IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 18, 2018, accepted June 5, 2018, date of publication June 8, 2018, date of current version June 29, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2845378

Toward a Consensus on the Definition and Taxonomy of Power System Resilience

AMIN GHOLAMI[1], (Student Member, IEEE), TOHID SHEKARI[1], (Student Member, IEEE), MOHAMMAD HASSAN AMIRIOUN[2], FARROKH AMINIFAR[2], (Senior Member, IEEE), M. HADI AMINI[3], (Graduate Student Member, IEEE), AND ARMAN SARGOLZAEI[4], (Member, IEEE)

[1]Georgia Institute of Technology, Atlanta, GA 30332, USA
[2]School of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran 11365-4563, Iran
[3]Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213, USA
[4]Department of Electrical and Computer Engineering, Florida Polytechnic University, Lakeland, FL 33805, USA

Corresponding author: Arman Sargolzaei (a.sargolzaei@gmail.com)

ABSTRACT This paper analyzes the notion of resilience in power systems from a fundamental viewpoint and thoroughly examines its practical implications. This paper aims to describe and classify different high-impact rare (HR) events, provide a more technical definition of power system resilience, and discuss linkages between resilience and other well-established concepts, such as security and reliability. Most relevant decisions of system operators in the face of HR events involve a significant level of stress and strain. In order to make informed decisions within this context, it is crucial to have an all-inclusive picture of the state of the system. This paper provides an appropriate framework that not only characterizes the various states of the system but also derives informed decisions from a resilience-oriented perspective. It also describes and analyzes diverse resilience improvement strategies. Comprehensive models and classifications are provided to clearly capture various aspects of power system resilience.

INDEX TERMS High-impact rare (HR) events, power system restoration, proactive management, resilience assessment, resilience improvement.

I. INTRODUCTION

Ever-increasing dependence on electricity has led to numerous difficulties with the occurrence of any short- or long-term interruption or outage. A plethora of hazards stemming from natural, technical, or human factors could jeopardize the continuous, secure, and reliable supply of electricity. Historically, power systems have been designed, built, and operated in a way that could not be influenced by credible contingencies. They may be, however, affected by high-impact, rare (HR) events.

In retrospect, power experts have adopted several ways to face severe disturbances in power systems. In this line, system protection schemes (SPSs) or remedial action schemes (RASs) are generally accepted as effective mechanisms that detect abnormal or predetermined system conditions and mitigate potential threats in power systems. SPSs and RASs may be comprised of automatic control measures, such as changes in demand, generation (MW and MVAr), or grid configuration to preserve network stability, bus voltages, or transmission line flows. Nevertheless, the occurrence of large and combinational incidents (e.g., simultaneous generator and line tripping) motivated the need for special defensive measures commonly referred to as *defense plans*. A defense plan is defined as a set of coordinated SPSs and RASs which together can minimize the risk of forthcoming contingencies cascading to widespread blackouts. Particularly, a defense plan could be considered another layer of a protection system and is the last resort for maintaining the system stability [1].

The aforementioned plans and mechanisms are specifically tailored for transmission networks. Nowadays, distribution systems require more attention since they have embraced revolutionary changes including the proliferation of distributed energy resources (DERs), bi-directional flow of power, and mesh/loop topologies, which render them more complex and dynamic. Moreover, power distribution systems are historically behind power transmission systems in terms of observability and monitoring system deployment. The available

statistics pertaining to recent widespread interruptions are a testimony to the claim representing the growing importance of distribution networks. Accordingly, it has been estimated that 90% of customer outages in the United States are related to distribution networks [2].

In the aftermath of unprecedented disasters and attacks in recent years, resilience has become a buzzword in power system discipline. Resilience study is mainly concerned about the mitigation of catastrophic HR events, whose likelihood cannot be estimated via historical data. The variety and number of definitions for power system resilience has significantly increased over past several years, making it difficult to find a universal understanding of the term ''resilience'' in power systems. Moreover, a fundamental question has remained unanswered in power system community: how resilient is a given power system? Additionally, if our system is not resilient enough, what are the optimal resilience enhancement strategies? The ultimate goal of our paper is to address these questions. Specifically, the main contributions of our paper are as follows:

- Conceptualize the different types of HR events in power systems;
- Present a historical overview of resilience concept;
- Provide a unified approach to define resilience in power systems;
- Identify the linkages between the terms *resilience*, *security*, *reliability*, and *stability* in power systems; and clarify the relationships between the terms *resilience*, *vulnerability*, and *robustness;*
- Illustrate different temporal phases of system behavior following an HR event; and propose an eight-point linear approximation of system performance;
- Develop a seven-stage resilience assessment framework for determining the level of resilience in a power system. The aim of the proposed framework is to identify the trouble spots (i.e., vulnerabilities) in the face of HR events.
- Identify and classify effective strategies for resilience improvement.
- Describe operator actions during the phases of performance of a power system in case of an HR event; and construct a mapping between resilience improvement measures and their effectiveness on the level of performance of the system (this mapping is constructed from Fig. 9 to Fig. 10 in Section IX).

The rest of our paper is organized as follows. Sections II and III introduce the preliminary definitions required to define the concept of power system resilience. The classification of HR events, as the origins of resilience-related incidents, is expressed in Section IV. The historical overview of resilience concept and the unified definition of the power system resilience is presented in Section V. Section VI expresses how we can measure the resilience of a power grid in the system level. Section VII explains how resilience impacts the operating states of a power system. Section VIII and IX represent various stages of the resilience assessment method, and what measures we can take to improve the resilience of a power grid, respectively. Finally, the conclusions and possible future directions are given in Section X.

II. KNOWN, UNKNOWN, AND UNKNOWABLE EVENTS

In the wake of global climate change, the frequency and intensity of extreme weather events have increased on an unprecedented scale. Harvey, Irma, and Maria are not unknown names to our nation, and the Globe, because of how devastating these hurricanes has impacted many lives. This trend, which is projected to continue, has adversely affected the performance of power systems. Severe weather events are among the leading causes of widespread power outages in the United States [2]. For instance, in 2012, Hurricane Sandy left about 8.5 million households and businesses, including tens of millions of people, without power and in some cases, restoring power took a couple of weeks. During 2003 to 2012, approximately 679 power outages, each affecting at least 50,000 customers, occurred due to weather events in the United States, and 80%−90% of these outages stemmed from failures in distribution systems [3].

Aside from extreme weather events, the current power systems infrastructure is highly vulnerable to cyber and physical attacks which could cause small and large-scale power outages. A major cyber-attack on the U.S. electrical grid can cause an economic loss - of more than $1 trillion. In a large blackout, facilities with backup generators may be able to function, but all other facilities, including but not limited to phone systems, internet, television, radio, and street lights, will likely be shut down. A blackout can also raise mortality rates as health and safety systems fail, and a decline in trade as ports shut down [4]. This issue stems, in part, from the proliferation of information and communications technology (ICT) usage in electricity grids. On the one hand, the advent of ICT has promoted the development of smart grids, while on the other hand, it has set the stage for acts of sabotage. The recent hack of a Ukrainian power grid on Dec 23, 2015 shows how easy it can be to plunge a community into darkness. The attack impacted 225,000 customers in three different distribution level service territories and lasted for several hours [5].

The growing concern over extreme weather events, along with the cyber and physical security threats, has underscored the need for a resilient power grid. Providing a precise definition for the notion of resilience in power systems is a decisive and pivotal step toward the design, standardization, and operation of resilient grids. In this regard, the discernment of potential threats to power system resilience could considerably pave the way for reaching a precise definition. Indeed, a key question ought to be addressed: What are the salient characteristics of extreme weather events or cyber-attacks? The short answer is that they are black or gray swans.

A black swan is a metaphor for an unpredictable, high-impact, and rare (UHR) event. This type of event is also referred to as the ''*unknowable,*'' i.e., a rare cataclysmic event

with unforeseen or unobserved consequences upon random occurrence. The proliferation of the smartphones and the impact of Google search technology are examples of positive black swans. In contrast, the devastating consequences of the September 11 attacks (9/11) and the 2004 Indian Ocean tsunami are negative black swans. Obliterating impacts of a severe earthquake is another instance of black swans. To summarize, the key elements of black swans are rarity, extreme impact, and retrospective predictability (people make concoct explanations after the event) [6], [7].

On the other hand, a gray swan is a metaphor for a partially-predictable, high-impact, and rare (PHR) event, which is disregarded by many people [7]. This category of events has rarely observed impacts and can be interpreted as "*unknown*" (PHRs can be modeled to some extent, yet a considerable part of them is unknown). Weather events (such as tornado and flooding) are examples of gray swans. It is worth mentioning that black and gray swans might be seen sooner by looking for the warning signs of a process excursion.

When we consider a rare phenomenon to be *unknowable* or *unknown*, we are referring to the presence or absence of a conceptual model to describe that particular phenomenon (i.e., the incapability of our theories to provide meaning to the rare event we observe and measure) [8]. From a mathematical point of view, if we define a probability distribution function (PDF) as a mathematical description of a random phenomenon in terms of the probabilities of outcomes, then three situations may arise [8]:

- When a PDF is completely specified (i.e., both outcomes and probabilities are known), the situation is referred to as *known*. For example, the PDF for the unavailability of generating units (namely the forced outage rate (FOR)) is known. In these situations, the law of large numbers (LLN) and the central limit theorem (CLT) hold true.
- When probabilities cannot be assigned to at least part of the space (i.e., outcomes are specified but probabilities are not), the situation is *unknown*. Note that gray swans fall into this category. We do not know the odds of a gray swan, but we can imagine how a power grid might be affected by one.
- When even the outcomes cannot be identified in advance, the situation is *unknowable*. Note that unknowable events enter the domain of unknown once they occur. Retrospectively, black swans belong to this category.

It is worth noting that there is not always a bright line that separates black swans from gray swans. Although we may easily put some events at one, or the other, end of the spectrum, personal perspectives cause individuals to disagree on whether a high-impact event is a black or gray swan [6]. Additionally, developments in science and technology may transform some events from black to gray swans.

Since the historical data of known situations are available (e.g., the fault rate in transmission lines), they can be characterized by probabilistic methods. On the other hand, there are no (or few) statistical data available about unknown situations. In this case, we can describe the event with possibilistic approaches using a fuzzy membership function. The possibility theory is a mathematical theory for dealing with certain types of uncertainty and is an alternative to the probability theory. This theory is widely used when there are no historical data available for a phenomenon, i.e., HR events in this paper [9] (see also [10], [11] for more details on fuzzy sets and fuzzy decision making).

III. RISK AND UNCERTAINTY: A DIFFERENT INTERPRETATION

The need to address black and gray swans has attracted new attention to an old idea about risk from decades ago, known as "Knightian uncertainty" [12]. Frank Knight clearly distinguished risk from uncertainty, especially when we have imperfect knowledge about an event. According to Knight's idea, risk refers to *known* situations, where both the outcomes and the odds are specified. Uncertainty, on the other hand, relates to *unknown* situations, where we are unable to set accurate odds for the outcomes. It goes without saying that gray swans (as "unknown" situations) are equivalent to Knight's definition of uncertainty (see Fig. 1). It seems that in real-world examples, the majority of events are highly complicated and that forecasting always pertains to "uncertainty," not "risk." In this context, risk should be applied to a highly-controlled environment, such as a pure game of chance in a casino, whereas uncertainty could be applied to almost everything else. (see [13], [14] for uncertainty in knowledge and ignorance hierarchy.)

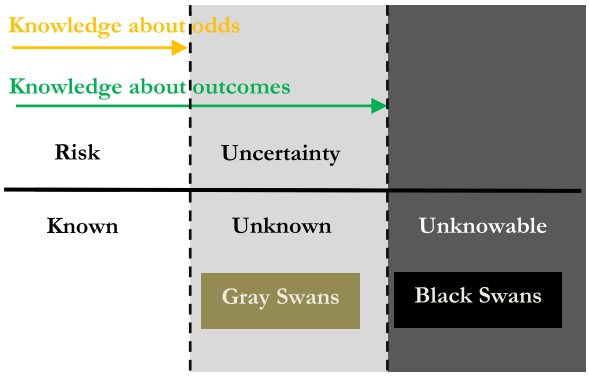

FIGURE 1. Tripartite distinction between known, unknown, and unknowable.

Knight's theory about risk and uncertainty could facilitate analyzing the impact of gray swans on power systems. Recent major blackouts around the world may partially stem from imperfect risk assessments conducted by independent system operators (ISO). Perhaps ISOs regarded their risk assessments as precise while operating in conditions of Knightian uncertainty.

Typically, it is infeasible to estimate the likelihood of rare events (the rarer the event, the fuzzier the odds) [7]. Studying the grid's recorded history cannot produce accurate estimates

of future probabilities since the history might not contain a single rare event (e.g., a 100-year flood is not likely to show up in 10 years of historical data) [6]. Therefore, we cannot rely on accurate probability estimates to cope with these incidents. Knight's perspective on risk and uncertainty eliminates the need to understand the probabilities of a rare event; rather, we can focus on the effects of an event if it occurs. We do not know the odds of an earthquake, but we can imagine how a microgrid might be affected by one. In this sense, Knightian uncertainty is not merely a quasi-philosophical outlook; the objective perception of Knightian uncertainty is a pressing practical problem.

More generally, *resilience engineering* provides the fundamental prerequisites for studying black and gray swans (see [15] for a detailed comparison between resilience engineering and risk assessment). Note also that although it is difficult to determine accurate estimates of rare event probabilities, information from domain experts, Bayesian statistical methods, and Monte Carlo simulations can help determine interval estimates for their possibilities [6], [16], [17].

IV. CLASSIFICATION OF HR EVENTS

HR events can be divided into four major categories based on their origins and impacts on power systems: technical cascading failures, extreme natural events, cyber and physical attacks, and space weather [18].

A. TECHNICAL CASCADING FAILURES

The north American Electric Reliability Corporation (NERC) defines cascading failure as "*the uncontrolled successive loss of system elements triggered by an incident at any location*" [19]. In practice, power systems are designed and operated so that they can withstand credible (e.g., N-1) contingencies. However, other possible failures, such as hidden failures in relays or errors in situational awareness, may trigger a sequence of outages and finally lead to a cascading failure. The U.S.-Canadian blackout on August 14, 2003 is one of the recent cascading failures that caused enormous social and economic damages. This incident affected approximately 50 million people in eight U.S. states and two provinces of Canada. During this event, over 400 transmission lines, 531 generation units, and 261 power plants tripped out. The main causes of the blackout were declared as: limited understanding of the system, inadequate level of situational awareness, deficient vegetation management (tree trimming), and failure in state estimator (SE) and real-time contingency analysis software (RCAS) [20].

A cascading failure can be analyzed and studied in two main phases (e.g., different time-scales): slow cascade and fast cascade [21]. In the slow cascade phase, the failure spreads over a lengthy period of time (from several minutes up to several hours). The system operators usually cannot prevent the cascading in this phase. The reason is that they are hardly aware of the damaging consequences of the failures occurred during this phase. During the fast cascade phase, the power system becomes unstable. The main problems emerging in this phase include transmission line overloads, voltage collapse, frequency oscillation, dynamic instability, and inappropriate under frequency load shedding [22]. It is almost impossible for operators to manually stop the cascading during this phase since the short time period between each sequential event ranges from only milliseconds to tens of seconds.

In particular, changes in the power demand can lead to a cascading failure. In general, these changes can be categorized into two groups: i) small and gradual changes and ii) large and sudden changes. To handle the first group, power systems are equipped with several load-frequency control loops (including governors and AVRs) which compensate for the gradual changes in the demand. Regarding the second group, sudden and large changes in the demand would trigger under frequency load shedding (UFLS) relays where adequate loads will be curtailed to match the generation. Either of these cases can lead to cascading failures (the first group can lead to a slow cascade while the second one can lead to a fast cascade).

B. EXTREME NATURAL EVENTS

Extreme natural events such as floods, windstorms, hurricanes, tornados, tsunamis, and earthquakes have increasingly affected power systems in recent years. Among the most severe ones, the 2005 Hurricane Katrina blackouts, the 2012 Hurricane Sandy blackouts, and the 2011 Japan Earthquake blackouts can be stated [23]. It is expected that weather-related events will occur more often and with greater severity, mainly due to global warming and climate change. The adverse impacts of extreme natural events include flooding of power plants and substations (in the case of floods and tsunamis), the collapse of overhead transmission towers and distribution poles, the falling of trees on distribution lines (in the case of hurricanes, windstorms, and tornados), extensive damage to power plants, substations, and control buildings (in the case of earthquakes), etc. [23]. Extreme natural events might be seen sooner from seconds to several hours prior to the event depending on the event type and forecast models used for event prediction [23], [24].

C. CYBER AND PHYSICAL ATTACKS

Modern electricity grids, as interdependent cyber-physical systems, are prone to excessive risks from both cyber and physical aspects. Cyber-attacks are divided into seven groups based on the end goal of attackers: i) bad measurement injection (Man-in-the-middle (MITM) attack) [25], ii) bad command injection (manipulating command signals), iii) control center impersonation attack, iv) communication delay attack [26], [27], v) unresponsive command attack, vi) disabled RTU (denial of services (DoS) attack), and vii) coordinated cyber-attack [28]–[30]. For instance, in the coordinated cyber-attack on the Ukraine power grid, attackers gained access to the distribution management system (DMS) at two distribution centers. Subsequently, they opened breakers in 30 substations. Attackers also carried out

a DoS attack to prevent customers from reporting the outage [5].

On the other hand, power systems have been perpetually threatened with intentional physically malicious acts, and nothing precludes future attempts [31]. A notable example of such attacks is on power substations in 1996, which was aimed at cutting off London's power supply. In addition, an attack on a substation in California on April 16, 2013 resulted in damaging 17 giant transformers and 27 days repair time [32].

D. SPACE WEATHER EVENTS

Recently, threats imposed by space weather (or solar storms) have attracted attention in scientific communities. Quasi-DC electric currents (geomagnetically induced currents or GICs) may be injected into power grids as a result of severe geomagnetic storms. Geomagnetic storms are created when large eruptions of material from the Sun, known as coronal mass ejections (CMEs), pass over the Earth. Quasi-DC currents can disrupt the normal operation of critical grid components such as transformers and shunt reactors. Large-scale outages may occur if a few transformers are damaged by these currents [18]. In March 1989, a strong solar storm caused a half-cycle transformer saturation which generated harmonics that improperly tripped out five power lines, knocking out nearly 10 GW of generating capacity and collapsing the entire network in a minute [33]. The warning time of geomagnetic storms might vary from 30 minutes to several hours prior to the occurrence, based on the observations and measurements from magnetometers and data received from satellites. Real-time monitoring of Quasi-DC currents can be achieved using ground magnetic field recordings. In this context, a short-term forecast is based on the rate of change of a geomagnetic field (dB/dt), which is the main cause of Quasi-DC currents [33].

V. POWER SYSTEM RESILIENCE: BACKGROUND AND DEFINITION

Overlooking HR events is tempting because the likelihood of each event is both small and unknown [6]. Power systems, nonetheless, are vulnerable to a plethora of HR events, and occurrence of gray swans in the future is certain. Furthermore, even if a power system mitigates all of the gray swans, an unknowable black swan can still lead to immense damaging consequences.

Resilience is a concept that reflects how an infrastructural system can moderate the consequences of black and gray swans. A clear definition for this concept in power grids could pave the way for building more resilient systems. The word ''resilience'' is derived from the Latin word ''resilire,'' which means ''the ability to spring back or rebound'' [34]. In 2009, ASIS International defined resilience as ''the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event'' [35]. In 2010, the National Infrastructure Advisory Council (NIAC) offered a broader definition for infrastructure resilience: ''the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event'' [36]. Many other definitions have been developed for resilience in economic systems [37], social systems [38], organizational systems [39], complex systems [40], [41], etc. (see [42] for more definitions in various fields); however, the majority of definitions are comprised of the following common themes: avoidance, survival, and recovery.

The NIAC resilience definition is acknowledged by the NERC to be used in power systems [43]. However, it should be specifically tailored in the context of power systems. Moreover, some of the terms and concepts defined by NIAC already exist in power system terminology. The differences, therefore, should be clarified to avoid any possible misunderstanding. These issues will be elaborately discussed in the following sections.

VI. MEASURING THE RESILIENCE IN THE SYSTEM LEVEL

A. PRELIMINARIES

Generally, the resilience of power grids can be studied at two levels: component level and system level [44]. Component level studies primarily focus on either individual physical or cyber components in a power network. Recent developments in the design and implementation of such components have considerably improved their performance, thereby possessing an acceptable level of resilience [44]. However, the power grid is made up of many parts, whose interactions are complex and hard to compute. In order to capture both physical and cyber interdependencies of these components, power experts have made extensive efforts to study the resilience in the system level [34]. Indeed, researchers have found it more vital to study the power grid's macroscopic resilience rather than to dissect an individual component's resilience.

Technically speaking, defining appropriate system level resilience metrics enables authorities to perform analytical assessments, take different preventive measures, and in general, produce potential cost-effective solutions for encountering HR events [36], [43]. In order to measure the resilience in a holistic way, three key aspects must be taken into account [45]: measuring the ''*resilience of what, to what and, under what conditions*.''

As the main damaging consequences of HR events emerge in the distribution systems level, the answer to the first question is usually distribution networks rather than transmission systems [46]. Note that without loss of generality, a resilience metric can also be proposed in the transmission level. Regarding the second question, the resilience metric can be defined for either a black swan or gray swan. The key point is that having a conceptual model of the event enables the system operator to take effective measures to reduce the damaging

impacts of a catastrophe on the grid. Axiomatically, grey swans fall into these types of events. In this category of events, we can implement a set of resilience improvement measures before the contingency takes place. On the other hand, for black swans, the level of system resilience can be determined merely after the occurrence of the event.

The third aspect that should be considered in defining a resilience metric is the operating point of the power grid in question at instant of occurrence of the event. For the sake of providing further explanation, the resilience of a power system in the peak load condition may be different from the resilience of the same system in the light load condition [34]. Fig. 2 illustrates a conceptual model for measuring the resilience level of a power network.

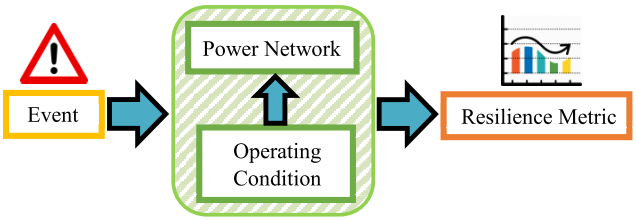

FIGURE 2. A conceptual model for measuring the resilience level of a power system.

B. DIFFERENT PHASES OF RESILIENCE

Analyzing power system performance in response to HR events helps us describe the temporal phases of the power system resilience. A typical power system performance as a function of time following a disturbance is illustrated in Fig. 3. In this figure, the vertical axis shows the performance of the system, which can be defined by various metrics, such as the availability of critical facilities, the number of people served, the amount of flow or services delivered, and the level of economic activity [47]. Each of the aforementioned performance metrics represents a different dimension of the resilience. In the horizontal axis, the resilience evaluation begins att_0, an HR event occurs at t_e, the specified performance index is degraded at t_d and reaches some minimum point at t_m. Subsequently, the recovery process begins at t_m, and the performance index is elevated until a local saturation point at t_{ir}. The recovery of the infrastructure further improves the performance, and the system returns to an acceptable operating state at t_r. As can be seen, the temporal process of the system response to a severe incident can be divided into three phases: avoidance, survival, and recovery.

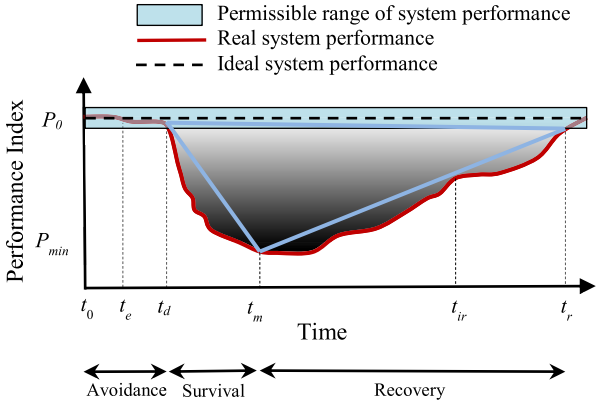

FIGURE 3. Performance of power system following an HR incident.

1) AVOIDANCE PHASE

This phase runs from t_0 to t_d. Specifically, t_0 is the instant when we become certain about the occurrence of the event (albeit with an accepted confidence level) and get prepared for taking proactive measures. Subsequently, the event occurs at t_e; however, depending on the type and severity of the event, the system performance does not necessarily degrade immediately. Indeed, the system performance is temporarily (i.e., $[t_e, t_d]$) preserved within the permissible range. The avoidance phase can be divided into two sub-intervals. The first sub-interval, which is called *preparedness and proactive management*, runs from t_0 to t_e. The length of this sub-interval might be zero for some HR events, like an earthquake, but minutes to hours for some others, like tornados. The second sub-interval, i.e., from t_e to t_d, is called *robustness*. The robustness of an electricity grid depends upon the structure of the system, its control and protection schemes, and the nature of the HR event. To clarify, the robustness of a power network with overhead lines is more threatened by tornados rather than floods. On the other hand, floods can affect the robustness of a power network with underground cables much more than tornados.

The time interval $[t_0, t_d]$ allows the system operators to anticipate possible damage and take positive steps toward reducing the impacts of HR events on the system following the occurrence of the event (i.e., t_e). For example, changing the operating point of the system (i.e., resilience-constrained optimal power flow) is a primary measure that can be implemented during the avoidance phase.

2) SURVIVAL PHASE

This phase, which runs from t_d to t_m, shows a significant performance reduction over a short period of time. The control and protection schemes and infrastructures are mainly in charge of this phase to maintain the system performance as high as possible. Hence, improving current protection and control mechanisms can effectively enhance the resilience of the system in the survival phase. For instance, recent developments in enhancing load shedding schemes have resulted in a lower amount of load curtailments encountering severe and unexpected disturbances [48], [49]. Such schemes can effectively maintain the system stability while dropping the minimum amount of loads.

3) RECOVERY PHASE

This phase is indicated in Fig. 3 between time t_m and t_r. In this phase, the system operator aims to restore the grid's

performance to the permissible range and recover the damaged infrastructures to a normal condition. Accordingly, the recovery phase consists of two main sub-intervals: system restoration (i.e., $[t_m, t_{ri}]$) and infrastructural recovery (i.e., $[t_{ri}, t_r]$). In the system restoration sub-interval, the network loads are re-energized as expeditiously as possible. In the infrastructure recovery phase, the damaged infrastructure is repaired and the network returns to a normal condition. Deploying fast system restoration schemes can substantially improve this aspect of system resilience [50], [51].

A detailed explanation about resilience improvement strategies will be provided in Section IX.

C. GENERAL FORM OF THE RESILIENCE METRIC

A suitable metric for evaluating the resilience of a power network should represent the performance of the system following an HR event. Meanwhile, temporal aspects should be reflected in the metric since the performance of an actual system changes considerably over time. Unlike routine outages, HR power outages may not be properly measured by reliability metrics which emphasize the probability and the frequency of power outages as well as the amount of load or energy not served. Although reliability indices can offer human operators with additional insight on the abnormal behavior of power systems, the static nature of these indices make them unsuitable for measuring the spatiotemporal impacts of HR events on power grid. New metrics are thus in essence for assessing the power system resilience. In addition, among applicable metrics for resilience assessment in the literature, a few of them suggested normalized metrics (varying between 0 and 1). Employing normalized metrics provides a comparable means for assessing the resilience in various operating conditions and power systems [52]. The ideal and real response of a power system to an incident is depicted in Fig. 3 with dash and solid trajectories, respectively. Based on the aforementioned properties, the general form of the resilience metric can be defined as [53]:

$$R = \frac{\int_{t_0}^{t_r} P(t)\,dt}{\int_{t_0}^{t_r} P_0 dt} = \frac{\int_{t_0}^{t_r} P(t)\,dt}{P_0\,(t_r - t_0)} \tag{1}$$

where R is the resilience metric and indicates how much our grid is resilient against a specific HR event. For the sake of comparison, the metric is per-unitized in such a way that it is bounded in the range [0, 1]. It goes without saying that limits of integration could be redefined to calculate the metric for a specific phase of performance (i.e., avoidance, survival, and recovery). Further, $P(.)$ denotes the performance index function, as defined in Fig. 3.

Another suitable metric which can be used for effectively measuring the resilience of a power grid is *resilience triangle* [13], [54]–[56], which is illustrated in Fig. 3 (blue triangle). As can be seen, this metric represents a metric of both the loss of performance of a system after an event and the amount of time it takes for the power grid to return to acceptable performance levels. Resilience improvement measures are generally designed to reduce the resilience triangle size by decreasing the performance degradation during an event (vertical axis) and/or reducing recovery time (horizontal axis). The metric can be generalized and represented in the mathematical form as follows:

$$R_{triangle} = \frac{\int_{t_0}^{t_r} [P_0 - P(t)]dt}{\int_{t_0}^{t_r} P_0 dt} = \frac{\int_{t_0}^{t_r} [P_0 - P(t)]dt}{P_0\,(t_r - t_0)} \tag{2}$$

Similar to the first metric, the resilience triangle metric is per-unitized in the range [0, 1]. However, in this metric as opposed to the first one, zero denotes a fully resilient system, whereas one represents a totally non-resilient system.

VII. OPERATING STATES OF A POWER SYSTEM: THE IMPACT OF RESILIENCE

A. TRADITIONAL VIEW

Two sets of constraints govern power system operation: equality (or load flow) constraints, denoted by **E**; and inequality (or limit) constraints, denoted by **I**. The equality constraints state that all of the customers must be served at all times, while the inequality constraints express that the system variables (e.g., voltage magnitudes) must always be kept within certain limits. Based on these two generic sets of equations, power system conditions are characterized into five operating states, as depicted in Fig. 4. In terms of notation in this figure, a bar or line over the letters **E** and **I** denotes the violation of the corresponding constraints. It is worth recalling the definition of each operating state [57]:

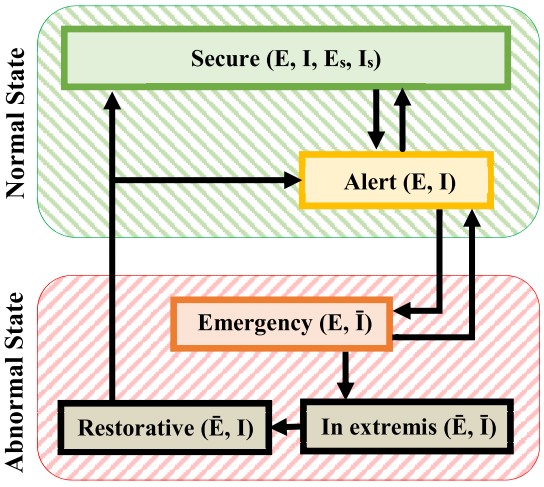

FIGURE 4. Power system operating states and transitions between them [57].

1) Secure: A power system is said to be in a secure state whenever all constraints are satisfied. Further, in this state, there are adequate margins (from both generation and transmission points of view) such that the power system will remain intact even after a single "*credible*" contingency occurs. Indeed, an adequate level of security is guaranteed in

this state. In the secure state shown in Fig. 4, $\mathbf{E_s}$ and $\mathbf{I_s}$ denote the fulfillment of equality and inequality constraints under all credible contingency scenarios.

2) Alert: If the security level drops under a given threshold (i.e., when there is a reduction in reserve margins), the power system enters the alert state. In this state, despite the fact that both the equality and inequality sets of constraints are satisfied, some disturbances could cause the violation of some inequality constraints (i.e., frequency, voltage, line currents, etc. will not stay in their permissible range). Consequently, system operators can analyze trouble spots and take appropriate preventive (pre-contingency) actions to increase the system security and bring the system back to the secure state.

3) Emergency: If a severe disturbance occurs before a preventive action can be taken, the system enters the emergency state. In this state, the set of load flow equations is satisfied, but some of the limit constraints are violated. Here, corrective actions should be taken in order to eliminate the violations and restore the system to at least the alert state.

4) In-extremis: The corrective actions are doomed to failure if they are not taken in time, and/or if the disturbance is severe enough to overstress the system (specifically in case of HR events). The system then falls into the in-extremis state where both equality and inequality constraints are violated. Power system operators would take heroic actions to save the system from a total collapse.

5) Restorative: Finally, once the collapse is halted or following a total collapse, the system is said to be in a restorative state. This state is characterized by feasible operation of the power system equipment but with portions of the load not being served and/or with loss of system integrity. Depending on the current circumstances, the system could then transit to either the alert state or to the secure state.

B. RESILIENCY-ORIENTED VIEW

The traditional operating states (which are designed for credible contingencies) are no longer adequate or relevant under HR events. However, once an HR event occurs, power systems would take a similar path, as depicted in Fig. 4. The resilience-driven operating states of the system following an HR incident are depicted in Fig. 5.

From a resilience-oriented viewpoint, power system conditions are described in terms of two additional sets of constraints: loose equality constraints, $\mathbf{E}^*$, and loose inequality constraints, $\mathbf{I}^*$. The former, i.e., $\mathbf{E}^*$, describes a condition where portions of the load are not being served with the aim of helping the system deal with an HR event. Such conditions could be achieved by emergency demand response programs or conservation voltage reduction (CVR). On the other hand, loose inequality constraints, $\mathbf{I}^*$, pertain to a condition where a wider range of operation is temporarily allowed. For instance, according to ANSI C84.1, distribution utilities may use loose voltage limitations (i.e., 107V-127V) in case of emergency, instead of the normal range (i.e., 114V-126V).

Accordingly, resilience-driven states of a power system are described below:

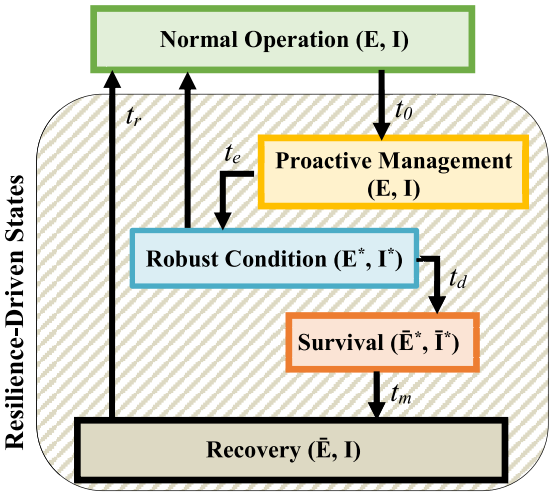

FIGURE 5. Resilience-driven operating states of power systems following an HR incident.

1) Normal Operation: In this state, there are no alerts or declared forecasts on the possibility of an HR event, and all equality and inequality constraints are satisfied. This state resembles the secure state in the traditional view.

2) Proactive management: As mentioned earlier, HR events might be seen sooner by looking for the warning signs of a process excursion. In other words, warning signs will increase the contingent possibility of such events (possibility is a function of time). For example, tornadoes and earthquakes may be foreseen several hours before they occur. The instant when the possibility of HR events increases is considered to be equal to t_0 in Figs. 3 and 5. At this instant, the system enters the avoidance phase. Note that the length of the period $[t_0,t_e]$ (i.e., when the system is in the proactive management state) may vary from a few seconds (e.g., for cyber-attacks) to several hours (e.g., for some weather incidents). All constraints ($\mathbf{E}$ and $\mathbf{I}$) are satisfied in this state; however, the system will enter the robust condition state if the predicted HR event occurs. Here, system operators can analyze the approaching event and take appropriate proactive actions to increase the level of preparedness.

3) Robust condition: In this state, the system is confronted with the event; however, its performance has not significantly degraded. Here, loose equality and inequality constraints (i.e., $\mathbf{E}^*$ and $\mathbf{I}^*$) govern the system. The performance of the system in this state is highly dependent on the level of reinforcement (hardening strategies) previously implemented in the planning phase. Further, appropriate corrective measures are effective if they are taken in a timely manner. If the system continues operating with no significant degradation (even with loose constraints), it can then return to the normal operation state. Otherwise, it enters the survival state at t_d.

4) Survival: In this state, the system is significantly degraded and both $\mathbf{E}^*$ and $\mathbf{I}^*$ constraints are violated. Similar to the in-extremis state, power system operators would take heroic actions to save the system from a total collapse.

5) Recovery: Once the system degradation stops, the system enters the recovery state. Similar to the restorative state (Fig. 4), the main goal of the system operator in this step is to return the system to its pre-event condition. This process is implemented step-by-step with portions of the load not being served and/or with loss of system integrity.

C. THE CONCEPT OF RESILIENCE: A DEEPER LOOK

For an electricity grid, reliability, security, stability, and resilience are pertinent concepts. Reliability reflects the probability of satisfactory system performance over a long period of time and under a given condition. Reliability can be inferred as the time average performance of the system. A certain level of reliability could usually be achieved through planning-oriented measures. In contrast to reliability, resilience is associated with the time-varying condition of the system over a short period of time and for the most part, a specified level of resilience could be attained via operation-oriented actions.

The concepts of security and resilience are similar to each other with only a few subtle differences. Security refers to the degree of risk in the system's ability to withstand credible contingencies without having any load shedding. Both concepts are related to the time-varying performance evaluation of the system in the operation condition. As the first and foremost difference, security is assessed for a system associated with a set of credible contingencies; however, resilience is measured in the network for an HR incident. Furthermore, in order to determine the resilience level of a grid to an HR event, a full cycle, including avoidance, survival, and recovery phases, should be passed (see Fig. 5). However, the network security level for a contingency can be calculated if the state of the system remains in or exits from the secure state (see Fig. 4). To clarify, if the state of the system after a contingency remains in the secure state, the security level of the network would be one; otherwise, it would be zero for that event. Stability is an important factor in security, which deals with the continuing operation of the system following a disturbance. It is axiomatic that when a system is secure, it may not be resilient. The reason is that the concept of security is defined for credible contingencies, but resilience is associated with HR incidents.

Finally, note that the terms vulnerability and resilience are subtly related. Vulnerability is the predisposition that deteriorates if an HR event occurs. In fact, vulnerabilities are specific features or conditions of the network which make it susceptible to threats.

VIII. RESILIENCE ASSESSMENT: HOW RESILIENT ARE THE POWER NETWORKS?

The main goal of this section is to develop a framework for determining the level of resilience in a power system. Note that addressing this question is a prerequisite for accurately identifying the trouble spots (i.e., vulnerabilities) and taking effective measures for elevating the resilience of the grid. HR events cause widespread damage to individual assets and components. Thus, a component-based approach is used to evaluate the performance of the system facing an HR event. Fig. 6 illustrates the proposed seven-stage resilience assessment framework. Specifically, the first three stages in this figure aim to define a resilience metric, characterize the HR event, and model the potential impacts of the event on the grid operation.

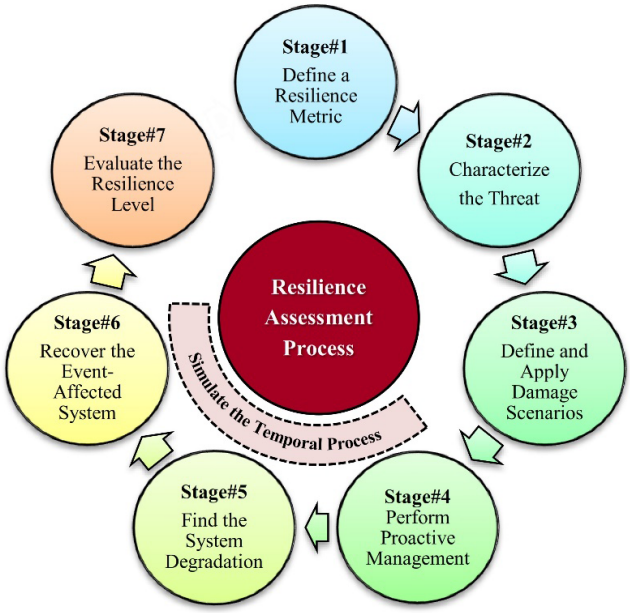

FIGURE 6. Resilience assessment process of a power system in response to an HR event.

During the next three stages (i.e., stages 4, 5, and 6), we attempt to simulate the behavior of the system in response to the designated HR event. Here, the two crucial points are: i) simulating the HR event and its spatiotemporal effects (from both physical and cyber perspectives) on the system, and ii) simulating the proactive, corrective, and restorative measures that can be taken (based on currently available resources and technologies) in response to the event. Accordingly, the performance curve is acquired. In practice, it is difficult, if not impossible, to acquire the real performance of the system in Fig. 3. To overcome this hurdle, we attempt to acquire a linear approximation of system performance, as shown in Fig. 7. This approximation facilitates the simulations since it requires only eight points, mainly denoting the beginning and the end of the avoidance, survival, and recovery phases. In the last stage, the pre-specified resilience metric is calculated, and accordingly, potential improvement measures are assessed. Further details on each of the aforementioned stages are provided in the following sections.

A. STAGE 1: DEFINE A RESILIENCE METRIC

The initial step toward resilience assessment is to define an appropriate resilience metric. As mentioned in Section VI, the metric defined in (1) would assess the resilience by evaluating the system performance in each sequential phase

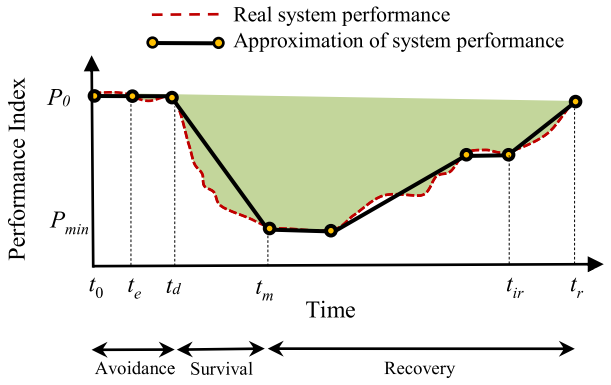

FIGURE 7. Eight-point linear approximation of system performance in response to an HR event.

of the system temporal behavior (i.e., avoidance, survival, and recovery) following the given HR event. Note that the devised resilience metric provides normalized values so that the resilience of a power grid under different HR events could be compared [58].

In order to calculate the resilience metric (1), an appropriate performance index ought to be defined. As previously mentioned, the performance index can be a technical index, such as the availability of critical facilities and the amount of load shedding. In some cases, the defined performance index goes beyond the system's technical characteristics and assesses the social welfare (e.g., the level of economic activity). Therefore, expert groups including stakeholders, industry managers and specialists, and policy makers of energy infrastructures should work on this aspect and decide to choose the ultimate performance index to be applied in their analysis [59].

B. STAGE 2: CHARACTERIZE THE THREAT

In this stage, the causes, effects, and physical (and/or cyber) aspects of the analyzed HR event are modeled. Note that Knight's idea obviates the need to have the probability of the event. Furthermore, black swans cannot be characterized in this stage (because they are *unknowable*), and we can evaluate the network resilience against them after their occurrence. Different gray swans, on the other hand, can be characterized as follows:

1) Extreme Natural and Space Weather Events: These types of events can be modeled using either a recorded (representing historical data from past events) or a predicted (projecting potential threats) event profile. In the former approach, the required historical data is provided by climate models (CMs), geophysical models (GMs), or real measurements from multiple weather or seismic stations [60].

In order to forecast an event profile, two main methods are introduced in the literature. If the data is provided by CMs or GMs, parametric modeling is used and the model parameters can be modified based on expert knowledge or real measurements. On the other hand, if the data is provided by real measurements, power law [61] and extreme value theory (EVT) [62] can be employed. In statistics, the power law states that a relative change in one quantity results in a proportional relative change in the other quantity, and this law can be used to describe gray swans. Moreover, EVT assesses the possibility of events that are more extreme than any other previously observed events (i.e., black and gray swans) [8]. In practice, natural events can be forecasted via analysis tools such as UKCP09 (developed by the Met Office, UK) [63] or Hazus (developed by Federal Emergency Management Agency, US) [64].

2) Technical Cascading Failures: A large number of methodologies have been proposed in the literature to model technical cascading failures. These methods can be classified into five groups [22]:

- *Topological Models*: Generally, cascading failures occur in all complex networks. Therefore, researchers made extensive efforts to adopt the complex network cascading failure analysis tools in power systems. The approaches in this group are relatively simple in implementation and analysis. Modified topological models and maximum flow models are among the approaches classified in this group [65], [66].
- *Scenario-Based Models*: Due to the significant level of uncertainties that initiate and exacerbate cascading failures and also the difficulty of simulating some factors such as human misoperation, scenario-based simulation tools are widely used in modeling and characterizing such events. PRACTICE models and Markov chain models are used as scenario-based models in the literature [67], [68].
- *High-Level Statistical Models*: Aside from the accuracy of common analysis tools, the computation burden should be considered an important factor in predicting the real-time propagation of a blackout. High-level statistical models ignore the detailed mechanisms of the cascading failure. Therefore, the simulation speed of these methods substantially increases. Such models provide an overall view of the event with tractable approaches such as CASCADE models and Branching process models [69], [70].
- *Dynamic Simulation Models*: These models consider the dynamic behavior of the power system with a high resolution of details during the cascading failure. Due to the high accuracy of the dynamic simulation models, they usually have a heavy computational burden. Existing dynamic simulation methods consist of OPA models, Manchester models, COSMIC models, multi-timescale quasi-dynamic models, ASSESS models, TRELSS models, and dynamic PRA models [71]–[76].
- *Other Models*: Other models including potential cascading models (PCM), hidden failure models, and historical data-based models, are also used in the literature to characterize technical cascading failures [77]–[79]. The main advantage of these methods is to effectively predict the potential cascading failures.

3) Cyber and Physical Attacks: Cyber and physical attacks can be analyzed with interdependent models, including complex network-based models and flocking-based hierarchical cyber-physical models.

- *Complex Network-Based Interdependent Models*: These models are widely used in the literature to characterize cyber-attacks. Interdependent networks cover a wide range of emerging networks in future complex systems, including electric power systems, communication networks, and electrified transportation networks [80]. A fundamental network-based interdependent model based on topological models is proposed in [81]. The disadvantage of this model is that it excludes the electrical property of the power system. To overcome this drawback, an efficient approach considering the power grid and the supporting control and communication network (CCN) is developed in [82]. In this model, substations, generators, and routers are involved. The authors in [83] proposed a comprehensive methodology that models the power system mesh structure and bidirectional links including data uploading and command downloading channels. These communication links connect cyber network nodes as well as a corresponding physical node, in power grids.
- *Flocking-Based Hierarchical Cyber-Physical Models*: References [64] and [65] propose a hierarchical cyber-physical multi-agent model of a smart grid based on the flocking theory. This model considers dynamic nodes, PMUs, and local cyber controllers. The frequency, phase angle, and other related parameters are involved in the generators, which are regarded as physical parts. Moreover, PMUs and local controllers serve as cyber elements. The model concentrates on control strategies for robustness and resilience of a coupling system.

C. STAGE 3: DEFINE AND APPLY DAMAGE SCENARIOS

The main goal of this stage is to identify damage scenarios for components and system modules when the system is affected by the approaching event. Thus, this stage gives a component view of adverse impacts of the identified threat. In other words, the status of components (on service or out of service) is estimated when influenced by the threat. For extreme natural events and space weather phenomena, fragility curves of components should be convolved with the threat pattern to extract vulnerable components and the extent of their vulnerability. For instance, overhead transmission and distribution lines are susceptible to windstorms, hurricanes, typhoons, and earthquakes, while power plants and substations are susceptible to heavy floods and earthquakes. In addition, power transformers are susceptible to space weather phenomena and Quasi-DC currents. Fragility curves can be derived empirically, experimentally, and analytically using expert judges, or through a combination of these methods [86]. A fragility curve specifies the failure probability of a component conditioned on the impact of a continuous range of threat intensities. In practice, a threshold value is compromised for each component as the failure probability over which the component is considered out of service.

In contrast to extreme natural events and space weather phenomena, damages incurred by cyber-attacks, physical attacks, and technical cascading failures are not represented by fragility curves. Damages incurred by these events depend on the threat identified, which differs from one case to another. Once the event is characterized through methods presented in stage 2, the damage status of each asset (including physical components and software applications and procedures) is recognized. Once the component view is accomplished, sub-system models (including system configuration, available components, services, resources, and infrastructures, etc.) are obtained. The result of this stage will specifically be used as a hint for the operator to perform a proactive management as will be discussed in the next stage.

D. STAGE 4: PERFORM PROACTIVE MANAGEMENT

In this stage, proactive management is performed to control the HR event by preparing for possible future problems or acting in anticipation of future problems. As mentioned in Section VI, proactive grid management is particularly performed during the avoidance phase with the goal of elevating the level of preparedness and mitigating the forecasted damaging consequence of HR events (see Fig. 3). The component and sub-system views obtained in the previous stage are helpful hints to understand how the power system should be prepared and operated prior to the event to mitigate possible damages at the onset of event. For instance, knowing that a substation is at the risk of outage due to a possible threat by flooding, the system operator may decide on preparing a mobile substation at the location under consideration prior to the event. In this circumstance, increasing the system scheduled reserve may be another solution to enhance the system preparedness against the characterized threat. The areas of proactive grid management are: 1) decision support systems (DSSs); 2) synchrophasor solutions; 3) symbiotic integration of synchrophasors with fast-acting controls [87]. Particularly, the authors in [88] have proposed a proactive management scheme in microgrids in order to elevate the level of preparedness in the face of HR events.

E. STAGE 5: FIND THE SYSTEM DEGRADATION

This stage is devised to give a system view (rather than a component view in stage 3) of adverse impacts imposed by an HR event. At first, the power system pre-event model is built using network-related data such as network single line diagram, load profile, critical loads and load supply priority, and available generation resources.

Regarding extreme natural events and space weather phenomena, the next step is convolving (mapping) the event profile characterized in stage 2 with the fragility curves of components. To do this, analytical and simulation-based techniques have been presented in the literature [24]. Analytical methods are usually suitable for small-scale networks due to their simplicity and low computational

burden while simulation-based methods are preferred for large-scale networks with high complexity. Among the analytical methods, Markov process is the most popular one in the literature [89]–[91]. Markov process models the step-by-step degradation of power system by making sequential chains representing the time-dependent evolution of the event impacts on the power system. Optimal power flow (OPF) algorithms are applied at each chain to find out the system degradation at the corresponding time instant. Scenario-based methods are also applicable to perform analytical calculations. If the number of vulnerable components is M, then 2^M anticipated damage scenarios (or a range of damage outcomes when incorporating uncertainty) are defined. Then, OPF algorithms are applied to the event-affected network in each scenario to realize the system status in defined scenarios at each time step during the event. The expected value of the questioned performance indicator (e.g., load supplied) will then be calculated for each time instant. Monte Carlo simulation (MCS) is the dominant approach among the simulation-based methods. Sequential MCS-based time-series enable the representation of events in a chronological order as they occur in reality in different locations of the system [23]. At each time instant, the event profile is convolved (mapped) with fragility curves of components and the procedure is taken for a large number of iterations. At each iteration, the failure probability of the component is compared with a uniformly distributed random number $r \sim U(0,1)$. If the failure probability of the component is greater than r, the component is considered damaged. The OPF algorithms can then be performed on the event-affected power system. Considering a large number of iterations, the expected value of the questioned performance indicator will then be obtained for the time instant under study [60].

Regarding technical cascading failures, the system degradation is obtained as the event is characterized (in stage 2). This is mainly due to the fact that the power system model is incorporated into the problem when identifying cascading failures. Indeed, the output of methods introduced in stage 2 (to characterize technical cascading failures) provides further information about the time-dependent performance of the power system [92].

In order to model the system degradation under cyber and physical attacks, attacker-defender-planner models are usually applied. In these models, the power system is analyzed iteratively under the budget constraints associated with attacker and defender. At each iteration, the impact of the event on the power system model is identified through methods discussed in stage 2. Then, an OPF is solved to discover the power system performance under associated constraints for both defender and attacker sides [5], [28], [93].

F. STAGE 6: RECOVER THE EVENT-AFFECTED SYSTEM

Despite all the efforts to save the system, blackouts are inevitable on many occasions, and consequently, power system resilience highly depends on the recovery process which is performed subsequent to the system survival phase (i.e., t_m in Fig. 3). This process itself includes the system restoration process that is carried out immediately after the survival phase, and the infrastructural recovery process that is performed by the repair crew in a longer time horizon, even days or weeks after the event. System operators can decide on appropriate restoration strategies based on the real-time system status and available resources. Moreover, microgrids would expedite the restoration process since they enable a simultaneously two-sided process, i.e., a downward process from the transmission grid and an upward process from the distribution level [2].

Although the restoration process can elevate the level of system performance, often the system does not return to the initial point prior to the event. It is mainly due to the significant loss of components during the HR events. The uncertainty of repair time depends on the severity of the event in addition to the quality of service (QoS) provided by the repair crew. Thus, appropriate possibilistic models should be employed to represent the mean time to repair (MTTR) for each failed component. The efficiency of the infrastructure recovery is also dependent on the availability and responsibility of interdependent infrastructures (such as gas and water networks, transportation systems, communication systems, etc.). Thus, a proper model should be devised to address the interdependence of power systems and other critical infrastructures. A more detailed explanation of the recovery process can be found in [50].

G. STAGE 7: EVALUATE THE RESILIENCE LEVEL

Using the resilience metric defined in stage 1, the level of resilience will be determined by the end of stage 6. Note that potential impacts of extreme weather events on the power system may be represented through probabilistic methods due to convolution of fragility curves with the event profile as discussed in stage 5. In this circumstance, the expected value of the performance index is calculated as the weighted sum of the performance index in all scenarios and the probability of each scenario is used as the associated weight of that scenario. Doing so for all time slots, the temporal variation of the expected performance index is obtained from which the resilience metric could be computed. It could thus be inferred that the resilience metric evaluates the expected behavior of power system against the extreme weather event. The specified metric in (1) conveys information about each phase of resilience (i.e., avoidance, survival, and recovery) in addition to the power system resilience as a whole. This metric provides the operator with the necessary information about the current status of resilience in the system and facilitates the assessment of alternatives for improvements. Such alternatives include, but are not limited to, infrastructure improvements, policy or operational revisions, and additional resources for recovery. The challenges and opportunities of possible practical measures for improving the grid resilience will be discussed thoroughly in the next section of this paper.

IX. RESILIENCE IMPROVEMENT

A. POTENTIAL AREAS OF RESILIENCE IMPROVEMENT: WHAT ACTIONS DO WE NEED TO IMPROVE RESILIENCE?

As mentioned earlier, the alarming rate of HR events (including black and gray swans) recalls the necessity of employing practical measures to cope with their adverse impacts. Note that the term ''alarming rate'' may imply a paradox because HR events are inherently classified as ''rare'' events. To clarify this, we should emphasize that although the number of HR events has increased on an unprecedented scale, they are still considered to be rare in comparison with credible (e.g., N-1) contingencies. Additionally, power system operators usually do not consider HR events in their analyses and studies, mainly due to their rareness as well as their unknown (or even unknowable) nature. In this section, we aim to propose a set of practical methods to incorporate these events in power system studies.

In the previous section, we presented a general framework for assessing the resilience of the grid, and in this section, we aim to identify potential areas of resilience improvement and then investigate practical measures associated with each area.

Fig. 8 presents a general view of resilience-improvement process, potential areas of resilience improvement, and the pertinent requirements of each area. According to this figure, from a short-term operation perspective, resilience improvements can be performed in three intervals: prior to, during, and after an HR event. Robustness is the ability of power system to keep operating while being stressed by the envisaged event. A power system mainly benefits from a degree of robustness due to inherent strength of components and hardening measures taken with the aim of reinforcing the grid. In addition, prior to an upcoming HR event (in the avoidance phase), proactive measures are taken to enhance the system robustness against the predicted event. The goal in this stage is to anticipate and absorb shocks and keep operating or to stay standing in face of the upcoming event [94]. During the event (in the survival phase), the system is degraded and corrective measures are taken to cope with the event and soften the system downgrade. Resourcefulness (the ability to align technical and human facilities in an efficient manner) and redundancy (the capability to start up or employ substitutes and alternative solutions) are the most important requirements of power system in the survival phase. Finally, after the HR event, rapidity (the ability of power system to quickly get back to normal state through restorative measures) is the key requirement of the recovery phase.

From a long-term perspective, resilience improvement could be achieved by learning new lessons from previous events with the goal of revising plans, reinforcing the grid, modifying procedures, and introducing new tools and technologies. In addition to lessons learned from previous events, long-term planning studies can also be performed to find out impacts of possible future events on the power system which in turn results in identifying a set of planning-oriented measures against the HR event under study. As shown in Fig. 8, post-event learning acts as a feedback from previous lessons or predicted impacts of possible future events to operation-oriented measures with the aim of improving the robustness, preparedness, redundancy, resourcefulness, and rapidity capabilities before the next catastrophe [43].

B. RESILIENCE IMPROVEMENT STRATEGIES

1) CLASSIFICATION

Fig. 9 represents a general classification of resilience improvement measures. As discussed in the previous section, based on possible time-scales for analyzing power system resilience, improvement measures can be divided into two main groups: planning-oriented measures and operation-oriented measures. Planning-oriented measures are intended for i) reinforcing the infrastructure assets through hardening measures, ii) devising the facilities required for efficient implementation of operation-oriented measures, and iii) maintenance scheduling of equipment and optimal allocation of resources. On the other hand, operation-oriented measures refer to adaptive and intelligent control strategies which are utilized for dealing with HR events.

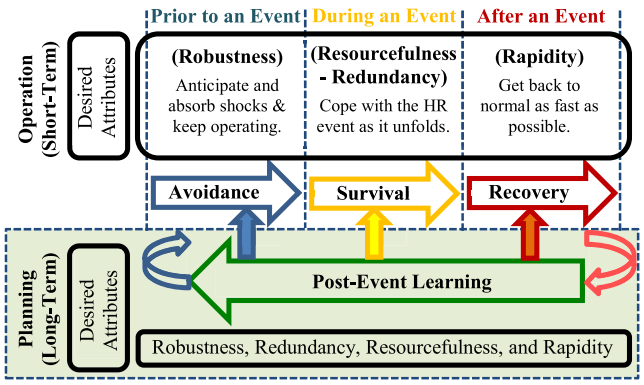

FIGURE 8. Different areas of resilience enhancement.

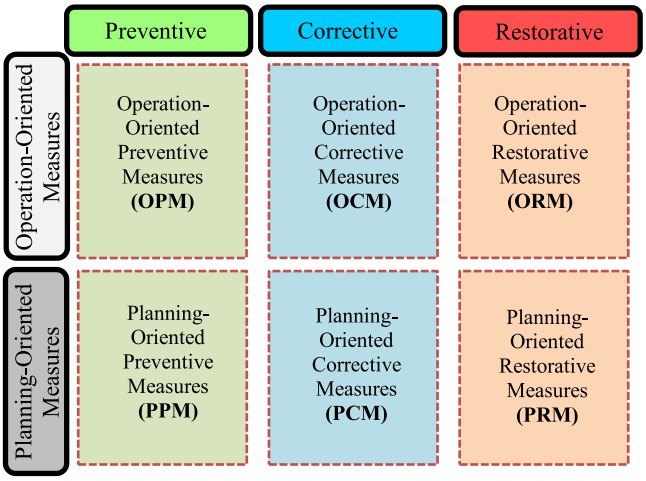

FIGURE 9. A General classification of resilience improvement measures.

Operation-oriented measures also cover the activities conducted during system restoration and infrastructure recovery.

From an action-based perspective, resilience improvement measures are divided into preventive, corrective, and restorative categories based on their functionality. Preventive measures aim to reduce the risk of failure for components, procedures, and applications prior to the event (in the avoidance phase). Corrective measures focus on revising the system performance during the event (in the survival phase) while restorative measures intend to restore the system performance to its pre-event status after the event (in the recovery phase).

2) OPERATION-ORIENTED MEASURES

Fig. 10 illustrates the mechanism of action of different operation-oriented measures before, during, and after an HR event. As mentioned earlier in Section V, HR events are predictable, from a few seconds to several hours before the event by looking for the warning signs of a process excursion. The instant at which the possibility of an HR event increases (i.e., t_0), the power system enters the avoidance phase. Developing appropriate models for an approaching event and analyzing its potential impacts on the system are two important tasks that can improve the preparedness and robustness of the system in this phase. Indeed, predicting the systems' status during and after a progressing HR event helps the system operator proactively anticipate and absorb possible shocks by taking some operation-oriented preventive measures (OPMs). For instance, increasing the scheduled reserve, generation rescheduling, CVR, and manning of normally unmanned substations are some examples of OPMs. In general, OPMs would change the operating point of the system (see Fig. 2), and as a consequence, the performance degradation will be reduced in the survival phase and the restoration process will be accelerated in the recovery phase [94]–[96]. For instance, in a power system with a high penetration of wind farms, the initial degradation in the system's performance in face of a windstorm may occur when the wind speed reaches the cut-out speed of wind turbines. Thus, the system operator could proactively perform a generation rescheduling excluding wind turbines to compensate for the lost generation as an OPM. In this way, the degradation will be postponed to stronger windstorms that affect the overhead transmission and distribution lines. As another viable OPM, the authors in [88] proposed a proactive management scheme in microgrids in order to enhance the system's preparedness for unintentional islanding events.

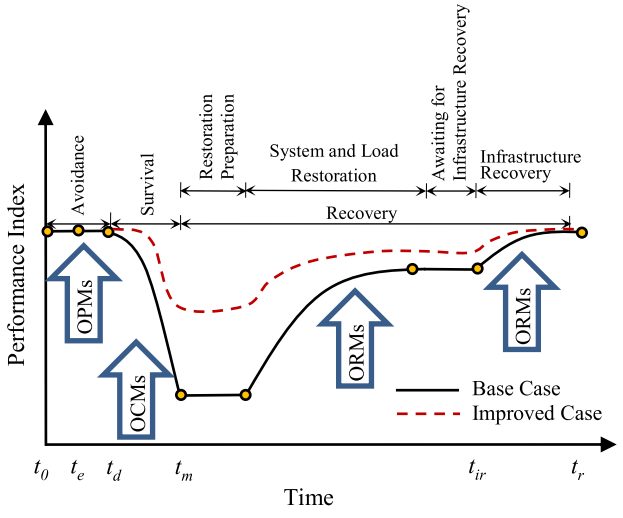

FIGURE 10. Effectiveness of operation-oriented measures.

As the power system enters the survival phase at t_d, control and protection schemes should be activated as operation-oriented corrective measures (OCMs) in order to preserve the power system functionality as much as possible. The main purpose of OCMs is to keep the power system from further cascading outages and total collapse. Advanced visualization and situational awareness are essential prerequisites for active interaction with the system as the event unfolds. Load shedding and controlled islanding are among the important OCMs usually implemented in this phase.

Once the system performance settles at a minimum level at t_m, the recovery process commences. As shown in Fig. 10, the recovery process is comprised of four temporal stages. In the first stage, namely the ''restoration preparation'' stage, the post-event system status is evaluated, a target level for system performance is defined, a strategy for rebuilding the network is selected, the system is sectionalized into a few subsystems (in the case of widespread blackouts), and steps are taken to supply the critical loads with the initial sources of power that are available in each subsystem [97]. Depending on the severity of the HR event, the target performance level may not be similar to the pre-event level, but it is important that it is clearly defined in advance to avoid missteps during the restoration process [98].

In the second stage (i.e., system and load restoration), the main goal is reintegration of the power network, as a means to achieving the ultimate objective of load restoration. To this end, skeleton transmission paths are energized, subsystems defined in the first stage are resynchronized, baseload units are prepared for restart, and sufficient load is restored to maintain the load-generation equilibrium. Note that the primary objective in this phase is to minimize the unserved loads, and the size of load pickups will be determined based on the response rate capabilities of available generators [50]. The effective system response rate and the responsive reserve increase with the combined capacity of the online generators, and load restoration can be accomplished in increasingly larger steps [50], [98]. All of the aforementioned tasks, which are known as operation-oriented restorative measures (ORMs), require either comprehensive guidelines that have been developed in advance or online decision-making tools.

As mentioned earlier, the level of system performance often does not return to the pre-event level due to potential damage to critical infrastructure assets. Thus, the last

two stages of the recovery process are dedicated to infrastructure recovery (see Fig. 10). Infrastructure recovery may take hours, days or even weeks depending on the severity of the HR event, availability of other critical infrastructures, and efficiency of the repair crew's actions. Thus, repair actions should be optimally planned so that the infrastructure recovery will be fulfilled in a timely manner.

3) PLANNING-ORIENTED MEASURES

Planning-oriented measures include devising or revising preventive, corrective, and restorative actions in order to improve the robustness, preparedness, redundancy, resourcefulness, and rapidity capabilities before the next catastrophe occurs. Specifically, planning-oriented preventive measures (PPMs) are intended for foreseeing and granting system requirements to proactively anticipate HR events and prevent system degradation. Hardening (reinforcing) measures are introduced as one category of PPMs taken to increase system robustness against HR events. For instance, elevating substations and reinforcing transmission and distribution poles are two hardening measures taken against heavy floods and hurricanes, respectively. Devising OPMs is the second aspect of PPMs. Successful implementation of OPMs in the avoidance phase is highly dependent on the quality of long-term PPMs. Planning software and hardware tools for system condition monitoring, demand-side management and load control, and VAR compensation resources are examples of PPMs required to improve the functionality of OPMs in the avoidance phase. The third aspect of PPMs is planning the maintenance and repair activities of system assets and equipment. In particular, a substantial number of cascading failures are initiated from the malfunction of critical software or hardware assets. Therefore, maintenance and repair activities should be performed in time to avoid sudden failure or malfunction of critical assets such as transformers, generators, transmission and distribution lines, insulators, relays and switches, etc. It is to be noted that real-time monitoring data should be implemented to proactively detect and resolve possible malfunctions in critical assets.

Likewise, planning-oriented corrective measures (PCMs) are taken to equip the system with the tools required for the implementation of OCMs in the survival phase. Optimal placement of separation relays, which endows the grid with structural modularity and enables the deployment of intentional islanding during the survival phase is a pradigm for PCMs. Moreover, segmentation of the transmission network into subnetworks connected through HVDC links to confine a cascading failure to the originating subsystem [99] and partial restructuring of the distribution systems into microgrids [100] are among the most important PCMs proposed by the Electric Power Research Institute (EPRI). Finally, planning-oriented restorative measures (PRMs) are implemented to improve the efficiency of ORMs during the process. Optimal allocation of black start resources and ensuring enough spare parts for critical assets are examples of PRMs that can expedite the recovery process.

It should be noted that planning-oriented measures for improving resilience are different from those of reliability in two aspects. One is the complexity of modeling HR events (black or gray swans) in resilience studies while there is less complexity in modeling credible contingencies in reliability studies. The second refers to the fact that the resilience assessment framework should be accurately accomplished to assess the impact of each planning-oriented measure on the temporal process of the system response (see Fig. 6). In contrast, a long-term average framework is taken into account in reliability studies.

Table 1 provides a detailed list of improvement strategies [2], [3], [88], [94]–[96], [101], [102], which are categorized based on their functionality. It must be stressed that some of these strategies, which elevate the resilience in multiple ways, are categorized in a specific class titled ''multifaceted.'' In the following paragraphs, we will explain how these strategies fall into the identified categories with illustrative examples.

TABLE 1. Resilience improvement strategies.

Strategy	Type
Proactive Management: Deploying resilience-oriented optimal power flow; manning of normally unmanned (sub) stations; giving updated training and plans to personnel prior to the event.	Preventive
Robustness Improvement: Undergrounding distribution and transmission lines; elevating substations; reinforcing poles and structures with stronger materials; relocating facilities to areas less prone to weather events; developing protocols for encrypted communication of critical data; vegetation management.	
Devising advanced control capabilities such as intentional islanding, automatic feeder switching, conservation voltage reduction (CVR), adaptive load shedding, adaptive protection, demand-side management, and fast operation of HVDC devices in order to reduce the number of customers affected by an HR event.	Corrective
Managing spare parts for critical equipment; building mobile generation units and substations; unit restarting and/or synchronization, load restoration, resynchronization of areas; performing network reconfiguration; coordinated scheduling of repair actions for infrastructure recovery.	Restorative
Building redundant transmission/distribution routes to provide greater ability to bypass damaged lines and reduce the risk of cascading failures; segmentation of the transmission network into sub-networks connected through HVDC links to confine a cascading failure to the originating subsystem; developing DC networks; developing DERs and microgrids which endow the system with structural modularity and hierarchies; developing synchrophasor technology with the ability to increase the visualization and situational awareness; assessing the interdependence of critical infrastructures (water, transportation, fuel, telecommunication, etc.) and plan appropriate alternatives in case of infrastructure outage.	Multifaceted

For example, *deploying resilience-oriented optimal power flow* falls into the proactive management category. This approach usually changes the system operating states to a more conservative point (e.g., more spinning reserve) and therefore, increases the system preparedness to extreme events. Indeed, the system operator rescues the power grid

encountering severe contingencies at the expense of additional preparation cost (see [88], [94], [96], [103] for numerical studies on proactive management).

Overhead lines are exposed to physical damages during the HR events such as extreme weather conditions. *Undergrounding distribution and transmission lines* is a pre-disturbance strategy (i.e., robustness improvement) which can be effectively used to overcome the aforementioned weakness (see [104] for a detailed analysis of undergrounding).

Adaptive load shedding and protection schemes play an important role following the HR events. These methods, if they are designed and implemented effectively, could significantly decrease the performance reduction of the system after the event occurrence. Thus, they are categorized in the corrective actions class in the table (see [48], [49] for numerical studies on adaptive load shedding).

Building mobile generation units and substations will help restore the grid to the normal operating condition much faster, when the generation units/substations are significantly damaged and a considerable amount of time is needed to fix them. Accordingly, this strategy is classified as a restorative resilience improvement strategy (see [105] for more details).

As mentioned earlier, the strategies in the manifested group can enhance the resilience in multiple ways. For example, let consider *building redundant transmission/distribution routes to provide greater ability to bypass damaged lines and reduce the risk of cascading failures*. This approach can obviously improve the robustness of the grid to HR events as it increases the stability margin of the system. Additionally, existence of redundant lines in the system makes the restoration process much faster and easier since the flexibility of the network is reinforced with this strategy.

It is worth mentioning that for each one of the foregoing strategies, we need to make a compromise between the cost of the strategy deployment and the profit resulting from the resilience enhancement. This is an open research topic which must be addressed in the future studies.

C. COST-EFFECTIVENESS ANALYSIS OF IMPROVEMENT STRATEGIES

Planning-oriented measures (mostly recognized with hardening or reinforcing measures, e.g., [60], [93], [106]) are often technically efficient but are not economically affordable. In contrast, operation-oriented measures are often technically less efficient but much more affordable than hardening measures. Thus, a cost-benefit study is required as a guide to take optimal measures in terms of technical and economic issues. A hybrid approach is usually applied to compromise the implementation of cost and technical efficiency.

X. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

Recent widespread blackouts throughout the world have shed light on the fact that electric power networks must not only guarantee reliability against credible contingencies, but also enable resilience to HR events such as earthquakes, cyclones, cyber-attacks, and cascading failures. With this aim in mind, we first characterized the main features of HR events in order to specifically identify the events, attackers, or attacks that can put the system at risk. We then clarified the notion of resilience in power systems and highlighted its differences with other well-established concepts, including reliability, stability, and security. From a resilience-oriented point of view, we drew a comprehensive picture of the state of the system, thereby facilitating the decision-making processes with respect to proactive, corrective, and restorative control actions. Finally, we proposed a new framework for resilience assessment, and identified the main resilience improvement strategies.

Future studies could be conducted on developing appropriate spatiotemporal models for HR events (particularly for a set of events that have been non-modellable so far). Describing the interaction of protection and control systems in the face of HR events is also a promising research direction.

REFERENCES

[1] M. Begovic *et al.*, "Defense plan against extreme contingencies—CIGRE TF C2.02.24," CIGRE, Tech. Rep., 2006.
[2] A. Gholami, F. Aminifar, and M. Shahidehpour, "Front lines against the darkness: Enhancing the resilience of the electricity grid through microgrid facilities," *IEEE Electrifc. Mag.*, vol. 4, no. 1, pp. 18–24, Mar. 2016.
[3] *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*, Executive Office President, White House, Washington, DC, USA, 2013. [Online]. Available: https://www.energy.gov/sites/prod/files/2013/08/f2/GridResiliencyReport_FINAL.pdf
[4] C. Lopez, A. Sargolzaei, H. Santana, and C. Huerta, "Smart grid cyber security: An overview of threats and countermeasures," *J. Energy Power Eng.*, vol. 9, no. 7, pp. 632–647, 2015.
[5] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Ind. Control Syst., Washington, DC, USA, Tech. Rep., 2016.
[6] K. Hole and L.-H. Netland, "Toward risk assessment of large-impact and rare events," *IEEE Security Privacy*, vol. 8, no. 3, pp. 21–27, May/Jun. 2010.
[7] N. N. Taleb, *The Black Swan: The Impact of The Highly Improbable*, vol. 2. New York, NY, USA: Random House, 2007.
[8] F. X. Diebold, N. A. Doherty, and R. J. Herring, *The Known, the Unknown, and the Unknowable in Financial Risk Management*, vol. 1. Philadelphia, PA, USA: Univ. Pennsylvania, 2008.
[9] D. Dubois and H. Prade, "Possibility theory, probability theory and multiple-valued logics: A clarification," *Ann. Math. Artif. Intell.*, vol. 32, nos. 1–4, pp. 35–66, 2001.
[10] R. E. Bellman and L. A. Zadeh, "Decision-making in a fuzzy environment," *Manage. Sci.*, vol. 17, no. 4, pp. B-141–B-164, 1970.
[11] G. J. Klir and B. Yuan, *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Upper Saddle River, NJ, USA: Prentice-Hall, 1995.
[12] F. H. Knight, *Risk, Uncertainty, and Profit*. Chelmsford, MA, USA: Courier Corporation, 2012.
[13] B. M. Ayyub, "Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making," *Risk Anal.*, vol. 34, no. 2, pp. 340–355, 2014.
[14] B. M. Ayyub, "On uncertainty in information and ignorance in knowledge," *Int. J. Gen. Syst.*, vol. 39, no. 4, pp. 415–435, 2010.
[15] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-Technical Systems*. Farnham, U.K.: Ashgate Publishing, 2012.
[16] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*. Hoboken, NJ, USA: Wiley, 2009.
[17] B. J. Garrick, *Quantifying and Controlling Catastrophic Risks*. San Diego, CA, USA: Academic, 2008.
[18] "The resilience of the electricity system," United Kingdom Parliament, House Lords, London, U.K., 1st Rep. Session 2014-15, Feb. 2015.
[19] M. Vaiman *et al.*, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, May 2012.

[20] *U.S.—Canada Power System Outage Task Force: Final Report on the Implementation of Task Force Recommendations*, Dept. Energy, Washington, DC, USA, 2004.
[21] P. Henneaux, P.-E. Labeau, and J.-C. Maun, "A level-1 probabilistic risk assessment to blackout hazard in transmission power systems," *Rel. Eng., Syst. Safety*, vol. 102, pp. 41–52, Jun. 2012.
[22] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renew. Sustain. Energy Rev.*, vol. 80, pp. 9–22, Apr. 2017.
[23] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters—A review," *IEEE Trans. Power Syst.*, vol. 31, no. 2, pp. 1604–1613, Mar. 2016.
[24] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electr. Power Syst. Res.*, vol. 127, pp. 259–270, Oct. 2015.
[25] A. Abbaspour, A. Sargolzaei, and K. Yen, "Detection of false data injection attack on load frequency control in distributed power systems," in *Proc. North Amer. Symp. (NAPS), NAPS*, 2017, pp. 1–6.
[26] A. Sargolzaei, K. K. Yen, M. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901–15912, 2017.
[27] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, Mar. 2016.
[28] S. Sridhar, "Cyber risk modeling and attack-resilient control for power grid," Ph.D. dissertation, Dept. Elect. Comput. Eng., Iowa State Univ., Ames, IA, USA, 2015.
[29] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, *Smart Grids: Security and Privacy Issues*. New York, NY, USA: Springer, 2017.
[30] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, *Security Challenges of Networked Control Systems*, vol. 145. New York, NY, USA: Springer, 2018.
[31] E. I. Bilis, W. Kroger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Syst. J.*, vol. 7, no. 4, pp. 854–865, Dec. 2013.
[32] N. Nezamoddini, S. Mousavian, and M. Erol-Kantarci, "A risk optimization model for enhanced power grid resilience against physical attacks," *Electr. Power Syst. Res.*, vol. 143, pp. 329–338, Feb. 2017.
[33] J. G. Kappenman, *The Vulnerability of the US Electric Power Grid to Space Weather and the Role of Space Weather Forecasting*. Goleta, CA, USA: Metatech Corporation, 2003.
[34] N. Suri and G. Cabri, *Adaptive, Dynamic, and Resilient Systems*. New York, NY, USA: Auerbach, 2014.
[35] *Organizational Resilience: Security, Preparedness and Continuity Management Systems*, Standard ASIS SPC.1-2009, ASIS International.
[36] A. R. Berkeley, III, M. Wallace, and C. Coo, "A framework for establishing critical infrastructure resilience goals," Nat. Infrastruct. Advisory Council, U.S. Dept. Homeland Secur., Washington, DC, USA, Final Rep., 2010.
[37] C. Perrings, "Resilience and sustainable development," *Environ. Develop. Econ.*, vol. 11, no. 4, pp. 417–427, 2006.
[38] W. N. Adger, "Social and ecological resilience: Are they related?" *Prog. Human Geogr.*, vol. 24, no. 3, pp. 347–364, 2000.
[39] E. Hollnagel, D. D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. Farnham, U.K.: Ashgate Publishing, 2007.
[40] E. Jen, "Stable or robust? What's the difference?" *Complexity*, vol. 8, no. 3, pp. 12–18, 2003.
[41] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renew. Sustain. Energy Rev.*, vol. 58, pp. 1060–1069, May 2016.
[42] A. W. Righi, T. Abreu, P. Wachs, T. A. Saurin, and P. Wachs, "A systematic literature review of resilience engineering: Research areas and a research agenda proposal," *Reliab. Eng. Syst. Safety*, vol. 141, pp. 142–152, Sep. 2015.
[43] (2012). *Severe Impact Resilience?: Considerations and Recommendations*. [Online]. Available: https://www.nerc.com/comm/OC/SIRTF Related Files DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf
[44] H. H. Willis and K. Loa, "Measuring the resilience of energy distribution systems," RAND Corporation, Santa Monica, CA, USA, Tech. Rep., 2015.
[45] M. A. Pflanz, *On the Resilience of Command and Control Architectures*. Fairfax, VA, USA: George Mason Univ., 2011.
[46] C. Ji, Y. Wei, and H. V. Poor. (2016). "Resilience of energy infrastructure and services: Modeling, data analytics and metrics." [Online]. Available: https://arxiv.org/abs/1611.06914
[47] M. Bruneau *et al.*, "A framework to quantitatively assess and enhance the seismic resilience of communities," *Earthquake Spectra*, vol. 19, no. 4, pp. 733–752, 2003.
[48] T. Shekari, A. Gholami, F. Aminifar, and M. Sanaye-Pasand, "An adaptive wide-area load shedding scheme incorporating power system real-time limitations," *IEEE Syst. J.*, vol. 12, no. 1, pp. 759–767, Mar. 2016.
[49] T. Shekari, F. Aminifar, and M. Sanaye-Pasand, "An analytical adaptive load shedding scheme against severe combinational disturbances," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 4135–4143, Sep. 2016.
[50] A. Gholami and F. Aminifar, "A hierarchical response-based approach to the load restoration problem," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1700–1709, Jul. 2015.
[51] A. Arab, A. Khodaei, S. K. Khator, and Z. Han, "Electric power grid restoration considering disaster economics," *IEEE Access*, vol. 4, pp. 639–649, 2016.
[52] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1289–1310, Jul. 2017.
[53] M. Ouyang and L. Dueñas-Osorio, "Multi-dimensional hurricane resilience assessment of electric power systems," *Struct. Safety*, vol. 48, pp. 15–24, May 2014.
[54] M. D'Lima and F. Medda, "A new measure of resilience: An application to the London underground," *Transp. Res. A, Policy Pract.*, vol. 81, pp. 35–46, Nov. 2015.
[55] M. Bevilacqua, F. E. Ciarapica, and G. Marcucci, "Supply chain resilience triangle: The study and development of a framework," *World Acad. Sci. Eng. Technol. Int. J. Soc. Behav. Edu. Econ. Bus. Ind. Eng.*, vol. 11, no. 8, pp. 1923–1930, 2017.
[56] K. Tierney and M. Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR News*, vol. 250, pp. 14–18, May/Jun. 2007.
[57] L. H. Fink and K. Carlsen, "Operating under stress and strain," *IEEE Spectr.*, vol. 15, no. 3, pp. 48–53, Mar. 1978.
[58] D. G. Dessavre, J. E. Ramirez-Marquez, and K. Barker, "Multidimensional approach to complex system resilience analysis," *Reliab. Eng. Syst. Safety*, vol. 149, pp. 34–43, May 2016.
[59] J.-P. Watson *et al.*, "Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2014-18019, 2014.
[60] S. Espinoza, M. Panteli, P. Mancarella, and H. Rudnick, "Multi-phase assessment and adaptation of power systems resilience to natural hazards," *Electr. Power Syst. Res.*, vol. 136, pp. 352–361, Jul. 2016.
[61] A. Clauset, C. R. Shalizi, and M. E. J. Newman, "Power-law distributions in empirical data," *SIAM Rev.*, vol. 51, no. 4, pp. 661–703, 2009.
[62] L. de Haan and A. Ferreira, *Extreme Value Theory: An Introduction*. New York, NY, USA: Springer, 2006.
[63] *UKCP09 Project—UK Climate Projections*, Defra and Met Office, U.K., 2009.
[64] *Hazus-MH 2.1: Technical Manual*, National Institute of Building Sciences, Federal Emergency Manage. Agency, (NIBS FEMA), Washington, DC, USA, 2015, p. 718.
[65] Y. Dai, G. Chen, Z. Dong, Y. Xue, D. J. Hill, and Y. Zhaod, "An improved framework for power grid vulnerability analysis considering critical system features," *Phys. A, Stat. Mech. Appl.*, vol. 395, pp. 405–415, Feb. 2014.
[66] A. Dwivedi and X. Yu, "A maximum-flow-based complex network approach for power system vulnerability analysis," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 81–88, Feb. 2013.
[67] E. Ciapessoni, D. Cirio, and A. Pitto, "Cascadings in large power systems: Benchmarking static vs. time domain simulation," in *Proc. IEEE Power Energy Soc. General Meeting*, Oct. 2014, pp. 1–5.
[68] X. Zhang, C. Zhan, and C. K. Tse, "Modeling the dynamics of cascading failures in power systems," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 192–204, Jun. 2017.
[69] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos Interdiscip. J. Nonlinear Sci.*, vol. 17, no. 2, p. 26103, 2007.
[70] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probab. Eng. Inf. Sci.*, vol. 19, no. 1, pp. 15–32, 2005.

[71] S. Mei, F. He, X. Zhang, S. Wu, and G. Wang, "An improved OPA model and blackout risk assessment," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 814–823, May 2009.
[72] D. P. Nedic, "Criticality in a cascading failure blackout model," *Int. J. Elect. Power Energy Syst.*, vol. 28, no. 9, pp. 627–633, 2006.
[73] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. H. Hines, "Dynamic modeling of cascading failure in power systems," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2085–2095, May 2016.
[74] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, and S. Mei, "A multi-timescale quasi-dynamic model for simulation of cascading outages," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3189–3201, Jul. 2016.
[75] J. P. Paul and K. R. W. Bell, "A flexible and comprehensive approach to the assessment of large-scale power system security under uncertainty," *Int. J. Elect. Power Energy Syst.*, vol. 26, no. 4, pp. 265–272, 2004.
[76] P. Henneaux, P.-E. Labeau, J.-C. Maun, and L. Haarla, "A two-level probabilistic risk assessment of cascading outages," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2393–2403, May 2016.
[77] N. Bhatt *et al.*, "Assessing vulnerability to cascading outages," in *Proc. IEEE/PES Power Syst. Conf. Expo. (PSCE)*, Mar. 2009, pp. 1–9.
[78] J. Chen, J. S. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *Int. J. Elect. Power Energy Syst.*, vol. 27, no. 4, pp. 318–326, May 2005.
[79] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model validation for the August 10, 1996 WSCC system outage," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 967–979, Aug. 1999.
[80] M. H. Amini, K. G. Boroojeni, S. S. Iyengar, P. M. Pardalos, F. Blaabjerg, and A. M. Madni, *Sustainable Interdependent Networks: From Theory to Application*. Cham, Switzerland: Springer, 2018.
[81] C. M. Schneider, N. Yazdani, N. A. M. Araújo, S. Havlin, and H. J. Herrmann, "Towards designing robust coupled networks," *Sci. Rep.*, vol. 3, no. 1, p. 1969, 2013.
[82] M. Parandehgheibi and E. Modiano. (2013). "Robustness of interdependent networks: The case of communication networks and the power grid." [Online]. Available: https://arxiv.org/abs/1304.0356
[83] Y. Wang, Z. Lin, X. Liang, W. Xu, Q. Yang, and G. Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Frontiers Inf. Technol. Electron. Eng.*, vol. 17, no. 5, pp. 465–478, 2016.
[84] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, "A flocking-based dynamical systems paradigm for smart power system analysis," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2012, pp. 1–8.
[85] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.
[86] C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power system resilience to extreme weather: Fragility modeling, probabilistic impact assessment, and adaptation measures," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3747–3757, Sep. 2016.
[87] J. Giri, "Proactive management of the future grid," *IEEE Power Energy Technol. Syst. J.*, vol. 2, no. 2, pp. 43–52, Jun. 2015.
[88] A. Gholami, T. Shekari, F. Aminifar, and M. Shahidehpour, "Microgrid scheduling with uncertainty: The quest for resilience," *IEEE Trans. Smart Grid*, vol. 7, no. 6, pp. 2849–2858, Nov. 2016.
[89] Y. Liu and C. Singh, "Reliability evaluation of composite power systems using Markov cut-set method," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 777–785, May 2010.
[90] R. Billinton and J. Acharya, "Consideration of multi-state weather models in reliability evaluation of transmission and distribution systems," in *Proc. Can. Conf. Elect. Comput. Eng.*, 2005, pp. 916–922.
[91] A. I. Sarwat, A. Domijan, M. H. Amini, A. Damnjanovic, and A. Moghadasi, "Smart Grid reliability assessment utilizing Boolean driven Markov process and variable weather conditions," in *Proc. North Amer. Power Symp. (NAPS)*, 2015, pp. 1–6.
[92] Q. Chen, "The probability, identification, and prevention of rare events in power systems," Ph.D. dissertation, Dept. Elect. Eng., Iowa State Univ., Ames, IA, USA, 2004.
[93] S. D. Manshadi and M. E. Khodayar, "Resilient operation of multiple energy carrier microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2283–2292, Sep. 2015.
[94] M. H. Amirioun, F. Aminifar, and H. Lesani, "Resilience-oriented proactive management of microgrids against windstorms," *IEEE Trans. Power Syst.*, to be published.
[95] M. H. Amirioun, F. Aminifar, and H. Lesani, "Towards proactive scheduling of microgrids against extreme floods," *IEEE Trans. Smart Grid*, to be published.
[96] A. Gholami, T. Shekari, and S. Grijalva, "Proactive management of microgrids for resiliency enhancement: An adaptive robust approach," *IEEE Trans. Sustain. Energy*, to be published.
[97] M. M. Adibi and N. Martins, "Power system restoration dynamics issues," in *Proc. IEEE Power Energy Soc. General Meeting, Convers. Delivery Elect. Energy 21st Century (PES)*, Jul. 2008, pp. 1–8.
[98] M. M. Adibi and L. H. Fink, "Power system restoration planning," *IEEE Trans. Power Syst.*, vol. 9, no. 1, pp. 22–28, Feb. 1994.
[99] H. Clark, A.-A. Edris, M. El-Gasseir, K. Epp, A. Isaacs, and D. Woodford, "Softening the blow of disturbances," *IEEE Power Energy Mag.*, vol. 6, no. 1, pp. 30–41, Jan./Feb. 2008.
[100] R. Lasseter *et al.*, "Integration of distributed energy resources: The CERTS microgrid concept," Consortium Electr. Rel. Technol. Solutions, USA, LBNL Rep. LBNL-50829, 2002.
[101] M. Panteli and P. Mancarella, "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1733–1742, Sep. 2017.
[102] R. J. Campbell, *Weather-Related Power Outages and Electric System Resiliency*. Washington, DC, USA: Congressional Research Service, 2012.
[103] Y. Wang, M. Shahidehpour, L. L. Lai, L. P. L. P. Huang, H. L. H. L. Yuan, and F. Y. Xu, "Resilience-constrained hourly unit commitment in electricity grids," *IEEE Trans. Power Syst.*, to be published.
[104] L. Xu, "Undergrounding assessment phase 3 report?: Ex ante cost and benefit modeling," Florida Electr. Utilities, Newberry, FL, USA, Tech. Rep., 2008.
[105] *IEEE Guide for Switchgear—Unit Substation—Requirements*, IEEE Standard C37.121-2012, 2013.
[106] S. Ma, B. Chen, and Z. Wang, "Resilience enhancement strategy for distribution systems under extreme weather events," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1442–1451, Mar. 2018.

AMIN GHOLAMI (S'14) received the B.Sc. degree (Hons.) in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2013, and the M.Sc. degree (Hons.) in electrical engineering from the University of Tehran, Tehran, in 2016. He is currently pursuing the Ph.D. degree with the Georgia Institute of Technology, Atlanta, GA, USA. His research interests include power system optimization and control, power system resilience, and smart grid applications.

TOHID SHEKARI (S'14) received the B.Sc. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2013, and the M.Sc. degree in electrical engineering from the University of Tehran, Tehran, in 2016. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. His current research interests include power system resilience, intrusion detection in power system substations, cyber security in power systems, and power system operation.

MOHAMMAD HASSAN AMIRIOUN received the B.Sc. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2011, the M.Sc. degree in electrical power engineering from the Iran University of Science and Technology, Tehran, Iran, in 2013, and the Ph.D. degree in electrical power engineering from the University of Tehran, Tehran, in 2018. His research interests include power system resilience, power systems operation and economics, and integration of electric vehicles in power systems.

FARROKH AMINIFAR (SM'15) received the B.Sc. degree (Hons.) from the Iran University of Science and Technology, Tehran, Iran, in 2005, and the M.Sc. (Hon.) and Ph.D. degrees from the Sharif University of Technology, Tehran, in 2007 and 2010, respectively, all in electrical engineering. He has been collaborating with the Robert W. Galvin Center for Electricity Innovation with the Illinois Institute of Technology, Chicago, IL, USA, since 2009. He is currently an Assistant Professor with the School of Electrical and Computer Engineering, University of Tehran, Tehran. His research interests include wide-area measurement systems, resilience analysis of cyber-physical power system studies, and smart grid initiatives. He received the 2011 IEEE Iran Section Best Ph.D. Dissertation Award, the 2013 IEEE/PSO Transactions Prize Paper Award, the 2015 IEEE Iran Section Young Investigator Award, the 2015 IEEE Transactions on Power Delivery Exceptional Reviewer Award, and the 2017 Outstanding Young Scientist Award of the Iran National Academy of Science. He is serving as an Editor for the IEEE Transactions on Sustainable Energy and the IEEE Power Engineering Letters.

M. HADI AMINI (S'11–GS'13) received the B.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2011, the M.Sc. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2013, and the M.Sc. degree in electrical and computer engineering from the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA in 2015, where he is currently pursuing the Ph.D. degree. He has published over 50 refereed journal and conference papers in the smart energy systems and transportation network-related areas. His current research interests include interdependent networks, distributed/decentralized optimization algorithms in power distribution systems, smart cities, electric vehicles, and smart grid. He is a member of the IEEE-Eta Kappa Nu Sigma Chapter, the honor society of the IEEE. He serves as a Technical Program Committee Member for the *International Conference on Smart Energy Systems and Technologies* (SEST 2018 and SEST 2019). He was a recipient of the Best Paper Award of the *Journal of Modern Power Systems and Clean Energy* in 2016, the Best Reviewer Award of the IEEE Transactions on Smart Grid from the IEEE Power & Energy Society in 2017, the Outstanding Reviewer Award of the IEEE Transactions on Sustainable Energy in 2017, and the Dean's Honorary Award from the President of the Sharif University of Technology in 2007. He ranked 26th among about 270 000 participants in the Nationwide Iranian University Entrance Exam for the B.Sc. degree in 2007. He serves as the Lead Editor for book series *Sustainable Interdependent Networks*. He serves as a reviewer for several high impact journals, and international conferences and symposiums in the field of power systems. www.hadiamini.com.

ARMAN SARGOLZAEI (S'10–M'15) received the M.S. and Ph.D. degrees in electrical and computer engineering from Florida International University (FIU), Miami, FL, USA, in 2012 and 2015, respectively. He was a Faulty Member with the Department of Electrical and Computer Engineering, FIU. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Florida Polytechnic University (FPU), Lakeland, FL, USA, where he oversees the Control Systems Laboratory. His peer-reviewed research on the theory and applications of networked control systems and cyber physical systems has been published in over 60 articles. He has an interdisciplinary background and experience emphasizing on networked control systems, cyber physical systems, and robotics. At FPU, he was recognized with the honor of the 2017 Faculty Research Excellence Award and the 2018 Faculty Research Excellence Award. He is currently part of editorial board for several journals. He serves as a Reviewer for the IEEE Transactions on Smart Grid, the IEEE Transactions on Cybernetics, the IEEE Transactions on Energy Conversion, the IEEE Transaction on Industrial Applications, and the IEEE Access.