Understanding Cyber-physical Resilience From A Power System Perspective

Nancy Mohamed
Electrical and Computer Engineering Department
University of Waterloo
Waterloo, ON, Canada
nancy.mohamed@uwaterloo.ca

Magdy M. A. Salama
Electrical and Computer Engineering Department
University of Waterloo
Waterloo, ON, Canada
msalama@uwaterloo.ca

***Abstract*—Resilience, as a concept, has been recently become a strategic objective for power grids. However, there are still some conceptual unclarities. Resilience is often mistakenly used as a synonym for reliability. A power system can be reliable but not resilient. This paper clarifies this misconception. It discusses resilience definitions, cycle, and states to better understand resilience aspects. It also discusses power grids' new vulnerabilities and sheds the light on both cyber-physical resilience and cyber contingency concepts. Finally, it reviews the strategies used to enhance grid resilience.**

Keywords—Resilience, Cyber-physical Vulnerability, Cyber Contingency, Grid hardening, Reliability, Microgrid, Reconfiguration.

I. Introduction

Lately, the concept of resilience has been introduced into power grids to handle the low probability high impacts events. Those events comprise natural disasters, cyber and physical attacks (including human errors). They are not common but can lead to devastating damage in power grids when they occur. Power grids are vulnerable to several natural phenomena such as, hurricanes, earthquakes, storms, and extreme temperatures. Due to global climate change, several weather events have increased in frequency and severity [1]. According to National Oceanic and Atmospheric Administration (NOAA) [2], the average number of storms the Atlantic produced per year, between 1975-1994, increased 67% in the period between 1995-2012. Moreover, the average annual number of severe hurricanes is more than doubled during the same period. Such extreme weather events cause large-scale power outages and lead to extensive damage in the grid. During the period 1985-2012, the climate change impacts had affected more than 50,000 customers. Therefore, extreme weather events are considered one of the most serious threats to the energy system.

The need for communication technologies to help monitor and collect data from all over the smart grid puts the grid at risk of cyber and cyber-physical attacks in addition to the existing physical vulnerabilities. The associated risks are due to many reasons including the following:

- The use of new technologies adds up to grid complexity and introduces new vulnerabilities, thus increasing exposure to potential attackers.
- Potential adversaries rise with the growing number of communication paths and entry points.
- Interconnected systems require large amounts of transferred data and private information to be exchanged, jeopardizing the safety of vital aggregated data.
- Excessive amounts of data that will be collected can lead to compromising data confidentiality, including breaches of customer privacy.

The growing risks of the aforementioned natural disasters and physical and/or cyber attack events are becoming more challenging, especially because those events have different sources of disruptions, thus are hard to expect and enumerate. Thus, nowadays, grid planners and operators need to figure out how to make the system be able to absorb those shocks as they unfold and keep working instead of trying to prevent against every single disruption. That's why power systems need to be more resilient.

The rest of this paper is organized as follows. Section II reviews the resilience definitions in multiple contexts. Section III explains the resilience cycle. Section IV discusses different resilience states and factors affects each state. Section V clarifies the misconception on resilience and reliability. Section VI discusses the physical and cyber vulnerabilities of the grid. In Section VII, grid cyber-physical resilience and cyber contingency are discussed. Section VIII argues the existing techniques to enhance power system resilience. Finally, Section IX concludes the paper.

II. Resilience Definitions

Although much research into grid resilience has been done over the past decades and is currently ongoing, resilience definitions are still too imprecise. Several definitions have been proposed in different disciplines. Back in 1973, in Ecology, resilience was defined as "a measure of the ability of systems to absorb changes and disturbance and still maintain the same relationships between populations or state variables"[3]. In [4], Bruneau et al. defined community seismic resilience as "the ability of social units to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes". They proposed a resilience framework comprises four interrelated dimensions: technical, organizational, social, and economic. In economic systems, resilience is "the ability of the system to withstand either market or environmental shocks without losing the capacity to allocate resources efficiently" [5]. In social systems, it is "the

978-1-7281-5442-8/20/$31.00 ©2020 IEEE

ability of groups or communities to cope with external stresses and disturbances as a result of social, political and environmental change" [6].

According to the National Infrastructure Protection Plan (NIPP) [7], a document developed by the U.S. Department of Homeland Security , resilience is defined as "the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident". The National Academy of Sciences (NAS) defined Disaster Resilience as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [8]. One salient features of this definition is its ability captures the temporal dimensions of resilience as will be discussed in Section IV. Since modern power grids are classified as a critical cyber-physical infrastructure, according to the National Infrastructure Advisory Council, grid resilience can be defined as "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" [9].

III. Resilience Cycle

As mentioned, the resilience specifically handles high-consequence, low-probability events. Indeed, the key to understanding resilience is realizing that disruptions cannot be prevented; instead, we can 1) prepare and plan for, 2) ride through, 3) recover from an event, and 4) observe and learn during this process. Therefore, this process involves four fundamental concepts, as illustrated in Fig. 1 [10], [11]. These concepts form the resilience cycle, as proposed by the National Infrastructure Advisory Council. The incident-focused stage can be seen as three steps reflecting measures taken prior to, during, and after a disruptive event. The post-incident stage focuses on the learning process by modifying plans and revising procedures and measures.

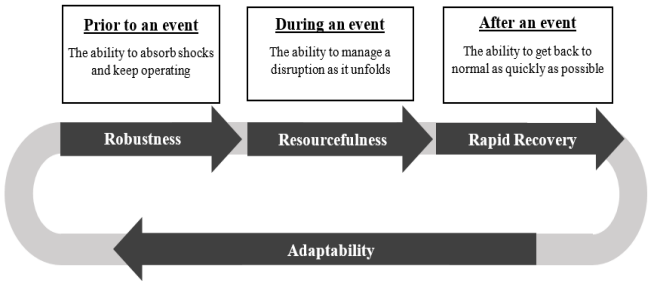

Fig. 1. Resilience Cycle

IV. Resilience States

Based on the resilience cycle, the system performance against a disruptive event can be represented by five states (phases) [12], [13], represented by a multi-phase resilience trapezoid as shown in Fig. 2.

A. Pre-disturbance State ($t_0 \leq t < t_{es}$)

Before the occurrence of a disruptive event, the system operates in a normal state as expected. During this state, system operators should define hazards and system vulnerabilities. They should also identify critical assets and plan for predictive actions.

B. Disruption State ($t_{es} \leq t < t_{ee}$)

At an instance t_{es}, a disruptive event hits the system, and degrades its performance from R_0 to R_d due to the failure of one or multiple system components. The final value of the resilience indicator, R_d, depends on several aspects such as, disruptive event type and severity, and network topology and robustness.

C. Degraded State ($t_{ee} \leq t < t_{rs}$)

This state starts at the end of the disruptive event and ends at the start of the repair (recovery). Thanks to the integration of cyber systems in modern power grids, updated status of system components can be collected. Hereafter, damage assessment can be conducted for the purpose of taking appropriate corrective actions. The length of this state depends on several aspects including, resources and analysis tools in hand, operational flexibility, operator's training, etc.

D. Recovery State ($t_{rs} \leq t < t_{re}$)

This state is concerned with recovering the system as fast as possible. The recovery duration is affected by several aspects including, the damage caused, the amount of resources (material and human) available, the amount of high-priority loads existing, and the accessibility to the affected zones.

E. Post-disturbance State (Adaptation) ($t \geq t_{re}$)

This is a learning state where what happened during previous states should be analyzed and then assessed. Thanks to such analyses, development of the existing plans and standards are carried out in order to enhance the system to sustain future similar events. One revision example is revising federal emergency management plan after Hurricane Katrina [14], another example is when industry standards were revised after 2003 blackout [15].

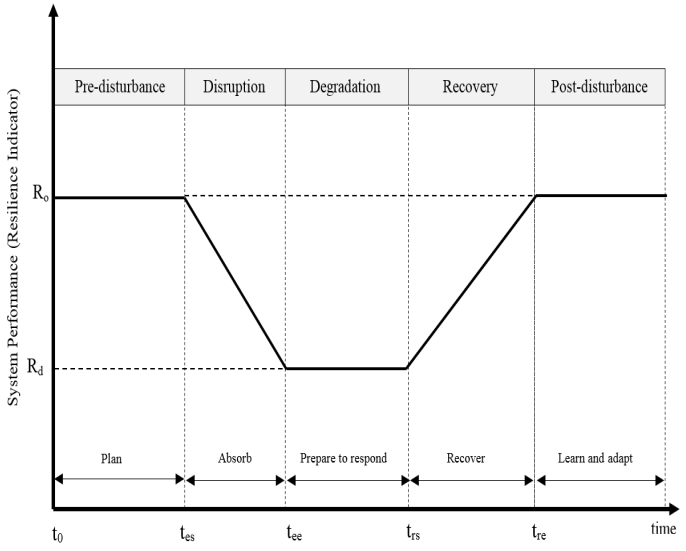

Fig. 2. Resilience States

V. Power System Reliability Vs. ResiliencE

Power systems reliability is a well-established concept. It is defined as "A measure of the ability of a system to deliver power to all points of utilization within acceptable standards and in amounts desired"[16]. Grid Reliability features adequacy and the security. Adequacy refers to the ability of the grid to supply the load, while Security denotes the system ability to survive sudden disturbances such as electric short circuits or unexpected losses of system components. Power grids are designed to sustain such typical outages.

Those typical power outages that reliability is concerned with are classified as high probability, low impact events such as line faults, device failure, insulation failure, etc. On the other hand, resilience is concerned with extreme events with low probability but high impacts such as, natural disasters, cyber-physical attacks, and human errors [17]. Such kind of events is less predictable and less controllable. They can cause multiple system components to fail, affecting large geographic regions in opposed to typical outages. In addition, because system is designed to meet N-1 criterion, single outages leaves the network intact in opposed to extreme events which cause multiple faults probably in multiple locations and hence need lots of resources and longer time to recover. Therefore, a power system can be reliable but not resilient to such extreme events.

Unlike resilience, reliability analysis does not encompass the adaptation phase, which helps enhance the infrastructural and operational resilience, as discussed in Section IV. For example, the reliability-oriented studies does not identify the extra resources and costs required to reduce outage consequences [18].

VI. Cyber and physical vulnerabilities of power grids

Power grids contain huge amounts of elements which are highly dispersed over the system, hence vulnerable to physical attacks. In addition to the existing physical vulnerability, cyber-physical attacks have become a potential threat to the grid. This section discusses those different kinds of power grid vulnerabilities.

A. Physical Vulnerabilities

Physical threats can target different elements of power grids such as, distribution and transmission lines, transformers, generators, sensors, actuators, etc. Physical security can be defined as the measures which prevent an attacker from getting an unauthorized physical access to facilities, equipment, or resources and damage them, e.g., theft and espionage[19]. Power utilities are working hard to protect their facilities from physical attacks through applying appropriate access control practices such as, CCTV surveillance and protective barriers.

B. Cyber Vulnerability

The need for communication technologies to help monitor and collect data from all over the smart grid puts the grid at risk of new vulnerabilities, i.e. cyber vulnerabilities. Cybersecurity denotes the information technology (IT) security, and it refers to the techniques used to protect data and cyber network assets from damage or unauthorized access. Confidentiality, integrity, and availability, known as CIA triad, are the three components of information security model [20]. Attacks are generally classified into two categories: passive attacks and active attacks [21]. Passive attacks are limited to eavesdropping and monitoring communication channels. In other words, the attacker does not aim at modifying any transmitted information. Instead, the main objective is the disclosure of confidential information, i.e. privacy attacks. However, the attacker can make use of that information in order to prepare for an active attack. On the other hand, in active attacks, an adversary tries to modify the content of the original message in some way. There are four different types of active attacks, namely denial of service (DoS), modification, replay, and fabrication attacks.

C. Cyber-physical Vulnerability

The integration of the cyber layer into power grids makes it easy to cause physical damage to grid elements through cyber attacks. Hence, Cyber-physical attacks (also known as cyber-enabled physical attacks [22]) are a kind of cyber attacks which adversely affect the physical components of power grids, whether intentionally or not [23].

VII. Grid Cyber-physical Resilience

To meet the smart grid requirements for a smarter and more reliable power grid, power grids have become more dependent on cyber infrastructure. In turn, power grids are now vulnerable to cyber-physical attacks, as mentioned in Section VI. Although those attacks are classified as low probability events, they, when occur, have such serious impacts on the network and can lead to massive blackouts. One example is the Ukraine power grid attack incident occurred in December 2015 [24], wherein malicious commands were sent to trip the critical lines in the regional grid through switching off 30 substations. This attack caused a widespread power outage that had affected 225,000 customers. Furthermore, denial-of-service attack on call-center was launched in order to deny customers information on the blackout and delay the restoration process. Such attack is classified as coordinated attack, i.e., attacks in which various commands are employed and various components are targeted. Therefore, N-1 criterion can no longer satisfy the new requirements of modern power grids. Hence, for contingency analysis, there is a need for a more comprehensive framework takes into account cyber contingencies along with the physical ones [25]. First, a set of combinations of system components, that can be compromised, should be obtained. Within this extremely large solution space, elimination methods based on power flow are used to assess each combination. Combinations which result in worst-case scenarios will be only considered, while the rest will be discarded.

VIII. Grid Resilience enhancement

There are two strategies proposed in the literature to enhance grid resilience: grid hardening and smart operational measures. The following subsections review and assess the methods used.

A. Grid Hardening

Grid hardening is the physical reinforcement of the system infrastructure in order to improve its ability to sustain the impacts of disruptive events, enhancing the infrastructural resilience. The following are examples of hardening-related measures:

Vegetation management [26]–[28]: During severe weather conditions, falling trees and branches result in excessive damage to power lines. Vegetation management includes two activities. The first is tree trimming and removal programs, which target all trees and bushes within a specified distance from conductors. The second is tree-growth regulators (TGRs). TGRs are chemicals that are injected into trees to control their growth. Since those activities are costly, optimal vegetation maintenance scheduling are done taking into account tree growth, weather studies, and crew availability.

Undergrounding [29]: The conversion of overhead lines to underground in order to lower damage and restoration during storm events. It also helps lower tree trimming cost. However, this conversion must be planned carefully because of the high initial and maintenance expenses. Another disadvantage is that it is susceptible to flooding and storm surges.

Besides vegetation management and undergrounding, there are other hardening strategies suggested such as, upgrading utility poles and adding guy wires [26], [30], elevating substations and control rooms to protect against flooding [30], and redundant transmission routes [31].

B. Smart operational measures

Smart operational measures denote the adaptive control strategies which can boost system performance in face of disruptive events. Smart operational measures are more affordable than hardening measures, yet they might not be as effective [32]. Examples of operational-oriented measures are: microgrids [33], optimal reconfiguration and DG islanding[31], adaptive protection and control systems [17], leveraging distributed energy resources [34].

IX. Conclusion

The devastating impacts of latest high-impact low-probability events are a motive for making power systems more resilient. In the light of this motivation, the differences between resilience and reliability were made clear. Cyber-physical resilience was discussed shedding the light on the concept of cyber contingency and how to incorporate it to grid contingency analysis. Different strategies for enhancing power grid resilience were discussed from a practical perspective.

References

[1] Q. E. R. Report, E. Transmission, and D. Infrastructure, "Chapter II INCREASING THE RESILIENCE , RELIABILITY , SAFETY , AND ASSET SECURITY OF TS & D," no. April, 2015.

[2] Maryland Energy Administration, "Resiliency through Microgrids Task Force Established," 2014.

[3] C. S. Holling, "Resilience and Stability of Ecological Systems," *Annu. Rev. Ecol. Syst.*, vol. 4, no. 1, pp. 1–23, Nov. 1973.

[4] 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, Nov-2003.

[5] C. Perrings, "Resilience and sustainable development," *Environ. Dev. Econ.*, vol. 11, no. 4, pp. 417–427, 2006.

[6] W. N. Adger, "Social and ecological resilience: Are they related?," *Prog. Hum. Geogr.*, vol. 24, no. 3, pp. 347–364, 2000.

[7] NIPP DHS, "National Infrastructure Protection Plan - DHS," *Dhs*, pp. 1–57, 2013.

[8] S. L. Cutter et al., "Disaster resilience: A national imperative", *Environ. Sci. Policy Sustain. Develop.*, vol. 55, no. 2, pp. 25-29, 2013.

[9] A. R. Berkeley Iii, M. Wallace, and NIAC, "A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations," *Final Rep. Recomm. by Counc.*, pp. 1–73, 2010.

[10] "Expert Meeting - Improving Power System Resilience in the 21st Century." [Online]. Available: https://sites.nationalacademies.org/PGA/ResilientAmerica/PGA_146736. [Accessed: 07-Jan-2020].

[11] Y. Lin, Z. Bie, and A. Qiu, "A review of key strategies in realizing power system resilience," *Glob. Energy Interconnect.*, vol. 1, no. 1, pp. 70–78, 2018.

[12] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," *IEEE Trans. Power Syst.*, vol. 32, no. 6, pp. 4732–4742, Nov. 2017.

[13] P. Dehghanian, S. Aslan, and P. Dehghanian, "Maintaining Electric System Safety Through An Enhanced Network Resilience," *IEEE Trans. Ind. Appl.*, vol. 54, no. 5, pp. 4927–4937, 2018.

[14] Keith Bea et al., Federal Emergency Management Policy Changes after Hurricane Katrina: A Summary of Statutory Provisions, RL33279, Washington, D.C.: Congressional Research Service, December 15, 2006.

[15] N. Scotia, "After the Blackout: Implementation of Mandatory Electric Reliability Standards in Canada Energy and Mines Ministers' Conference," 2015.

[16] A Akhikpemelo, N. Eyibo, and A. Adeyi, "Reliability Analysis of Power Distribution Network," *Cont. J. Eng. Sci.*, vol. 11, no. 2, pp. 53–63, 2016.

[17] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies," *Proc. IEEE*, vol. 105, no. 7, pp. 1202–1213, 2017.

[18] E. Vugrin, A. Castillo, and C. Silva-monroy, "Resilience Metrics for the Electric Power System : A Performance-Based Approach,"., p. 49, 2017.

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

[20] Y. S. Feruza, and T.-H. Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," Int. J. of Multimedia and Ubiquitous Engg. Vol. 2, No. 2, April, 2007.

[21] W. Stallings, 'Cryptography and Network Security (4th Edition)', 4th Edition, Prentice Hall; Nov. 26, 2005.

[22] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, 2005.

[23] G. Loukas, *Cyber-Physical Attacks: A Growing Invisible Threat*. 2015.

[24] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[25] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-Based Contingency Analysis," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3040–3050, Jul. 2016.

[26] A. Lippert, "Hardening and Resiliency," no. August, pp. 1–71, 2010.

[27] P. Zahodiakin, "Making distribution grids stronger, more resilient," *EPRI J.*, no. 4, pp. 4–8, 2016.

[28] P. A. Kuntz, R. D. Christie, and S. S. Venkata, "Optimal vegetation maintenance scheduling of overhead electric power distribution systems," *IEEE Trans. Power Deliv.*, vol. 17, no. 4, pp. 1164–1169, 2002.

[29] R. Brown, "Literature Review and Analysis of Electric Distribution Overhead to Underground Conversion," *Undergrounding Assess. phase 1 Final Rep.*, vol. 1019, no. V, pp. 1–59, 2007.

[30] A. R. Berkeley Iii, M. Wallace, and NIAC, "A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations," *Final Rep. Recomm. by Counc.*, pp. 1–73, 2010.

[31] Y. Lin and Z. Bie, "Tri-level optimal hardening plan for a resilient

distribution system considering reconfiguration and DG islanding," *Appl. Energy*, vol. 210, pp. 1266–1279, 2018.

[32] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018.

[33] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Bie, "Microgrids for Enhancing the Power Grid Resilience in Extreme Conditions," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 589–597, Mar. 2017.

[34] R. Arghandeh *et al.*, "The local team: Leveraging distributed resources to improve resilience," *IEEE Power Energy Mag.*, vol. 12, no. 5, pp. 76–83, 2014.