ as follows:

$$F(t)=P(T\le t) \tag{4}$$

$$R(t)=1-F(t) \tag{5}$$

The next concept to clarify is the term “stability”. Generally, stability is the system's ability to tolerate small perturbations. The concept of stability also comes up in control [52] and robust estimation theory [53]. Here, small disturbances stem from uncertainties in measurements and system models. The general definition of stability is as follows:

Definition 9. Stability is the ability of a system to remain intact after being subjected to small perturbations [54].

In power systems, stability for a given initial operating condition means the system will regain operation equilibrium state after small perturbations. Stability is focused on stability of equilibrium points. However, the concept of robustness in power systems goes beyond stability. In order to be robust and resilient, the electric grid has to be able to cope with small disturbances as well as major equipment failures, man-made attacks, and natural disasters [54].

The previous sections built a foundation for defining resilience in power systems and terms that overlap with resilience, such as robustness, stability and reliability. The next section presents a definition of electric grid cyber-physical resilience.

3. A framework for power system cyber-physical resilience

Understanding the nature of risk, its sources and its consequences is a major goal of risk assessment for a system. In power systems, in addition to the need for risk assessment, there is a need for actions performed in a timely manner to protect system functionality against risks, rapid changes and threats. Power systems are continually exposed to changing environmental and operational conditions caused by internal and external factors. The definition of resilience for power systems should be more holistic,

rigorous and dynamic than what is encompassed by the term “risk assessment”. Moreover, the electric grid is a complex, large scale and physically connected system with strong interdependencies between its components. A steady supply of electricity is vital for critical loads and facilities. However, continuous electricity delivery following natural and man-made disasters cannot be ensured without prioritizing loads and resources in response to disturbances. Power system resilience includes the survivability of the system and the system's ability to absorb the disturbances without losing its functionality. The following is a proposed definition for power system cyber-physical reliance.

Definition 10. Power system cyber-physical resilience is the system's ability to maintain continuous electricity flow to customers given a certain load prioritization scheme. A resilient power system responds to cyber-physical disturbances in real-time or semi real-time, avoiding interruptions of critical services. A resilient power system alters its structure, loads, and resources in an agile way.

Power system cyber-physical resilience centers around the system’s ability to recognize, adapt to, and absorb disturbances in a timely manner. Resilient system operation focuses on monitoring the system's boundary conditions to detect disturbances and adjusting control actions accordingly. Continuously monitoring the system creates a situational awareness for assessing risk, and supports system flexibility to mitigate disturbances. Power system resilience includes understanding the system’s boundary conditions and their changes during disturbances [34].

Resilience is the system’s ability to endure disturbing events in two ways: by absorbing disturbances (“absorbing potential”) and by recovering from disturbances (“recovery potential”). Resilience implies that the system can absorb disturbances, adapt to the new parameters and recover fast enough to mitigate the effects of the disturbing event.

Comparing a resilience framework to a risk assessment model (Fig. 1), we can see that power system resilience goes beyond the PAR model. First of all, in addition to knowing the severity of the hazard, one must know how long the system is being exposed to the hazard. Second, the probability of a disturbance is not a crucial factor in resilience, unlike in risk assessment. E.g., a longer duration storm causes more damage to the grid and requires more of a real-time resiliency response, whereas a merely more likely storm does not. This can be illustrated by considering how the impact varies according to the amount of time that a tree branch is touching an overhead line while its protection systems are not tripping. The longer the branch lies on the energized conductor, the longer the short circuit current the system experiences.

As mentioned above, power system resilience is the electric grid's ability to survive disturbances. Resilience in power systems depends on the reaction time following a disturbance that maintains service availability. To modify the PAR model for grid resilience, the system vulnerability in the time domain is changed to system survivability. Similarly, system capacity for resilience is based on the self-healing characteristics of the network. Durability, survivability, and self-healing are time-dependent factors for power system resilience.

Resilience assessment requires knowledge of the power system’s dynamic behavior and the system’s flexibility in accommodating sudden changes without a tremendous decline in its performance. Therefore, a resilience assessment framework starts with system identification and model validation. Network topology, physical characteristics, operational constraints and dynamic behaviors are established in the system identification step. Topology detection and state estimation are integrated into the system identification process.

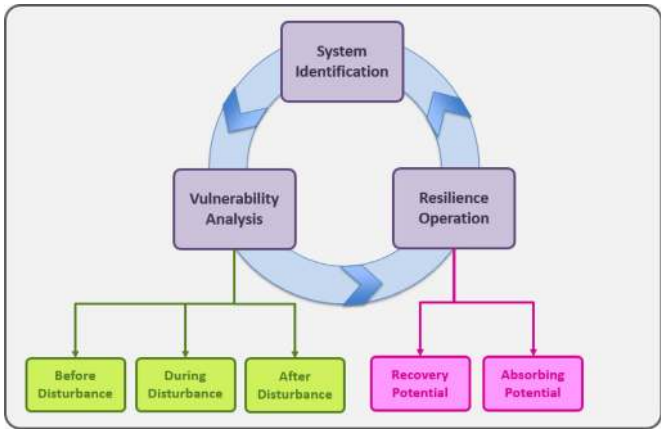

Fig. 3. Our resilience assessment framework for power systems [15].

The next step is system vulnerability analysis. The next section reviews different vulnerabilities in power systems. Due to the randomness of disturbing events, their consequences are presented according to their likelihood in probability language. As the consequences of disturbing events are time-dependent, the temporal dynamics of disturbing events must be considered in resilience assessment [17]. In addition to the disturbing events’ consequences, the system’s adaptability and its recovery speed are crucial time-dependent factors that must be taken into account. Hence, vulnerability analysis includes the system response before, during and after disturbances. Vulnerability assessment is a continuous process; the evaluation of disturbing events and the consequences of the system’s response to the events is ongoing.

The other component of the system resilience framework is the resilient operation. The ultimate goal of a resilient system is to maintain system functionality of its backbone while ensuring essential service to all the customers after extreme disturbing events. Resilient operation control defines new settings and equilibrium points for system operation. It has two main components, recovery potential and absorbing potential. These potentials are embedded in the resilience operation settings. Fig. 3 depicts our proposed resilience framework for power transmission and distribution networks.

Prior literature defines the absorbing potential as the degree to which a system can absorb the consequences of disturbing events [55]. The disturbance absorption in power systems depends on the components' design characteristics, the system topology, the control philosophy, and the protection coordination.

The recovery potential is the system’s ability to alter itself in undesirable situations by recognizing disturbing events and reorganizing itself [21]. A quick return to normal operation or a restorative operation state is an important part of the recovery potential. The next section reviews common cyber-physical vulnerabilities, summarizing the current discourse in power system resilience operations.

4. Vulnerabilities in power systems

Power transmission and distribution systems are greatly dispersed over a large geographical area and highly complex nonlinear engineering systems with different degrees of connectivity and multiple time-scale dynamical behaviors. One of the key issues is that the dynamic electricity supply and demand balance needs to be maintained in real-time. Natural disasters, severe weather conditions and attacks make reliable operation a very difficult task. Electricity transmission and distribution networks as cyber-physical systems are a combination of physical grid

components, sensors, communication devices, databases and software. Therefore, disturbing events in power systems can be organized into: 1) events in the physical grid components, grid structure and sensors, 2) events in the cyber infrastructure, software applications and data communication and 3) correlated events in power system components that have both cyber aspects and physical aspects, like control systems and state estimation systems.

4.1. Physical vulnerabilities

Physical vulnerabilities are primarily due to the disruption of aerial distribution and transmission lines during and after severe weather. Faults caused by contact between conductors and ground are the source of circuit breakers locking out, safety hazards and fires. The second most vulnerable components are transformers. Hardening the distribution lines is one approach for preventing or mitigating the catastrophic effect of weather-related disruptions. Structurally reinforcing towers and poles is one effective way to increase robustness [56]. Vegetation management is crucial for preventing faults, especially in distribution networks. It is worth noting here that almost 90% of customer outages in the United States are related to power distribution system problems [4].

In risk assessment studies, a common practice for determining infrastructure physical vulnerability is performing the fragility curve estimation [57]. This estimation method can also be used in resilience assessment. Han et al. [58] used data from a utility on the Gulf Coast to estimate fragility of overhead lines as a function of wind speed. Vickery et al. [59] introduced a curve-fitting technique for modeling structural damages. Francis et al. [60] presented underground lines' fragility curves.

There are extensive studies on the impacts of storms and natural disasters on the electric grid. Ref. [61] is a study on storms in Florida and their impacts on infrastructure. A more recent study on storm impacts on the grid and related state level legislation is presented in Ref. [62].

4.2. Cyber vulnerabilities

Cyber-attacks and intrusions have been on the rise in recent years all over the world. As our power grid has gotten smarter, its components' communication abilities and information technology sophistication levels have increased. Unfortunately, that has resulted in an increase in the number of intrusion access points. Cyber intrusions can divulge critical data and measurements and cause a Denial of Service (DoS). Malicious commands and measurement injections can lead to widespread damage.

Remark 4. Cyber-attacks can be classified into four categories: 1) Reconnaissance, 2) Denial of Service (DoS), 3) Command Injection, and 4) Measurement Injection [63,64].

The Department of Homeland Security [66] and the National Institute for Standards and Technology [65] have published assessments of cyber vulnerabilities in engineering systems. Table 4 shows some of the aforementioned vulnerabilities in smart grid related cyber systems. This list provides an overview of potential cyber-attacks on smart grids and the appropriate mitigation activities. Ten et al. and Hahn et al. [67,68] have analyzed different types of cyber attacks on smart grid monitoring and protection systems.

4.3. Cyber-physical vulnerabilities

The link between physical and cyber components in power systems makes it easy for cyber intrusions to cause physical damage to grid components [63]. Intelligent electronic devices

Table 4
Some of the cyber vulnerabilities in smart grids [65,66].

Category	Common vulnerability
Software domain vulnerability	1. Improper Input Data Validation 2. Poor Code Quality 3. Permissions and Access Control 4. Cryptographic Issues 5. Improper Software Configuration 6. Software Maintenance Issues
Access domain vulnerability	1. Permissions, Access and Privileges Control 2. Incorrect Authentication 3. Improper Security Configuration 4. Access Policy and Procedures Issues 5. Credentials Management
Network domain vulnerability	1. Improper Network Configuration 2. Weak Firewalls 3. Improper Network Component Configuration 4. Network Audit and Monitoring Issues

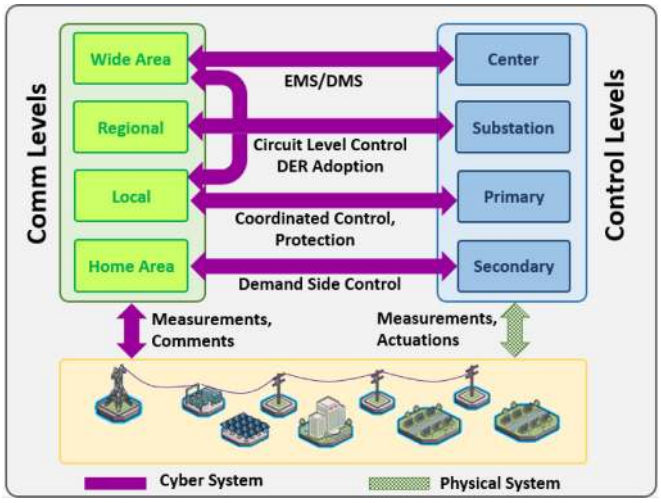

Fig. 4. A Typical cyber-physical control system for an electricity grid.

(IEDs) and, in general, measurement devices with embedded communication and data processing, are used for different levels of control and protection in power systems. Control systems are where the cyber and physical systems come together. Cyber-physical vulnerability analysis should therefore start with the control systems, as suggested in industrial control security guidelines [66]. There are a number of research studies on cyber and physical interdependencies in control systems. Laprie et al. [16] analyze cascading failures that follow cyber-attacks on infrastructure control systems. Sridhar et al. [69] present a classification method for control system vulnerabilities for electric grid risk assessment. Qi et al. [70] propose a robust control algorithm for mitigating impacts of cyber attacks on power systems. Fig. 4 illustrates the typical cyber-physical control system architecture for power systems.

Fig. 4 displays how measurement and control actuation signals are exchanged amongst physical network components. The solid arrows show the data path between different measurement and control components through communication lines. The communication links at the secondary control level of the distribution network and at the load level include advanced metering infrastructure (AMI) and home area network (HAN) technologies. The IEC 61850 standard is used for communication between coordinated control devices (voltage regulators, reclosers, breakers, etc.) and substations.

The Supervisory Control and Data Acquisition (SCADA) systems, AMI, and Distributed Energy Resource (DER) control systems play a major role in power system reliability services. These cyber-physical control and communication systems must be resilient against extreme disturbing events while maintaining acceptable grid performance under any circumstances. SCADA and AMI cyber-security issues have been explored by many researchers [71–74], but intelligent cyber-physical disturbance detection and the impact of DER on cyber-physical resilience has gotten less attention [75,76].

5. Distributed energy resources in microgrids, a case study for system resilience

A resilient power system needs structural flexibility, modularity and distributed decision-making integrated with intelligent control and communication capabilities. Unfortunately, electric grid observability is a major challenge, especially in distribution networks. Power system resilience requires detailed knowledge of the system's behavior in three time scales, historical, real-time, and forecasting, to develop effective controls and remediation actions. Present monitoring systems do not typically have such extensive knowledge, especially in the presence of intermittent renewable energy resources [77].

Yet, despite the physical connectivity of the electrical grid and the space-time correlations in wide area systems, measurement data from various sensors are not processed in an integrated and synchronized fashion. If they were, we could see a holistic unified spatiotemporal picture of grid behavior. A well-designed monitoring system could be the backbone of system observability, capturing power system stresses, disturbances, and component failures that cause outages and service interruptions. In recent years, power transmission systems have been equipped with time-synchronized phasor measurement units (PMUs) to monitor system stability. Distribution systems, however, are lagging behind in this regard. Technologies like micro-synchrophasors and line sensors can help fill the gap [78].

The fact that power systems are merging with cyber systems means we now have cyber-physical systems and a resultant infrastructural Internet of Things (IoT), or "smart cities". These smart cities including microgrids are highly interconnected entities that are to prone disturbances in different temporal and spatial scales. To minimize the impacts of disturbances, resilient controllers can shed lower priority loads. Grid partitioning, suggested in earlier work, can be of use. Breaking distribution systems into islands [79], building AC and DC microgrids [9,80], adopting more distributed energy resources (DER) [81], using intelligent power flow control systems [82] and creating distributed agent-based distribution network control systems [83] are all examples of efforts to find a general solution for contingency reduction, power flow control and flexible grid operation. Clark *et al.* [9] suggest segmenting the grid into asynchronous sub-systems with HVDC interconnections and converter interfaces. HVDC links let different sub-systems have independent frequency responses to disturbances. Grid segmentation lets system operators control power flows inside each segment while mitigating instabilities and cascading failures in the larger system when subject to a major disturbance. In the extreme case, one segment may collapse while other segments remain alive.

The advent of distributed energy resources (DER), such as renewable generation, electric vehicles, and controllable loads introduces great opportunities to help the grid survive and recover from extreme events. DER can provide local energy as well as more advanced ancillary services, even after extreme events. As illustrated in Fig. 5, a solution can be achieved with a combination of

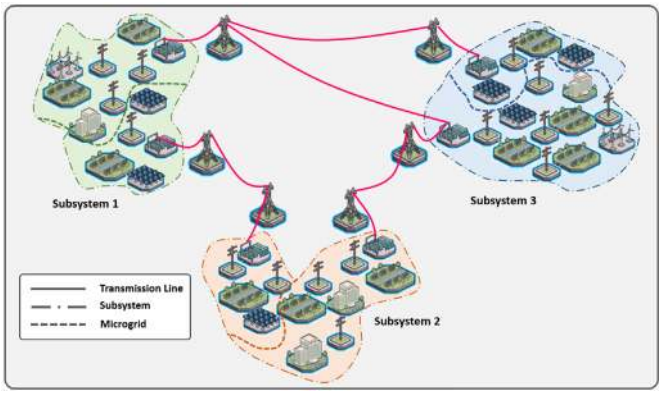

Fig. 5. Schematic of transmission and distribution networks with island operation capabilities.

intelligent contingency control on the transmission side along with DER adoption and microgrids on the distribution side. The interconnected power transmission and distribution systems need sufficient numbers of measurement devices, coordinated control devices, and a communication network and hierarchical control system for data transmission and analysis. The resilient distribution management system maintains distribution networks' functionality with DER control, grid partitioning, load prioritizing, load shedding, and switching actions, along with new assumptions for equality and inequality constraints [15].

The intelligent distribution management system uses real-time control schema during emergency conditions. It takes advantage of a time-synchronized monitoring system for disturbance/failure detection via an updated alarm mechanism. With an intelligent distributed control system, DER, controllable loads, energy storage units, and switches can all participate in making the grid more resilient during and after disturbances. The current state of DER operation is the result of current standards and interconnection agreements that were developed when the penetration of distributed resources was low. Given the significant number of distributed resources that now exist at many utilities, and the forecasted growth of distributed resources, it is prudent to explore whether or not utilities could further leverage these resources in response to extreme events.

The IEEE1547 standard and Rule 21 from the California Energy Commission are initial efforts to regulate the interconnection, operation and measurement requirements for distributed energy resources. These regulations can be used as the basic standard for upcoming resilient grid operation frameworks with DER interconnections.

6. Conclusions and future work

Most electric grid operators have recognized the need to transition from a conventional grid to a smart grid, or even further, to the Infrastructural Internet of Things, or smart cities. Technically speaking, a smart grid is an electric grid with increased utilization of information and communications technology (ICT). The ICT infrastructure collects, distributes, analyzes, and responds to the behavior of all components to improve the quality of service and maintain the energy flow. Cyber-physical resilience is crucial for smart grid operators and stakeholders. However, power system cyber-physical resilience is not well defined yet; this is due to the lack of interpretability standards, limited real-time data, and poor observability in power distribution systems.

First and foremost, this paper provides a clear definition of concepts related to service availability such as reliability,

robustness and risk assessment.. Since “robustness” and “reliability” are often misapplied, the authors then elucidate the differences between those terms and the term resilience in the context of power systems. Second, this paper provides a review of resilience concepts in other disciplines to lay the foundation for a holistic definition of resilience for the power system community. Third, it proposes a framework for defining resilience in power systems that divides the ways the system endures extreme disturbing events into two categories: absorbing disturbances and recovering from disturbances. Both capabilities are time-varying components of the system behavior that mitigate the effects of the disturbing events. A resilient system must go beyond risk assessment and carry out a set of actions in a timely manner to ensure adequate system functionality in the face of risks, sudden changes and threats. Power systems are continually facing variable operational conditions caused by internal and external factors. We posit that the concept of resilience in infrastructural systems must be centered on more holistic, rigorous and temporal analyses than those typically performed in traditional risk assessment.

The proposed framework shows the emerging need for advanced monitoring systems and measurement data analysis to detect, locate and evaluate disturbances quickly. Moreover, the actual monitoring systems in power transmission and distribution systems lack the sophistication to observe interdependency between different system levels. Additionally, cyber-physical interoperability has become more challenging with the advent of distributed energy resources and the adoption of Internet of Things (IoT) concepts in power systems. The dependencies between cyber and physical components have to be considered both when studying resilience itself and when creating a resilience assessment framework for power systems. The proposed resilience framework considers system vulnerability in physical, cyber and cyber-physical domains. This paper also suggests developing new standards and modifying available standards to address interoperability, monitoring system design, and cyber-physical interdependency issues for the resilient operation of the electric grid.

This paper does not include quantitative benchmarks for cyber-physical resilience. However, this paper does serve as a guideline for developing such metrics. Future work will focus on developing multidimensional time-dependent metrics for measuring cyber-physical resilience with several factors in mind, namely disturbance durability, recovery potential and absorbing potential of the cyber-physical power system.

References

[1] Maynard T, Beercroft N. Business blackout, in innovation series. Cambridge, UK: Lloyd's and the University of Cambridge Centre for Risk Studies; 2015. p. 61.
[2] President EOot. Economic benefits of increasing electric grid resilience to weather outages. United States: The White House Office of Science and Technology; 2013.
[3] Campbell RJ. Weather-related power outages and electric system resiliency. United States: Congressional Research Service, Library of Congress; 2012.
[4] Beaty W. Electric power distribution systems: a nontechnical guide. Tulsa, Oklahoma, United States: PennWell Books; 1998.
[5] Mili L, Center NV. Taxonomy of the characteristics of power system operating states. In: 2nd NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop. Tuscon, Arizona; 2011.
[6] Gouveia, C, Moreira J, Moreira C, Pecas Lopes J. Coordinating storage and demand response for microgrid emergency operation.
[7] Momoh JA. Smart grid design for efficient and flexible power networks operation and control. In: Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES, IEEE; 2009.
[8] Lu Z, Lu X, Wang W, Wang C. Review and evaluation of security threats on the communication networks in the smart grid. In: Military Communications Conference, 2010-MILCOM 2010, IEEE; 2010.
[9] Clark H, Edris AA, El-Gasseir M, Epp K, Isaacs A, Woodford D. Softening the blow of disturbances. Power Energy Mag IEEE 2008;6(1):30–41.
[10] Lachs W. Controlling grid integrity after power system emergencies. Power Syst IEEE Trans 2002;17(2):445–50.
[11] Rehtanz C, Bertsch J. Wide area measurement and protection system for emergency voltage stability control. In: Power Engineering Society Winter Meeting, IEEE; 2002.
[12] Little RG. Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences, IEEE; 2003.
[13] McDaniels T, Chang S, Cole D, Mikawoz J, Longstaff H. Fostering resilience to extreme events within infrastructure systems: characterizing decision contexts for mitigation and adaptation. Glob Environ Chang 2008;18(2):310–8.
[14] Zhu Q, Basar T. Robust and resilient control design for cyber-physical systems with an application to power systems. In: Decision and Control and European Control Conference (CDC-ECC), 50th IEEE Conference on, IEEE; 2011.
[15] Arghandeh R, Brown M, Del Rosso A, Ghatikar G, Stewart E, Vojdani A, von Meier A. The local team: leveraging distributed resources to improve resilience. Power Energy Mag IEEE 2014;12(5):76–83.
[16] Laprie J-C, Kanoun K, Kaâniche M. Modelling interdependencies between the electricity and information infrastructures. In: Computer safety, reliability, and security. Springer; 2007. p. 54–67.
[17] Haimes YY. On the complex definition of risk: a systems-based approach. Risk Anal 2009;29(12):1647–54.
[18] Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. San Mateo, CA, United States: Morgan Kaufmann; 1988.
[19] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1(1):11–27.
[20] Wisner B. At risk: natural hazards, people's vulnerability and disasters. Routledge, NY, United States: Psychology Press; 2004.
[21] Francis R, Bekera B. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab Eng Syst Saf 2014;121(0):90–103.
[22] Singley JA. Hazard versus risk. Chem Health Saf 2004;11(1):14–6.
[23] Susan S. Climate change 2007 – the physical science basis: Working group I contribution to the fourth assessment report of the IPCC, Vol. 4. Cambridge, United States: Cambridge University Press; 2007.
[24] Birkmann J. Measuring vulnerability to promote disaster-resilient societies: conceptual frameworks and definitions. In: Measuring vulnerability to natural hazards: towards disaster resilient societies; 2006. p. 9–54.
[25] Wolf S, Lincke D, Hinkel J, Ionescu C, Bisaro S. A formal framework of vulnerability. Final deliverable to the ADAM project. Potsdam, Germany: Potsdam Institute for Climate Impact Research; 2008.
[26] Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliab Eng Syst Saf 2011;96(1):64–74.
[27] Holling CS. Resilience and stability of ecological systems. Ann Rev Ecol Syst 1973;4:1–23.
[28] Gunderson LH, Holling C, Light SS. Barriers and bridges to the renewal of ecosystems and institutions. Columbia, United States: Columbia University Press; 1995.
[29] Walker1a B, Carpenter S, Anderies1b J, Abel1b N, Cumming G, Janssen M, Lebel L, Norberg J, Peterson GD, Pritchard R. Resilience management in social-ecological systems: a working hypothesis for a participatory approach. Conserv Ecol 2002;6(1):14.
[30] Kendra JM, Wachtendorf T. Elements of resilience after the world trade center disaster: reconstituting New York City's Emergency Operations Centre. Disasters 2003;27(1):37–53.
[31] Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces 2006;36(6):530–44.
[32] Perrings C. Resilience and sustainable development. Environ Dev Econ 2006;11(4):417–27.
[33] Adger WN. Social and ecological resilience: are they related? Prog Hum Geogr 2000;24(3):347–64.
[34] Hollnagel E, Woods DD, Leveson N. Resilience engineering: Concepts and precepts. Burlington: Ashgate Publishing, Ltd.; 2007.
[35] Sugden AM. Resistance and resilience. Science 2001;293(5536):1731.
[36] Jackson S. Architecting resilient systems. Accident avoidance and survival and recovery from disruptions. Hoboken, NJ, London: John Wiley; 2010.
[37] Monroe B, Oliviere D. Resilience in palliative care: achievement in adversity. Oxford: Oxford University Press; 2007.
[38] Handmer JW, Dovers SR. A typology of resilience: rethinking institutions for sustainable development. Org Environ 1996;**9**(4):482–511.
[39] Sundström GA, Hollnagel E. On The Art of Creating and Managing Policies: Facilitating the Emergence of Resilience. In: Proceedings 2nd Symposium on Resilience Engineering; 2006.
[40] Pavard B, Dugdale J, Saoud NB-B, Darcy S, Salembier P. Design of robust socio-technical systems. Juan les Pins, France. Resil Eng 2006.
[41] Walker B, Gunderson L, Kinzig A, Folke C, Carpenter S, Schultz L. A handful of heuristics and some propositions for understanding resilience in social-ecological systems. Ecol Soc 2006;11(1):13.
[42] Sheard S, Mostashari A. A framework for system resilience discussions. In: 18th Annual International Symposium of INCOSE. Utrecht, Netherlands; 2008.
[43] Nathanael D, Marmaras N. The interplay between work practices and prescription: a key issue for organizational resilience. In: Proceedings of the 2nd Resilience Engineering Symposium; 2006.
[44] Paton DF. Community resilience: integrating hazard management and community engagement. Launceston: School of Psychology; 2005.
[45] Romero N, Nozick LK, Dobson, I, Xu, N, Jones DA. Transmission and Generation Expansion to Mitigate Seismic Risk; 2013.
[46] Ericsson GN. On requirements specifications for a power system communications system. Power Deliv IEEE Trans 2005;20(2):1357–62.

[47] Remedial Action Scheme Definition Development. North American Electric Reliability Corporation: Washington, DC; 2014.
[48] Howell L. 8th ed. Global Risks 2013. Geneva: World Economic Forum; 2013.
[49] Carlson JM, Doyle J. Complexity and robustness. Proc Natl Acad Sci 2002;99 (Suppl. 1):2538–45.
[50] Brown RE. Electric power distribution reliability. Boca Raton, FL: CRC Press; 2002.
[51] Osborn J, Kawann C. Reliability of the US electric system – Recent trends and current issues; 2002.
[52] Sastry S. Nonlinear systems: analysis, stability, and control, 10. New York: Springer; 1999.
[53] Mili L, Cheniae MG, Rousseeuw PJ. Robust state estimation of electric power systems. Circuits Syst I: Fundam Theory Appl IEEE Trans 1994;41(5):349–58.
[54] Kundur P, Paserba J, Ajjarapu V, Andersson G, Bose A, Canizares C, Hatziargyriou N, Hill D, Stankovic A, Taylor C, Van Cutsem T, Vittal V. Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. Power Syst IEEE Trans 2004;19(3):1387–401.
[55] Ehlen MA, Vugrin ED, Warren DE. A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Albuquerque, NM, United States: Sandia National Laboratories; 2010.
[56] Amin M. North America's electricity infrastructure: are we ready for more perfect storms? Secur Priv IEEE 2003;1(5):19–25.
[57] Shinozuka M, Feng MQ, Lee J, Naganuma T. Statistical analysis of fragility curves. J Eng Mech 2000;126(12):1224–31.
[58] Han SR, Guikema SD, Quiring SM. Improving the predictive accuracy of hurricane power outage forecasts using generalized additive models. Risk Anal 2009;29(10):1443–53.
[59] Vickery PJ, Lin J, Skerlj PF, Twisdale Jr LA, Huang K. HAZUS-MH hurricane model methodology. I: hurricane hazard, terrain, and wind load modeling. Nat Hazards Rev 2006;7(2):82–93.
[60] Francis RA, Falconi SM, Nateghi R, Guikema SD. Probabilistic life cycle analysis model for evaluating electric power infrastructure risk mitigation investments. Clim Chang 2011;106(1):31–55.
[61] Bigger JE, Willingham MG, Krimgold F, Mili L. Consequences of critical infrastructure interdependencies: lessons from the 2004 hurricane season in Florida. Int J Crit Infrastruct 2009;5(3):199–219.
[62] Before And After The Storm. Edison Electric Institute; 2014.
[63] Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S, Adhikari U. Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information; 2013.
[64] Zeller, M. Myth or reality—Does the Aurora vulnerability pose a risk to my generator? In: Protective Relay Engineers, 2011 64th Annual Conference for IEEE; 2011.
[65] Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) security. NIST Spec Publ 2008;800(82):16.
[66] Common Cybersecurity Vulnerabilities in Industrial Control Systems. Department of Homeland Security, Control Systems Security Program; 2011.
[67] Ten C-W, Hong J, Liu C-C. Anomaly detection for cybersecurity of the substations. Smart Grid IEEE Trans 2011;2(4):865–73.
[68] Hahn A, Govindarasu M. Cyber attack exposure evaluation framework for the smart grid. Smart Grid IEEE Trans 2011;2(4):835–43.
[69] Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. Proc IEEE 2012;100(1):210–24.
[70] Qi H, Wang X, Tolbert LM, Li F, Peng FZ, Ning P, Amin M. A resilient real-time system design for a secure and reconfigurable power grid. Smart Grid IEEE Trans 2011;2(4):770–81.
[71] Cleveland FM. Cyber security issues for advanced metering infrasttructure (ami). In: Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, IEEE; 2008.
[72] Neuman C, Tan K. Mediating cyber and physical threat propagation in secure smart grid architectures. In: Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on; 2011.
[73] Vale Z, Morais H, Faria P, Khodr H, Ferreira J, Kadar P. Distributed energy resources management with cyber-physical SCADA in the context of future smart grids. In: MELECON 2010 – 2010 15th IEEE Mediterranean Electrotechnical Conference; 2010.
[74] Cardenas AA, Amin S, Sastry S. Secure control: Towards survivable cyber-physical systems. In: Distributed Computing Systems Workshops, ICDCS'08. 28th IEEE International Conference on; 2008.
[75] Erol-Kantarci M, Mouftah HT. Management of PHEV batteries in the smart grid: Towards a cyber-physical power infrastructure. In: 7th IEEE International Wireless Communications and Mobile Computing Conference (IWCMC); 2011.
[76] Kleissl J, Agarwal Y. Cyber-physical energy systems: focus on smart buildings. In: Proceedings of the 47th Design Automation Conference ACM; 2010.
[77] von Meier A, Arghandeh R. Chapter 34-every moment counts: synchrophasors for distribution networks with variable resources. In: Jones LE, editor. Renewable energy integration. Boston: Academic Press; 2014. p. 429–38.
[78] von Meier A, Culler D, McEachern A, Arghandeh R. Micro-synchrophasors for distribution systems. In: IEEE 5th Innovative Smart Grid Technologies Conference. Wsahington D.C.; 2014.
[79] Lopes JP, Moreira C, Madureira A. Defining control strategies for microgrids islanded operation. Power Syst IEEE Trans 2006;**21**(2):916–24.
[80] Jouneghani RA, Pipattanasomporn M, Rahman S, Flywheel energy storage systems for ride-through applications in a facility microgrid.
[81] Arghandeh R, Broadwater R. Distributed Energy Storage Control for Optimal Adoption of Solar Energy in Residential Networks (ASME Power2012). American Society of Mechanical Engineers Power Conference. American Society of Mechanical Engineers: Anaheim, CA, USA; 2012.
[82] Divan D, Johal H. Distributed facts—a new concept for realizing grid power flow control. Power Electron IEEE Trans 2007;22(6):2253–60.
[83] Wang X, Hopkinson K, Thorp J, Giovanini R, Birman K, Coury D. Developing an agent-based backup protection system for transmission networks. In: First International Conference on Power Systems and Communication Systems Infrastructures for the Future; 2002.