# Smart Distribution Networks Resilience Quantification

Subjects: Energy & Fuels | Engineering, Electrical & Electronic | Telecommunications
Contributor: Youba NAIT BELAID

The introduction of pervasive telecommunication devices, in the scope of smart grids (SGs), has accentuated interest in the distribution network, which integrates a huge portion of new grid applications. High impact low probability (HILP) events, such as natural hazards, manmade errors, and cyber-attacks, as well as the inherent fragility of the distribution grid have propelled the development of effective resilience tools and methods for the power distribution network (PDN) to avoid catastrophic infrastructural and economical losses.

Keywords: resilience ; quantification ; smart grids ; power networks ; information and communication networks

## 1. Introduction

Current information and communication technologies (ICTs) have achieved a high degree of penetration in all critical infrastructure (CI) systems, owing to the ever-increasing capabilities of their services in terms of coverage, throughput capacity, latency, scalability, and privacy [1][2][3][4]. In power systems, the massive introduction of telecommunication devices accelerated the shift toward smart grids (SGs) [5] that come with a whole new package of functionalities such as automated control, smart sensing and metering, high-power converters, and modern energy management techniques based on the optimization of demand, energy, and network availability [6]. The high-performance smart grid allows thereby for the insertion of new applications in the network like distributed generation, Industrial Internet of Things (IIOT), and electrical vehicles [7]. This comes, however at the expense of increased complexity, which brings new vulnerabilities and broadens the attack surface [8]. Recent extreme events of natural disasters, cyber-attacks, and man-made errors which we refer to as HILP events, have shown that SGs are susceptible to strong disruptions given the large-scale networks they represent, and the attendant interdependencies [9]. Some recent examples are the power disruptions in the US in 2017, caused by hurricanes and wildfires [10], which caused a cumulative damage of $306.2 billion, affecting a total of 47 million people—nearly 15 percent of the nation's population. For instance, at the peak of hurricane Irma, more than 6.7 million electrical customers were without power [11], and hurricane Maria severely damaged the Puerto Rico power grid leaving 1.5 million people out of power [12]. China's severe ice storm in 2008 resulted in the service disruption of 2000 power substations and 8500 towers leading to power interruptions in 13 provinces and 170 cities [13], and over 4 million customers went on power outage for over seven days during the Great East Japan Earthquake in 2011 [14]. During the Ukraine power grid cyber-attack in 2015, 30 power substations were turned off, and hundreds of thousands of people were without electricity for a period from 1 to 6 h [15][16].

Events like these reveal the need for strategies that are able to cope with such harsh impacts, especially given that the capacity to operate resiliently against attacks and natural disasters is one of the multiple smart grid attributes [17]. Resilience is defined as the ability to "anticipate, absorb, adapt to and/or rapidly recover from a disruptive event" [18]. In line with this definition, the U.S. Presidential Policy Directives-21(PPD-21) introduces resilience as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [19]. This same directive involves the "fail safe" paradigm in system engineering through recommendations for cyber-physical security, while highlighting the shift toward "safe-to-fail" paradigm brought by cyber-physical resilience. Many conceptual frameworks are proposed for understanding and evaluating resilience, where the time dimension is very important, as various facets (anticipation, absorption, robustness, survivability, mitigation, flexibility, adaptability, restoration, and recovery) are linked to different temporal phases that describe system performance during an extreme event [20][21][22][23][24][25]. Resilience moves from traditional risk assessment, which relies on probabilistic analysis of likely failures, toward dealing with unexpected events, requiring mitigation and healing strategies. The main difference is that risk assessment aims to achieve situational awareness and diagnosis, while resilience moves one step further by incorporating reactive actions against the contingency and launching restoration operations, which maintain the functionality of most critical loads and/or make them rapidly recoverable [26].

Within the growing literature on power system resilience [27][28][29][30][31], utilities are particularly interesting in quantitative assessments of resilience, which propose relevant indicators to guide cost-benefit studies before planning investments. In this context, multi-dimensional characteristics of resilience are a considerable challenge [32][33][34]. Ouyang and Dueñas-Osorio [35] tackled technical, organizational, and social dimensions of resilience, while providing an alternative to evaluate the economic dimension by estimation of economic losses. Only the technical dimension of the power network is widely investigated in the literature [36], which reveals the need to examine all other dimensions for a comprehensive analysis of resilience [33][37][38]. Technical and organizational dimensions are the most suitable in the case of power grids as they can be applicable at individual system levels, while social and economic dimensions are better suited for community level (interdependent systems), to which resilience studies should converge in the future [38]. Temporal multi-phase resilience quantification is a well-adopted technique that can embed other dimensions by linking them to technical and organizational dimensions through the implementation of enhancement strategies. Unlike [35], most proposed metrics in literature exclude pre-event and post-recovery phases, suggesting that quantification is conducted for a single scenario and not for a sequence of disruptive events, which corroborates the relevance of resilience for HILP disruptions. Work in [39] introduced resilience-based component importance measures centered in the recovery phase; on the one hand by establishing a ranking for load restoration using optimal repair time, and on the other hand, by quantifying the potential loss in optimal system resilience due to a delay in component repair process (computed through resilience reduction worth metric). Likewise, [40] focuses on the recovery stage of resilience, with the goal of comparing different restoration strategies and selecting an appropriate performance measure. Authors in [41] proposed a multi-phase framework to assess the resilience of the UK power transmission network under a windstorm. The framework considered both infrastructural and operational aspects, introducing four simple metrics to describe the degree and speed of degradation, duration of the disruption, and recovery speed. Grid connectivity and operational metrics can jointly describe the whole span of post-event analysis, and be used for planning short-term mitigation and recovery, or long-term hardening [42]. Resilience strategies to minimize system performance loss can be further analyzed under budget constraint by a tri-level planner-attacker-defender model [43], where a planner optimizes long-term transmission network expansion before an attack hits the system. Short-term switching operations are then applied in reaction. Resilience is quantified using customer demand not supplied, which includes both mitigation and recovery capabilities in the system. Many other optimization models and performance measures are adopted in related studies [44][45].

Given widely stretched power networks, resilience studied at the system level for generation and transmission, does not (or negligibly) include distribution grid components [35][39][40][41][42][43]. In 2010, only 15% to 20% of feeders implement distribution automation in the North American grid, one of the most advanced electrical systems [46]. This illustrates that the PDN is the most fragile level of electrical systems due to legacy “blindness” and manual operations along with electromechanical components [47], especially with the fact that an estimated 90% of customer outages in the US are related to this part of the system [48].

The advent of smart grids renewed interest in enhancing the PDN performance [49] as nearly all SG provided abilities of self-healing, high reliability, energy management, and real-time pricing are empowered by technologies introduced at the distribution level such as advanced metering, automation, distributed generation, and distributed storage [50]. ICTs are the main enabler of this new portfolio of applications [7], by transforming a traditionally one-way, limited-control, and radial PDN into a two-way power flow, intelligent, and mesh-networked grid capable of guaranteeing improved service for all connected loads [51]. In this regard, expected high-performance capabilities of smart distribution grid can succeed in coping with most failures in the system [49][50]. The smart PDN remains susceptible to HILP events, or even more prone in some cases, due to increased uncertainty (in events, load, distributed generation, market prices) [52][53][54] and strong dependency on telecommunications that widen the attack surface [55] and may cause undesirable cascade effects [56]. Consequently, the resilience of smart PDN becomes a concern from both electric and communication domain perspectives, as a failure in the telecommunication service may affect the electric service [57] and vice-versa [58]. Recent publications recommend a joint handling of smart PDN resilience quantification as the robustness and adaptation ability of a coupled system are even lower than a single system [56][59][60][61]. However, such an approach needs to build upon a solid understanding of resilience assessment of electric and communication domains when considered distinctly.

The present paper aims to set the ground for future joint evaluation of PDN resilience by reviewing relevant works, centered thus far on electric service, and to a lesser extent on ICT service. Essentially, the type of HILP event is identified from each selected contribution with details in the method used for contingency characterization. Also, the measure of performance, recognized as an enabler for resilience quantification [62], is tracked through this work to explain how it is defined and computed, relying usually on system modeling, or empirical and surrogate models in some cases. In addition, a classification based on the temporal phase where resilience evaluation takes place is proposed, which allows for addressing practical requirements of utility companies. The resilience phase-based approach was linked with different objectives of the assessment, from simple metrics evaluation, to either planning or response for survivability and recovery,

achieved through a variety of improvement strategies for which allocation is optimized under the constraint of a limited budget. This bridges resilience studies and economic considerations in order to help stakeholders in investment plan elaboration and crisis decision-making. Aspects of cost, critical load, microgrids, and uncertainty of hazards, load, and distributed generation are discussed to show their high importance, and available tools to date for their involvement in the study.

We extend by this work the wide spectrum of subjects associated with resilience quantification in power networks (modeling and simulation, enhancement strategies, metrics, and extreme events), covered in recent reviews [28][36][44][45][63][64][65]. The main contributions and novelty of this paper can be summarized as follows: (a) focus on resilience assessment of both electric and telecommunications domains of smart power distribution networks. (b) Detailed analysis and classification of performance calculation techniques. (c) Fine-grained categorization of quantitative resilience works based on time of evaluation and target objective.

Finally, despite the considerable number of works analyzed and relatively deep examination of reviewed methods for resilience quantification in smart PDNs, this paper does not claim to be comprehensive in the issues addressed (and related references), but remains complete enough to give a good overall perspective of the research trends and understanding of challenges and opportunities.

## 2. Resilience in Smart Grids

Amid desired functionalities for smart grids lays the need for capabilities like: self-healing, high reliability, power quality, and resistance against various disasters and attacks [50]. Resilience represents a promising approach to meet such requirements, by being able to address network circumstances not handled by widely adopted principles of reliability and quality of service.

### 2.1. From Reliability to Resilience

Reliability is the ability of an item (component or system) to operate under designated operating conditions for a designated period of time or number of cycles, where this ability can be formulated through a probability [66]. In electrical networks, this is equivalent to maintaining the delivery of electric services to customers in the face of routine uncertainty under operating conditions [67]. Metrics like Energy Not Supplied (ENS), Average Customer Curtailment Index (ACCI), System Average Interruption Duration Index (SAIDI), System Average Interruption Frequency Index (SAIFI), Customer Average Interruption Duration Index (CAIDI) are widely used to describe PDN reliability [68][69]. System operators use such indicators to track and enhance the performance of their networks. These indices are further used by system regulators and system operators in service level agreements (SLAs), in order to define penalty thresholds and ensure that the right compensation is paid based on the experienced outages. Reliability metrics are relevant to assess the impact of recurrent events with available historical records, over which maintenance actions are applicable; excluding major hazards such as severe weather events [70]. Some of these metrics were extended to capture more severe events, where metrics like STorm Average Interruption Frequency Index (STAIFI) and STorm Average Interruption Duration Index (STAIDI) are proposed [71]. However, a demonstration was made that these two metrics are not relevant for resilience evaluation because, when used during a storm, they show large deviation that can be even greater than the values of STAIDI and STAIFI [62].

Resilience is “the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events” [72]. Unlike reliability, which focuses on the frequency and duration of failures “event-agnostically,” resilience seeks to further track the dynamics and resources of response, adaptability, and ability to restore. This is relevant to HILP hazards where consequences in the system need to be studied with respect to specific events, as each disruption has its distinguishing characteristics [73]. Thus, the fundamental difference resides in the scale, scope, and duration of events handled: resilience targets events with strong impact in a wide geographical area with long duration of outages, while reliability handles local impact in short duration outages [74].

Despite this difference between the two concepts, mainly due to events each of them tackles, they remain closely related because enhancing resilience or reliability may require the same strategies, with resilience being more general, confirming that being resilient typically encompasses being reliable, but not vice versa [75].

### 2.2. Resilience and QoS in ICT Networks

ICT networks traditionally rely on QoS metrics to define SLAs [76]. These metrics consisting of delay, jitter, bandwidth, packet loss, bit error rate, and traffic load are performance measures that do not give a comprehensive view of network

state. Therefore, other complementary metrics are adopted in SLAs in order to better quantify the system state, namely availability metrics.

In the initial introduction of Quality of Resilience (QoR) in [77], QoS is divided into short-term quality parameters referred to by availability, and long-term quality parameters grouped under QoR. In other words, resilience is considered as an aspect of QoS, as latency or packet loss. However, QoR is presented in [78] as a concept-treating quality at different levels of the Open Systems Interconnection model (OSI-model), including the network level which corresponds to traditional QoS. Figure 1 shows how QoR extends QoS to include other types of quality: Quality of Experience (QoE), Quality of Delivery (QoD), and Quality of Protection (QoP). This is done by considering the additional metrics from each level. QoR is used as a transverse evaluation for all aforementioned qualities. This is done by considering the metrics that describe different resilience stages. From a high-level perspective, we can say that QoR is a shift from client-centric evaluation, conducted using QoS, toward a more general framework that includes the system potential in terms of resources, organizational processes, and humans.

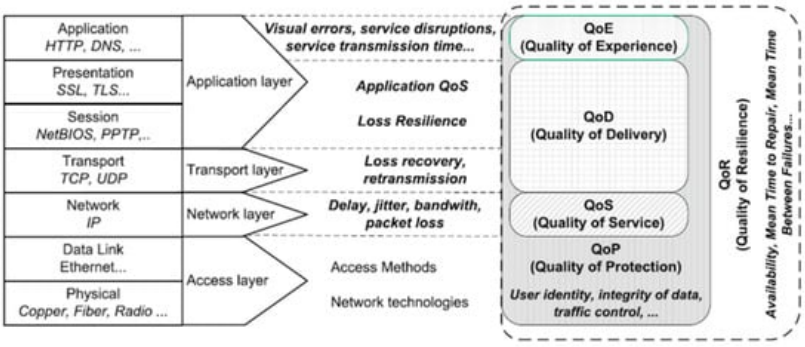


**Figure 1.** OSI-based classification of quality in relation with resilience [78].

Once again, in both cases above, the need for resilience stems from harsh large-scale events imposing consideration of stress in the system and recovery strategies. Then, despite the slight divergence in terminology that is still the case today, the two concepts go beyond the traditional QoS evaluation, to capture both requirements of customers and enhancement strategies of operators. Nevertheless, the idea that resilience takes in QoS is gaining more attention [75], suggesting that a system cannot be resilient if it does not offer acceptable QoS, but providing acceptable QoS is not the only requirement for a network to be resilient.

## 3. Taxonomy of Resilience Evaluation Methods

The panoply of methods proposed for qualitative evaluation of resilience in electric power networks [20][21][22][23][24][25] is not enough to convince critical infrastructure operators in general, and utilities in particular, to adopt the resilience-based design. They are unable to systematically discover hidden vulnerabilities and critical elements [79]. To overcome this, stakeholders need to have a closer, more tangible grasp of resilience, using quantitative analyses which gained huge momentum in recent years. Most of these analyses are performance-based, where performance is defined in various ways in order to fit different participants and study objectives [80]. The fact that almost all works selected in this paper happen to belong to this high-level method of quantification comes to stress the consensus in progress toward the adaptation of this method as a tool for resilience quantification.

In Figure 2, we propose four aspects based on which the state-of-the-art papers on resilience metrics for smart power distribution network could be classified, evaluated, and compared. Some of these aspects will be further elaborated in the later sections. For instance, in Section V we classify the papers based on extreme event handled, performance calculation method, and both type and computational method of resilience metrics. Each of these four aspects is explained in detail below.

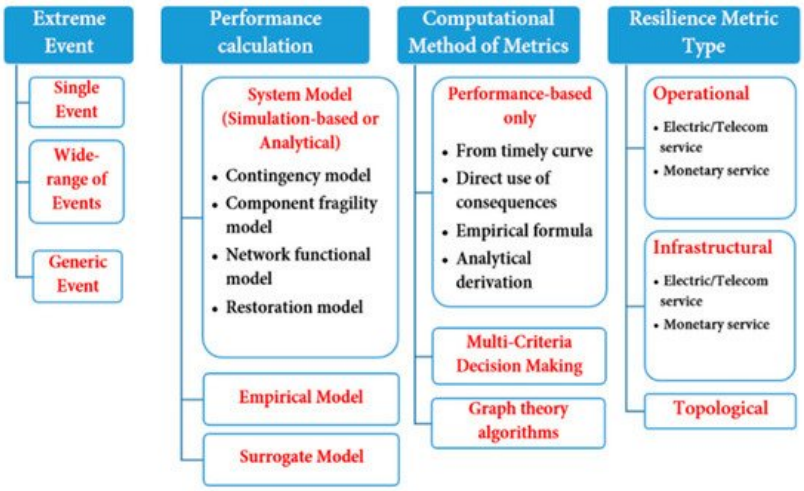


**Figure 2.** Proposed classification for resilience evaluation frameworks.

## 4. Resilience Quantification Objectives

Four broad classes of resilience metrics are generally adopted: (i) average performance metrics, (ii) integrated multi-phase metrics, (iii) time-dependent metrics, and (iv) probability-based metrics [81]. In the case of a HILP event, probability distributions are often not available, whereas the other three classes depend on the measure of performance in the network. Thus, a reasonable statement is that an ideal evaluation of resilience may consist of a complete tracking of the time-dependent performance function P(t). This way, network operators can have the value of performance at any instant for the complete event duration. However, despite the apparent dependence of P(t) in time, performance function does not necessarily change with time if it is not for the extreme event which hits the system. In other words, performance function depends on many parameters including hazard intensity, system preparedness, resilience strategies in hand, and priority decisions made, all of which cause network state to change. This sends back the problem of resilience multi-dimensionality, which makes developing closed form derivation for resilience function challenging and hitherto out of reach. Performance-based methods try to include all previously mentioned parameters and additional ones into a temporal curve describing the performance evolution of the network. It can be said that many resilience features are embedded in a performance curve as shown in Figure 3, because the construction of such a graph takes into consideration all factors intervening during a catastrophic contingency.


**Figure 3.** Performance curve for resilience quantification.

A salient advantage of such an approach is to have the temporal follow-up of network state which allows decision-makers to be in a best-informed posture. Four main phases can be distinguished, among which some can be further detailed into sub-phases:

- Anticipation phase (phase I): Represents the time period before the event occurrence, when performance is at its nominal level. Monitoring information, impact projections, and historical data when available are used for prediction studies, and all possible defensive measures are implemented. This serves particularly in the case of multi-hazard management where risks and vulnerabilities to each event are investigated. For single hazard resilience analysis which is the most relevant in the case of HILP event, this phase is not considered and a post-event resilience study is adopted. However, this also refers to the period of normal operation where reliability and risk management for recurrent failures can be conducted, which participates in system resilience, because a resilient system needs to be first as reliable and low-risk as possible. In addition, security measures for protecting the system and preparing it to withstand malicious behaviors are implemented at this stage [82].

- Mitigation phase (phase II): Once an extreme event hits the network, reliance is on system robustness, reactivity, and absorption to minimize the effect on services and infrastructure. Adding to some preparation policies that could be anticipated, many dynamic actions can be implemented to reduce the aftermath, like distribution automation actions, load shedding, and monitoring actions in power distribution networks or customer prioritization in telecom networks. These actions can withstand performance degradation that is in place, or serve to coordinate between entities in order to achieve an accurate assessment of consequences and prepare next crisis management steps.

- Recovery phase (phase III): Unlike short-timed low impact incidents where maintenance actions are achieved relatively fast, in major events, recovery actions can require anywhere between several weeks to months [83]. The main reason is that, given the safety of emergency crews and logistic constraints, restoration is conducted carefully and waits for the reduction in hazard intensity, or more generally identification of restoration windows. Priority is first given to service restoration where all alternative (even temporary) ways to provide services are explored and deployed allowing to regain an intermediate level of performance. Complete recovery will take more time and effort as it involves mostly infrastructure catering which turns out to be very challenging.

- Learning phase (phase IV): This phase is less considered than the two previous phases in quantitative resilience frameworks, generally with the argument that resilience is best examined in face of exogenous threats [84]. The post-recovery phase should still be looked at closely in order to draw conclusions about damages experienced by the network and how various implemented policies helped to alleviate consequences. Data collection through field surveys and supervisory management tools enable improvement in system performance and enhancement in preparation for upcoming extreme events backing the vision for a sustainable network.

Many works [13][27][45][63] explore each of these phases with slightly different denominations. Here a generalizing description is adopted where the four above-mentioned phases are considered, with mitigation and recovery divided each into two sub-phases in order to better explain all involved mechanisms. Resilience quantitative frameworks can be assessed based on phases they handle [64]. The more phases taken into consideration, the better the insight into system operation during extreme events. Furthermore, the layout can be used to seek answers for the following questions: When is resilience evaluation conducted and for which reason?

Figure 4 distinguishes time instants at which resilience quantification can be conducted, and objectives of this evaluation. The former here orients/guides/steers the latter, because for example, an operator who aims to plan investments for his network will most likely opt for pre-event evaluation, while another who only wants to see the impact induced by a contingency in his network may adopt post-recovery damage evaluation. Knowing “why” resilience is to be evaluated serves as a guideline to choose “when” it should be done. Without loss of generality, resilience evaluation can be induced from the performance curve in Figure 3; so it is important to know when system operators can get such a representation. Three options are available:

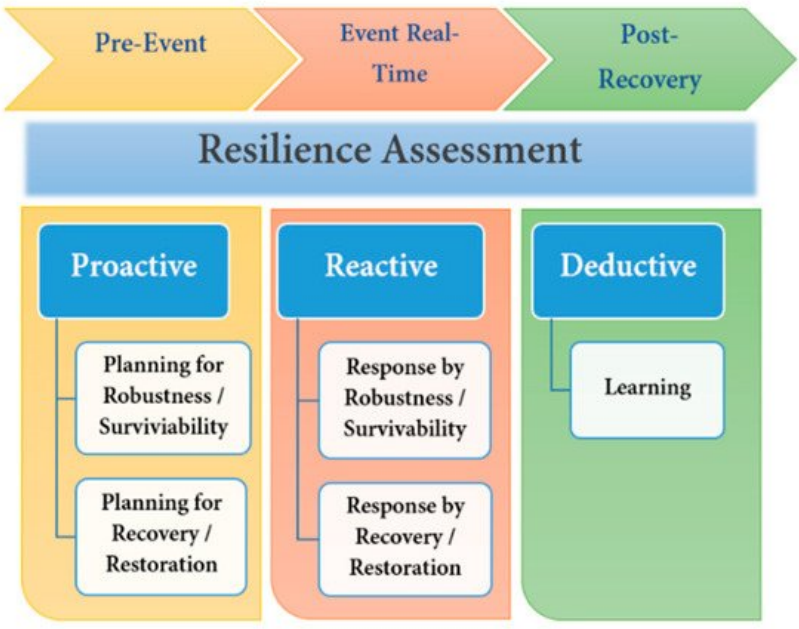


**Figure 4.** Options for resilience evaluation timing and associated objectives.

- Proactive evaluation: The procedure in this case is to drive pre-event studies with the goal of obtaining resilience indicators before contingency happens. The outbuilding is in prediction data, recommendations of experts, supervision alerts, and historical records. However, for HILP anomalies, little information is available, then designing preventive measures appeals for simulation tools, emulation, and analytical models which help to make projections for the impact that will be borne by the network in face of uncertain events.

Once metrics are computed, they can be used to make informed decisions about resilience strategies to implement in order to minimize the impact and speed up recovery. In other words, the output of this phase is planning schemes which enhance robustness, survivability, restoration, and recovery of the system that can be summarized in the concept of resilience. The prominent advantage of a proactive evaluation is the ability to look-forward that allows foreseeing what is coming. On the other hand, the large number of possible contingency scenarios and little relevant data cause low-confidence results.

- Reactive evaluation: Quantification is carried out as the event happens, meaning that resilience metrics are computed on-the-fly, and policies adopted to cope with severe hazards are taken from the inherent reaction capacity of the system without support from pre-event recommendations. Metrics are calculated as the event goes for the two broad phases of robustness and recovery. In such real-time setup, information that can be gathered is realistic and narrows down failure modes space. However, the flexibility margin can be very tight because the HILP event hits the network by surprise while no anticipative actions are in place. There are no good or bad choices between proactive and reactive evaluation, they are both suitable for resilience analysis and can be complementary. The goal is to find a balanced fit for a given use case [85].

- Deductive evaluation: When resilience metrics are computed at the end of a HILP disturbance, they mainly serve to draw conclusions about how the system handled an external event [86][87][88]. Results of this are intended to point out axes of improvement for future reference in similar extreme situations, and can also be considered as performance evolvement baseline. Further, the output of such post-recovery evaluation can be fed to the pre-event phase for hazards in the future, closing a kind of a cycle with the evaluations presented above.

Proactive approaches are dominant in resilience engineering, especially when considering the fact that in some cases the reactive approach is subsumed therein. The combination of the two is simply referred to as proactive approaches.

## References


1. Soldani, D.; Manzalini, A. Horizon 2020 and Beyond: On the 5G Operating System for a True Digital Society. IEEE Veh. Technol. Mag. 2015, 10, 32–42.
2. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Thi ngs. IEEE Access 2018, 6, 6900–6919.
3. O'Mahony, M.J.; Politi, C.; Klonidis, D.; Nejabati, R.; Simeonidou, D. Future Optical Networks. J. Light. Technol. 2006, 2 4, 4684–4696.
4. Galli, S.; Scaglione, A.; Wang, Z. For the Grid and Through the Grid: The Role of Power Line Communications in the S mart Grid. Proc. IEEE 2011, 99, 998–1027.
5. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid—The New and Improved Power Grid: A Survey. IEEE Commun. Sur v. Tutor. 2012, 14, 944–980.
6. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid Technologies: Communi cation Technologies and Standards. IEEE Trans. Ind. Inform. 2011, 7, 529–539.
7. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. A Survey on Smart Grid Potential A pplications and Communication Requirements. IEEE Trans. Ind. Inform. 2013, 9, 28–42.
8. Moslehi, K.; Kumar, R. A Reliability Perspective of the Smart Grid. IEEE Trans. Smart Grid 2010, 1, 57–64.
9. Momoh, J.A. Smart grid design for efficient and flexible power networks operation and control. In Proceedings of the 20 09 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–8.
10. The President's National Infrastructure Advisory Council. Surviving a Catastrophic Power Outage—How to Strengthen t he Capabilities of the Nation. Available online: (accessed on 7 December 2020).
11. U.S. Departement of Energy. Infrastructure Security and Energy Restoration. Hurricane Irma & Hurricane Harvey Event Summary (Report #28). September 2017. Available online: (accessed on 7 December 2020).

12. Román, M.O.; Stokes, E.C.; Shrestha, R.; Wang, Z.; Schultz, L.; Carlo, E.A.S.; Sun, Q.; Bell, J.; Molthan, A.; Kalb, V.; et al. Satellite-based assessment of electricity restoration efforts in Puerto Rico after Hurricane Maria. PLoS ONE 2019, 14, e0218883.
13. Panteli, M.; Mancarella, P. The Grid: Stronger, Bigger, Smarter? Presenting a Conceptual Framework of Power System Resilience. IEEE Power Energy Mag. 2015, 13, 58–66.
14. Bie, Z.; Lin, Y.; Li, G.; Li, F. Battling the Extreme: A Study on the Power System Resilience. Proc. IEEE 2017, 105, 1253–1266.
15. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. IEEE Trans. Power Syst. 2017, 32, 3317–3318.
16. Sullivan, J.E.; Kamensky, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. Electr. J. 2017, 30, 30–35.
17. The Smart Grid Implementation Strategy Team; National Energy Technology Laboratory. What is the Smart Grid? March 2009. Available online: (accessed on 7 December 2020).
18. Civil Contingencies, Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. October 2011. Available online: (accessed on 7 December 2020).
19. Obama, B.; Presidential Policy. Directive 21: Critical Infrastructure Security and Resilience. Homeland Security Digital Library. 12 February 2013. Available online: (accessed on 7 December 2020).
20. Cimellaro, G.P.; Reinhorn, A.M.; Bruneau, M. Seismic resilience of a hospital system. Struct. Infrastruct. Eng. 2010, 6, 127–144.
21. Ganin, A.A.; Massaro, E.; Gutfraind, A.; Steen, N.; Keisler, J.M.; Kott, A.; Mangoubi, R.; Linkov, I. Operational resilience: Concepts, design and analysis. Sci. Rep. 2016, 6, 19540.
22. Henry, D.; Ramirez-Marquez, J.E. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab. Eng. Syst. Saf. 2012, 99, 114–122.
23. Madni, A.M.; Jackson, S. Towards a Conceptual Framework for Resilience Engineering. IEEE Syst. J. 2009, 3, 181–191.
24. Panteli, M.; Mancarella, P. Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events. IEEE Syst. J. 2017, 11, 1733–1742.
25. Smith, P.; Hutchison, D.; Sterbenz, J.P.; Schöller, M.; Fessi, A.; Karaliopoulos, M.; Lac, C.; Plattner, B. Network resilience: A systematic approach. IEEE Commun. Mag. 2011, 49, 88–97.
26. Arghandeh, R.; von Meier, A.; Mehrmanesh, L.; Mili, L. On the definition of cyber-physical resilience in power systems. Renew. Sustain. Energy Rev. 2016, 58, 1060–1069.
27. Gholami, A.; Shekari, T.; Amirioun, M.H.; Aminifar, F.; Amini, M.H.; Sargolzaei, A. Toward a Consensus on the Definition and Taxonomy of Power System Resilience. IEEE Access 2018, 6, 32035–32053.
28. Wang, Y.; Chen, C.; Wang, J.; Baldick, R. Research on Resilience of Power Systems under Natural Disasters—A Review. IEEE Trans. Power Syst. 2015, 31, 1604–1613.
29. Espinoza, S.; Panteli, M.; Mancarella, P.; Rudnick, H. Multi-phase assessment and adaptation of power systems resilience to natural hazards. Electr. Power Syst. Res. 2016, 136, 352–361.
30. Li, Z.; Shahidehpour, M.; Aminifar, F.; AlAbdulwahab, A.; Al-Turki, Y. Networked Microgrids for Enhancing the Power System Resilience. Proc. IEEE 2017, 105, 1289–1310.
31. Reed, D.A.; Kapur, K.C.; Christie, R.D. Methodology for Assessing the Resilience of Networked Infrastructure. IEEE Syst. J. 2009, 3, 174–180.
32. Zhao, X.; Chen, Z.; Gong, H. Effects Comparison of Different Resilience Enhancing Strategies for Municipal Water Distribution Network: A Multidimensional Approach. Math. Probl. Eng. 2015, 2015, 1–16.
33. Cutter, S.L. The landscape of disaster resilience indicators in the USA. Nat. Hazards 2016, 80, 741–758.
34. Dessavre, D.G.; Ramirez-Marquez, J.E.; Barker, K. Multidimensional approach to complex system resilience analysis. Reliab. Eng. Syst. Saf. 2016, 149, 34–43.
35. Ouyang, M.; Dueñas-Osorio, L. Multi-dimensional hurricane resilience assessment of electric power systems. Struct. Saf. 2014, 48, 15–24.
36. Mahzarnia, M.; Moghaddam, M.P.; Baboli, P.T.; Siano, P. A Review of the Measures to Enhance Power Systems Resilience. IEEE Syst. J. 2020, 14, 4059–4070.

37. Kontokosta, C.E.; Malik, A. The Resilience to Emergencies and Disasters Index: Applying big data to benchmark and v alidate neighborhood resilience capacity. Sustain. Cities Soc. 2018, 36, 272–285.

38. Chang, S.E.; Shinozuka, M. Measuring Improvements in the Disaster Resilience of Communities. Earthq. Spectra 200 4, 20, 739–755.

39. Fang, Y.-P.; Pedroni, N.; Zio, E. Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. IEEE Trans. Reliab. 2016, 65, 502–512.

40. Albasrawi, M.N.; Jarus, N.; Joshi, K.A.; Sarvestani, S.S. Analysis of reliability and resilience for smart grids. In Proceedi ngs of the 2014 IEEE 38th Annual International Computer Software and Applications Conference, Vasteras, Sweden, 2 1–25 July 2014.

41. Panteli, M.; Mancarella, P.; Trakas, D.N.; Kyriakides, E.; Hatziargyriou, N.D. Metrics and Quantification of Operational a nd Infrastructure Resilience in Power Systems. IEEE Trans. Power Syst. 2017, 32, 4732–4742.

42. Dehghanian, P.; Aslan, S.; Dehghanian, P. Maintaining Electric System Safety through an Enhanced Network Resilienc e. IEEE Trans. Ind. Appl. 2018, 54, 4927–4937.

43. Fang, Y.; Sansavini, G. Optimizing power system investments and resilience against attacks. Reliab. Eng. Syst. Saf. 20 17, 159, 161–173.

44. Jufri, F.H.; Widiputra, V.; Jung, J. State-of-the-art review on power grid resilience to extreme weather events: Definition s, frameworks, quantitative assessment methodologies, and enhancement strategies. Appl. Energy 2019, 239, 1049–1 065.

45. Das, L.; Munikoti, S.; Natarajan, B.; Srinivasan, B. Measuring smart grid resilience: Methods, challenges and opportunit ies. Renew. Sustain. Energy Rev. 2020, 130, 109918.

46. Farhangi, H. The path of the smart grid. IEEE Power Energy Mag. 2010, 8, 18–28.

47. Ipakchi, A.; Albuyeh, F. Grid of the future. IEEE Power Energy Mag. 2009, 7, 52–62.

48. Beaty, H.W. Electric Power Distribution Systems: A Nontechnical Guide; PennWell Books: Tulsa, OK, USA, 1998.

49. Heydt, G.T. The Next Generation of Power Distribution Systems. IEEE Trans. Smart Grid 2010, 1, 225–235.

50. Brown, R.E. Impact of Smart Grid on distribution system design. In Proceedings of the 2008 IEEE Power and Energy S ociety General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–4.

51. Amin, S.M.; Wollenberg, B. Toward a smart grid: Power delivery for the 21st century. IEEE Power Energy Mag. 2005, 3, 34–41.

52. Ma, S.; Chen, B.; Wang, Z. Resilience Enhancement Strategy for Distribution Systems under Extreme Weather Events. IEEE Trans. Smart Grid 2018, 9, 1442–1451.

53. Bertsimas, D.; Litvinov, E.; Sun, X.A.; Zhao, J.; Zheng, T. Adaptive Robust Optimization for the Security Constrained Un it Commitment Problem. IEEE Trans. Power Syst. 2013, 28, 52–63.

54. Soroudi, A.; Ehsan, M. IGDT Based Robust Decision Making Tool for DNOs in Load Procurement Under Severe Uncert ainty. IEEE Trans. Smart Grid 2012, 4, 886–895.

55. Chen, P.-Y.; Cheng, S.-M.; Chen, K.-C. Smart attacks in smart grid communication networks. IEEE Commun. Mag. 201 2, 50, 24–29.

56. Chai, W.K.; Kyritsis, V.; Katsaros, K.V.; Pavlou, G. Resilience of interdependent communication and power distribution networks against cascading failures. In Proceedings of the 2016 IFIP Networking Conference (IFIP Networking) and W orkshops, Vienna, Austria, 17–19 May 2016; pp. 37–45.

57. Zio, E.; Sansavini, G. Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. IEE E Trans. Reliab. 2011, 60, 94–101.

58. Kwasinski, A. Effects of Notable Natural Disasters of 2017 on Information and Communication Networks Infrastructure. In Proceedings of the 2018 IEEE International Telecommunications Energy Conference (INTELEC), Torino, Italy, 7–11 October 2018; pp. 1–8.

59. Martins, D.L.; Girão-Silva, R.; Gomes, Á.; Jorge, L.M.G.; Musumeci, D.F.; Rak, D.J. Interdependence between Power G rids and Communication Networks: A Resilience Perspective. In Proceedings of the DRCN 2017—Design of Reliable C ommunication Networks, 13th International Conference, Munich, Germany, 8–10 March 2017; p. 9.

60. Yang, Z.; Chen, Y.; Marti, J. Modelling cascading failure of a CPS for topological resilience enhancement. IET Smart Gri d 2020, 3, 207–215.

61. Liu, X.; Chen, B.; Chen, C.; Jin, D. Electric power grid resilience with interdependencies between power and communic ation networks—A review. IET Smart Grid 2020, 3, 182–193.

62. Ji, C.; Wei, Y.; Poor, H.V. Resilience of Energy Infrastructure and Services: Modeling, Data Analytics, and Metrics. Proc. IEEE 2017.

63. Kandaperumal, G.; Srivastava, A.K. Resilience of the electric distribution systems: Concepts, classification, assessmen t, challenges, and research needs. IET Smart Grid 2020, 3, 133–143.

64. Chi, Y.; Xu, Y.; Hu, C.; Feng, S. A State-of-the-Art Literature Survey of Power Distribution System Resilience Assessme nt. In Proceedings of the 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, USA, 5–9 Aug ust 2018; pp. 1–5.

65. Chi, Y.; Xu, Y. Resilience-oriented microgrids: A comprehensive literature review. In Proceedings of the 2017 IEEE Inno vative Smart Grid Technologies—Asia (ISGT-Asia), Auckland, New Zealand, 4–7 December 2017; pp. 1–6.

66. Kafka, P. Reliability and Safety. CERN. February 2002. Available online: (accessed on 13 December 2020).

67. Grid Modernization Laboratory Consortium. Grid Modernization: Metrics Analysis (GMLC1.1)—Resilience. April. Availab le online: (accessed on 13 December 2020).

68. IEEE Guide for Electric Power Distribution Reliability Indices. In IEEE Std 1366–2003 (Revision of IEEE Std 1366–199 8); Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2008; pp. 1–50.

69. Billinton, R.; Allan, R.N. Distribution systems—Basic techniques and radial networks. In Reliability Evaluation of Power Systems; Springer US: Boston, MA, USA, 1996; pp. 220–248.

70. IEEE. IEEE Draft Guide for Electric Power Distribution Reliability Indices; IEEE P1366/D6; November 2011; IEEE: Pisc ataway, NJ, USA, 2011; pp. 1–40.

71. Reed, D.A. Electric utility distribution analysis for extreme winds. J. Wind. Eng. Ind. Aerodyn. 2008, 96, 123–140.

72. Council, N.R. Disaster Resilience: A National Imperative; The National Academies Press: Washington, DC, USA, 2012.

73. Elliot, R.; National Rural Elec Association; Organization of MISO States; Aaronson, S.; Edison Electric Institute; Nationa l Associatio Advocates. Utility Investments in Resilience of Electricity Systems. 2019. Available online: (accessed on 13 December 2020).

74. DeMartini, P. Integrated, Resilient Distribution Planning. May 2020. Available online: (accessed on 13 December 2020).

75. European Network and Information Security Agency (ENISA). Enabling and Managing End-to-End Resilience. Report/S tudy. Available online: (accessed on 13 December 2020).

76. Chana, I.; Gill, S.S. Quality of Service and Service Level Agreements for Cloud Environments: Issues and Challenges. I n Cloud Computing. Computer Communications and Networks; Springer: Cham, Switzerland, 2014; pp. 51–72.

77. Tapolcai, J.; Cholda, P.; Cinkler, T.; Wajda, K.O.; Jajszczyk, A.; Verchere, D. Joint Quantification of Resilience and Quali ty of Service. In Proceedings of the 2006 IEEE International Conference on Communications, Istanbul, Turkey, 11–15 J une 2006; Volume 2, pp. 477–482.

78. Rak, J.; Hutchison, D. (Eds.) Guide to Disaster-Resilient Communication Networks; Springer International Publishing: N ew York, NY, USA, 2020.

79. Eusgeld, I.; Henzi, D.; Kröger, W. Comparative Evaluation of Modeling and Simulation Techniques for Interdependent C ritical Infrastructures; Laboratorium für Sicherheitsanalytik, ETH: Zürich, Switzerland, 2008.

80. Vugrin, E.D.; Castillo, A.R.; Silva-Monroy, C.A. Resilience Metrics for the Electric Power System: A Performance-Based Approach; SAND2017-1493, 1367499; Sandia National Lab. (SNL-NM): Albuquerque, NM, USA, 2017.

81. Rodriguez, D.R. Physical and Social Systems Resilience Assessment and Optimization. Ph.D. Thesis, University of So uth Florida, Tampa, FL, USA, 2018.

82. European Commission; Joint Research Centre. Institute for the Protection and the Security of the Citizen. In Risk Asses sment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art; Publications Office of the European Union, Grand Duchy of Luxembourg: Luxembourg, 2012.

83. Kwasinski, A. Effects of Hurricane Maria on Renewable Energy Systems in Puerto Rico. In Proceedings of the 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA), Paris, France, 14–17 October 2 018; pp. 383–390.

84. Huang, G.; Wang, J.; Chen, C.; Guo, C.; Zhu, B. System resilience enhancement: Smart grid and beyond. Front. Eng. Manag. 2017, 4, 271–282.

85. Jackson, S.; Ferris, T. Proactive and Reactive Resilience: A Comparison of Perspectives. INCOSE Insight 2015, 18, 7.

86. Zobel, C.W.; Khansa, L. Characterizing multi-event disaster resilience. Comput. Oper. Res. 2014, 42, 83–94.
87. Maliszewski, P.J.; Perrings, C. Factors in the resilience of electrical power distribution infrastructures. Appl. Geogr. 2012, 32, 668–679.
88. Kelly-Gorham, M.R.; Hines, P.; Dobson, I. Using historical utility outage data to compute overall transmission grid resilience. arXiv 2019, arXiv:1906.06811.