Open Access

Journal of Energy and Power Technology

LIDSEN Publishing Inc.

Original Research

Probabilistic Modeling of Cyber-Physical Microgrid Systems to Evaluate the Reliability and Resiliency Implications of Cyber Attacks

Rajesh Karki [1, *], Binamra Adhikari [2]

1. Professor, Dept. of Electrical & Computer Engineering, University of Saskatchewan, Canada; E-Mail: rajesh.karki@usask.ca
2. University of Saskatchewan, Saskatoon, Saskatchewan, Canada; E-Mail: binamra.adhikari@usask.ca

* **Correspondence:** Rajesh Karki; E-Mail: rajesh.karki@usask.ca

Academic Editors: Daming Zhang, Farhad Shahnia and Li Li

Special Issue: Design and Operation of Microgrids

Journal of Energy and Power Technology
2024, volume 6, issue 3
doi:10.21926/jept.2403015

Received: April 02, 2024
Accepted: August 04, 2024
Published: August 07, 2024

Abstract

The integration of cyber and physical layer of the grid has not only introduced a microscopic spectacle to observe and ensure the efficient flow of electricity but has also exposed the interdependencies of the network. These cyber-physical interdependencies are often exploited in the form of cyber-attacks that can disable a grid introducing substantial financial losses and observable social repercussions. Thus, it is important to address the impending Achilles heel by devising pragmatic approaches to comprehensibly upgrade the grid preventing huge financial and societal repercussions. In this regard, this paper proposes important methodologies in assessing the resiliency of a smart microgrid enabled distribution system in case of a cyber-attack and also steers discussion towards mitigation strategies and their influence in increasing the reliability and resiliency of the system. While doing so, it also aims to clarify the different principles of reliability and resiliency assessment. The paper describes an efficient bad-data detection strategy and its necessity in improving the reliability and resiliency of the system. The paper finds that a precipitous drop in reliability and resiliency is observed which can be effectively mitigated by the deployment of bad-data detection strategies and proposes efficient resiliency assessment methodologies to conduct similar studies.

Keywords

Reliability; resiliency; cyber-physical system; microgrid; data-injection attacks; situational awareness; cybersecurity

1. Introduction

As the use of Distributed Energy Resources (DER) has grown in recent decades, the centralized, bulky power system network has evolved into a more decentralized and dispersed network structure [1]. The integration of renewable resources such as photovoltaic (PV) sources, wind turbines, and energy storage systems (ESS), etc. has increased the need for advanced control mechanisms [2, 3]. This shift of power systems to smart grid technology has increased the deployment of information and communication technologies (ICT) for monitoring, controlling, and operating power networks [4]. The conventional power system has now switched to a cyber-physical system. Although these modern technologies have facilitated the remote controlling and effortless operation of the power network, it has increased the vulnerability of power systems to malicious cyber -attacks.

The power systems which were traditionally physical-only systems were already vulnerable to high impact low probability (HILP) natural disasters such as hurricanes, windstorms, earthquakes, etc. In the past few years, different cyber-related attacks have also been reported. Cyber intruders used spear-phishing to target various parts of Ukraine's power grid in December 2015. Hackers targeted more than 50 substations, knocking out electricity for more than 6 hours for nearly 225,000 customers and 130 MW of load [5]. A year later, another cyber-attack was reported in Kiev, Ukraine, which reduced power consumption in the city by about one-fifth for more than an hour [6]. Various other attempts to hack into the American power system's cyber network have also been reported [7]. These kinds of attacks will only increase in frequency in the future [8]. These kinds of malicious attacks in the power system have no doubt added more concern to the reliability and resiliency of the power grid.

Power system reliability is well-established and widely accepted practice by power system planners, operators, regulatory authorities, and policymakers. Power system reliability is subdivided into two basic aspects, adequacy i.e. the existence of sufficient facilities within the system to satisfy the customer load demand, and security i.e. the ability of the system to respond to disturbances arising from that system [9]. The overarching concept of reliability has always remained to deliver electricity with acceptable quality, continuity, and environmental compliance. Resiliency was first discussed in [10] as “a measure of the persistence of systems and of their ability to absorb change and disturbances and still maintain the same relationship between population and state variables.” The definition of power system resiliency has metamorphosed into the attribute of a system that reflects its ability to withstand high impact, low probability events, and recover from the consequent situation. Resiliency study, in general, is concerned with high impact low probability (HILP) events such as hurricanes, earthquakes, wildfires, etc. whereas reliability studies usually relate to high probability events with relatively low impacts such as a line to ground fault in transmission line [11, 12]. If we are only concerned with the reliability of the system, designing a system for N-1 or N-2 outages may be enough. However, such a design does not guarantee resiliency as several contingencies may occur due to extreme events [13]. The reliability of a system can be determined without having a detailed knowledge of an event, however, a system resilient to one event may not be resilient to other events [14]. Moreover, a reliable system may not necessarily be resilient [13]. Therefore, it is necessary to make a detailed assessment of the reliability and resiliency of the system against particular events separately.

Cyber-physical infrastructure refers to the integration of physical systems with digital communication and data exchange, forming a complex and interconnected framework. This integration, while enhancing operational efficiency, also introduces new vulnerabilities that can be exploited by cyber-attacks. Cyber-attacks pose a significant threat to modern systems, particularly those that heavily rely on digital communication and data exchange. These attacks can result in devastating consequences, including financial losses, data breaches, and even physical harm to infrastructure and individuals. Recent research highlights the criticality of secure communication in preventing cyber-attacks on power systems. Secure communication is a crucial aspect of preventing cyber-attacks. This involves ensuring that all communication between devices and systems is encrypted and authenticated to prevent unauthorized access. Additionally, implementing robust security protocols, such as firewalls and intrusion detection systems, can help detect and prevent cyber-attacks. Ensuring that all communication between devices and systems is encrypted and authenticated is essential to prevent unauthorized access. Studies have shown that encryption and authentication significantly reduce the risk of cyber intrusions [15, 16].

Additionally, implementing robust security protocols, such as firewalls and intrusion detection systems (IDS), is vital. Firewalls act as barriers between trusted and untrusted networks, controlling incoming and outgoing network traffic based on predetermined security rules [17]. Intrusion detection systems monitor network traffic for suspicious activity and potential threats, providing an additional layer of defense [18]. For instance, Ref. [15] emphasize the importance of cybersecurity in smart grid systems, suggesting that vulnerabilities in communication protocols can be mitigated through advanced encryption methods and regular security updates. Ref. [16] discuss various attack vectors in power systems and propose a comprehensive framework for enhancing cybersecurity through multi-layered defense strategies. Moreover, research by Ref. [17] highlights the role of firewalls in securing industrial control systems (ICS), which are integral to power infrastructure. Their study indicates that properly configured firewalls can significantly reduce the risk of cyber-attacks. Similarly, Ref. [18] provide insights into the effectiveness of intrusion detection systems in identifying and mitigating threats in real-time, thereby protecting critical infrastructure from potential disruptions.

Authors in Ref. [19] provide a comprehensive survey of learning-based methods for detecting cyber-attacks in IoT systems. It discusses various machine learning algorithms and their applications in detecting cyber-attacks, as well as future prospects for improving cyber-attack detection. Ref. [20] proposes an inoculated sub-observer-based approach for detecting cyber-attacks in a looped energy-water nexus. The approach detects anomalies in the system and prevent cyber-attacks. Ref. [21] proposes a track fusion-based mixture density estimation driven grid resilient approach for detecting and preventing cyber-attacks in power grids. The approach uses a combination of machine learning algorithms and data analytics to detect anomalies in the system and prevent cyber-attacks.

Ref. [22] proposes a median regression function-based state estimation approach for detecting and preventing cyber-attacks in modern power grid. The integration of physical systems with digital communication in cyber-physical infrastructure necessitates stringent security measures to prevent cyber-attacks. Encrypted and authenticated communication, combined with robust security protocols such as firewalls and IDS, are essential components in safeguarding these systems. Continued research and implementation of advanced security strategies are crucial for protecting modern power systems from the evolving threat landscape.

There is some interesting research that sheds some light on the area of detection of possible cyberattacks in the system. Ref. [23] proposes Cyber-attack Detection and Mitigation Platform (CDMP) to identify and mitigate possible False Data Injection Attacks (FDIAs) and Denial of Service (DOS) targeted towards Area Generation Control (AGC)'s loop of cyber-physical layers. Ref. [24] proposes a real-time and computationally efficient tool for anomaly detection in large-scale cyber-attacks with an accuracy of 99% (98% True Positive Rate and less than 2% False Positive Rate). Ref. [25] utilizes Petri-net models to simulate possible intrusion scenarios and builds 3 of the defense system in a substation i.e. Firewall, Intrusion Prevention System (IPS), and password models to protect the system against such attacks and assess the reliability in such scenarios. A novel cyber-physical resiliency metric is proposed in [26] for the transmission electric grid based on both operational and infrastructural components such that metrics are updated in real-time with changing scenarios. An innovative, self-healing mechanism for mitigation of cyber-attacks and recovery of power system observability on a Phasor Measurement Unit (PMU) Network is presented in [27], which used Software-defined Networking (SDN) reconfiguration mechanism to isolate compromised PMUs and connect uncompromised PMUs. [28] analyzed limitations of static and dynamic attack detection and identification procedures for a power network modeled via a linear time-invariant descriptor system and shown that dynamic detection and identification method exploits the network dynamics possibly requiring fewer measurement and outperforms the static counterpart with an example of a cyber-physical attack against the IEEE 14 bus system.

Few other pieces of literature have developed the metrics to quantify the impact of cyberattacks on the reliability and resiliency of power systems. Ref. [29] incorporates cyber malfunctions in reserve capacity models and power generation systems to quantitatively assess the impact of the malfunctions and deploy demand-side resource management strategies to effectively mitigate such contingencies. Ref. [30] explores the impact of cyber-attack in a wind farm and quantifies it in metrics like Loss of Load Probability (LOLP), Expected Energy Not Supplied (EENS), and Time to Compromise (TTC). Ref. [31] simulates a cyber-attack and assesses its impact on the distribution system proposing a Cyber-Physical Resiliency Metric (CPRM) that provides a score that can be used by the operator for monitoring the state and taking suitable control needed for the system performance. Ref. [32] presents two tools; Sync AED and Cyber-Physical Transmission Resiliency Assessment Metric (CP-TRAM) for resiliency assessment and decision support that helps visualize possible cyber and physical vulnerabilities in the power transmission network. A Cyber-Physical Security Assessment Metric (CP-SAM) based on quantitative factors affecting resiliency across different layers of microgrid system is provided by [26]. Ref. [33] proposes a cyber-security enhanced Distribution Automation System (DAS) that can identify the anomalies in data and help mitigate them in a distribution system. Ref. [8] proposed a multi-phase trapezoid as shown in Figure 1 to recognize and assess the stages that the grid goes through in the occurrence of extreme events.

This paper represents any kind of disturbances in the power system, its degraded state, and restoration process in the time domain, which allows developing the metrics to quantify resilience.

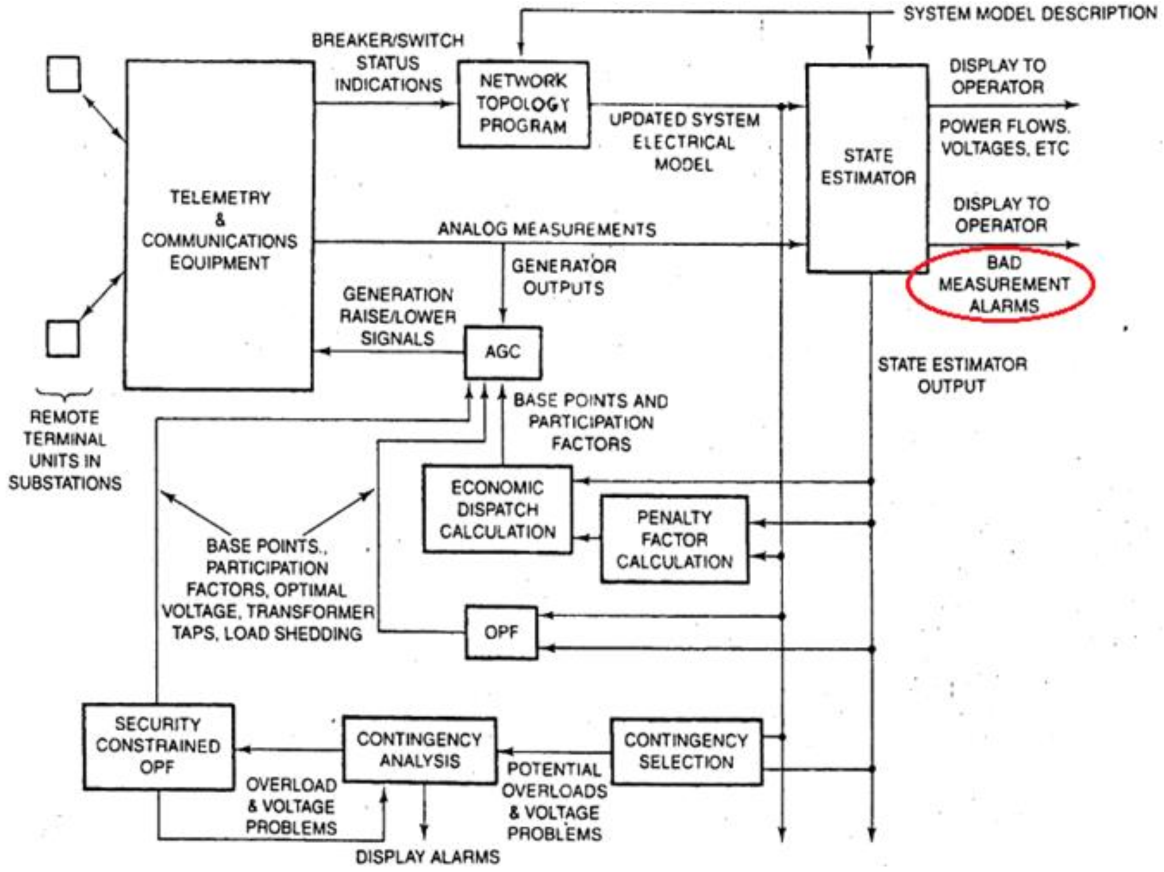
SYSTEM MODEL DESCRIPTION
BREAKER/SWITCH STATUS INDICATIONS
NETWORK TOPOLOGY PROGRAM
DISPLAY TO OPERATOR
POWER FLOWS, VOLTAGES, ETC
UPDATED SYSTEM ELECTRICAL MODEL
STATE ESTIMATOR
TELEMETRY & COMMUNICATIONS EQUIPMENT
DISPLAY TO OPERATOR
ANALOG MEASUREMENTS
BAD MEASUREMENT ALARMS
GENERATOR OUTPUTS
GENERATION RAISE/LOWER SIGNALS
AGC
STATE ESTIMATOR OUTPUT
REMOTE TERMINAL UNITS IN SUBSTATIONS
BASE POINTS AND PARTICIPATION FACTORS
ECONOMIC DISPATCH CALCULATION
PENALTY FACTOR CALCULATION
BASE POINTS, PARTICIPATION FACTORS, OPTIMAL VOLTAGE, TRANSFORMER TAPS, LOAD SHEDDING
OPF
SECURITY CONSTRAINED OPF
CONTINGENCY ANALYSIS
CONTINGENCY SELECTION
OVERLOAD & VOLTAGE PROBLEMS
POTENTIAL OVERLOADS & VOLTAGE PROBLEMS
DISPLAY ALARMS

Figure 1 Energy Control Center System Security Flowchart.

Three distinct phases can be visualized in the multi-phase resilience trapezoid. Phase I refers to the disturbance progress which lasts from the triggering of the event to the end of the events. Phase II is the post-disturbance degraded state which is the time duration between the end of the event and before any attempt to recover the system is initiated. The restorative state is the third state in the trapezoid that represents the time duration when the attempts to restore the system to the original state are carried out [34].

The above discussions point to an evident research gap in the development of a resiliency and reliability assessment framework that can incorporate cyber-attack and provide quantifiable metrics that reflect the behavior of the microgrid. Motivated by the need for resiliency and reliability study of a microgrid against a cyber-attack, this paper presents a framework for evaluating resiliency and reliability during an event of a cyber-attack. The contribution of this paper is summarized below:

- To develop a quantitative framework to assess smart-grid's resilience and reliability that incorporates cyber-attack modelling, impact assessment of cyber-attack to obtain expected resiliency and reliability indices.
- To develop a methodology to model cyber-attacks for analysis based on state-estimation and model its attack frequency on the smart-grid using a probabilistic model.
- To develop a bad-data detection strategy utilizing industry standard approaches and provide a comparative study based on the proposed framework.

The paper is divided to 5 sections. Section 1 contains introduction with majority of literature review on the subject area and specification of the problem. Section 2 of the paper contains detailed methodology on the modelling of cyber-attack and the reliability and resiliency assessment framework for cyber-attack. Section 3 is the result section where the case study and the result of the paper is shown. Section 4 contains discussion on proposed methodologies, metrics and the difference in assessment of reliability and resiliency of the system in event of a cyber-attack.

2. Modelling Methodology

2.1 Modelling a Cyber-Attack in a Power System

The field of power system is continuously evolving from the symbiosis of advancement in communication system and existing physical system. The access to an abundance of time-dependent information of system variables distributed over a wide area has benefited the utilities in numerous ways. However, a cyber-integrated network also introduces numerous access points that are vulnerable to malicious attacks with disastrous repercussions. A cyber-attack in a power system can be successful with consecutive exploitation in the following two phases [35]:

- Phase I: Access Point Exploitation

Relays, IED present in a smart grid are connected to the control room via dial-up modems, RS-232, or Ethernet. The control room and substation computers, IEDs, are isolated in an electronic security perimeter (ESP). ESP generally has a firewall to increase security. Inter-ESP link maybe wireless or may use leased bandwidth from a third party and is therefore at risk of penetration. Cyber-devices in an ESP can be compromised by accidental introduction of malware through Universal Serial Bus (USB), virus penetration or infected software patches. A compromised system within an ESP may establish communication with outside attackers. A device within an ESP can be compromised intentionally by an individual with authorized physical access. Phishing can be done to access control room’s computers.

- Phase II: Implementation of Cyber-Attack

After the penetration point is found, an attacker can perform any of the four classes of attacks:

  - Reconnaissance

It is usually done to identify weak points for attack before penetration, and to learn about the system model and details for further attacks.

  - Denial of Service (DoS) Attacks

This attack attempts to break communication links to stop command and sensor measurement from reaching its intended destinations.

  - Command Injection Attacks

This attack attempts to send false commands to the communication, measurement or protection devices to benefit the perpetrator.

  - Measurement Injection Attacks

This attack aims to alter the measured values to benefit the perpetrator. False Data Injection Attack (FDIA) is an existing example that falls in this class and is explored in this paper. FDIA are capable of disrupting the power system state estimation process by intentionally producing erroneous data to cause detrimental effects in the physical parts of the power system. Figure 1 [36] shows the information flow between the various operational functions within an energy control center computer system. The system receives a wide range of power system operational data from remote terminal units that encode measurement transducer outputs and opened/closed status information into digital signals that are transmitted to the operations center over communication circuits [36].

In this work, the distribution system is modelled as a graph G consisting of nodes or vertices V and edges E as shown in (1). The buses, sections, load points, circuit breakers and fuses are treated as nodes, whereas, the edges are the connections between the nodes.

$$G = \{V, E\} \tag{1}$$

The next step after deducing the graph model for the distribution system, is to derive a method to simulate a cyber-attack and assess its impact on the system. Theorem 3.1 in [37] states, "Suppose the original measurements z can pass the bad measurement detection. The malicious measurements z_a = z + a can pass the bad measurement detection if a is a linear combination of the column vectors of H, that is, a = Hc". These concepts are further developed in this work to model cyber-attacks on an active distribution system.

The DC based state-estimation model can be formulated as:

$$z = h(x) + e \tag{2}$$

where z = [(z1, z2, z3, …, zm)] denotes measured data, x = [(x1, x2, x3, …, xn)] denotes system states, e = [(e1, e2, e3, …, em)] denotes measurement noise that follows a Gaussian distribution with zero mean. h(x) is a mxn full rank matrix that denotes the function dependency between the measurements z and the state variables x. The precise form of h(x) is determined by the grid structure and the line parameters. The estimated state variable x' is expressed in (3).

$$x' = \left[[H]^T[W][H]\right] - 1[H]^T[W]z \tag{3}$$

Where W is a diagonal matrix whose elements are reciprocals of the variances of meter errors and H is the functional dependency matrix between the measurement z and state variable x.

In practice, the measurement residual is calculated and its 2-Norm i.e. ‖z-Hx‖ is compared with a threshold to check for the existence of bad measurement. Generally, it is found that ‖z-Hx‖ follows a χ^2 (v) distribution where v = m - n is the degree of freedom. Therefore, the threshold is set from χ^2 (v) distribution. From Theorem 3.1 obtained from [37], it is evident that an attack vector that complies, a = Hc where z_a = z + a will go undetected.

For the test system illustrated in Figure 2, let x = $[(x1, x2, x3)]^T$ represent the bus angles at buses 2, 3, and 4, respectively, and z = $[(z1, z2, z3, …, z7)]^T$ denote the measured data. Bus 1 is designated as the slack bus. For any c = [(c1, c2, c3)], the vector a = $[(a1, a2, a3, …, a7)]^T$ is computed using a = Hc, and the adjusted measurement z_a is determined. To find the successful combination of attack-vectors, brute-force approach is applied and the successful attack vectors that pass the following condition is recorded.

$$\|z_a - [H]\hat{x}_{bad}\| \le \tau$$

Here,

τ is a threshold taken from a Chi-squared distribution table.

x_{bad} is estimated state variable calculated after obtaining the H, W and z_a.

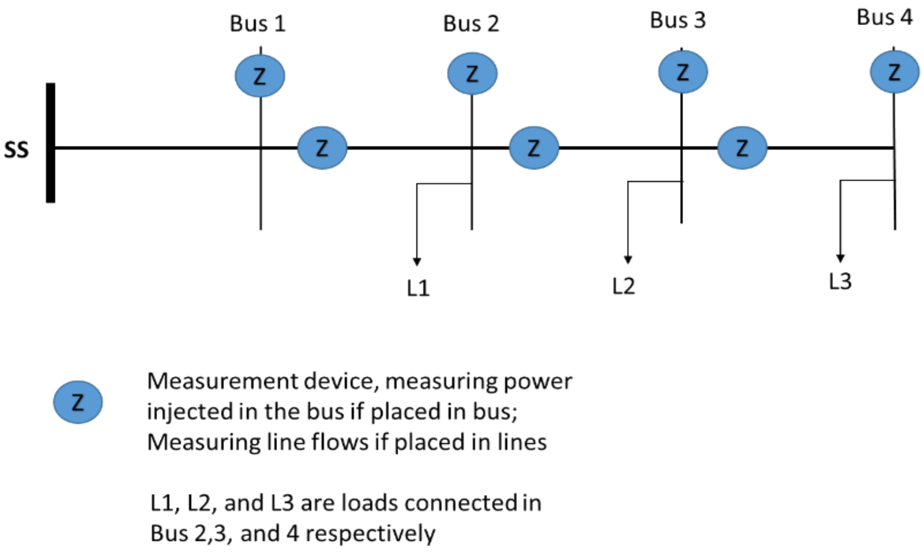
Bus 1
Bus 2
Bus 3
Bus 4
SS
Z
L1
L2
L3
Measurement device, measuring power injected in the bus if placed in bus; Measuring line flows if placed in lines
L1, L2, and L3 are loads connected in Bus 2,3, and 4 respectively

Figure 2 Distribution System Test Network.

All possible iterations for cc were performed, and the load loss for each combination of c, state variable x, injected error a, and measured data z was recorded. Figure 3 illustrates some of the load losses, keeping c1 constant while varying c2 and c3. The z-axis of the graph represents the load lost, and the x-axis and y-axis represent c2 and c3, respectively.

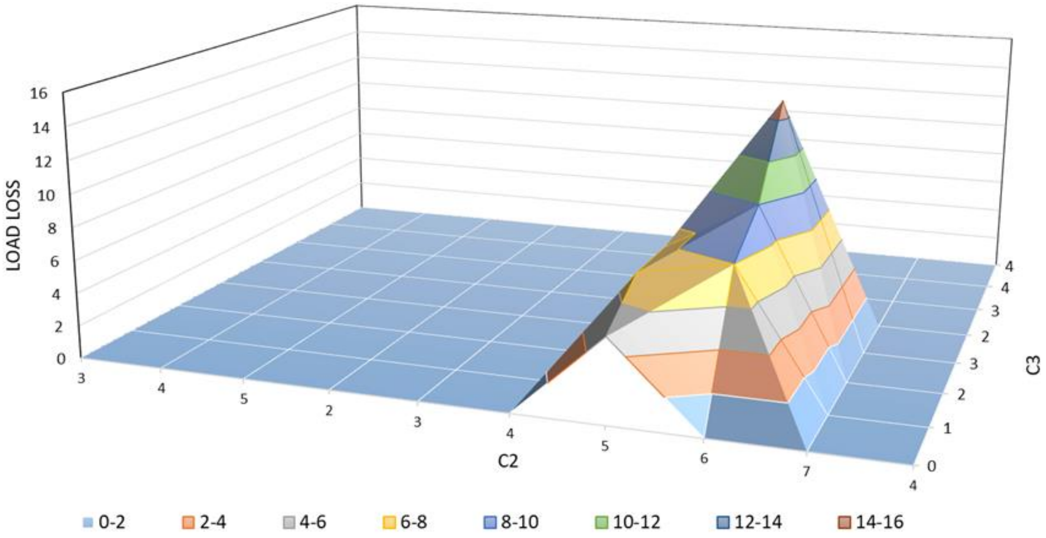

Figure 3 Possible Losses in the system due to FDIA.

2.2 Modelling Reliability and Resiliency Framework to Incorporate Cyber-Attack

As discussed in the previous sections, the interoperability of cyber-physical systems within a power system can be misused by perpetrators to cause substantial financial and social disruptions. A sequential Monte-Carlo Simulation (MCS) is used in this work to simulate the system states in response to various cyber-attack scenarios, and to obtain the probability distributions of the appropriate quantitative indices in order to understand the impact of such events in the distribution grid before, during and after the impact. This paper investigates the impact of cyber-attacks on both the reliability and the resiliency of a power distribution system.

The quantitative indices to assess the reliability of power systems has been well established and widely accepted. The loss of load expectation (LOLE) is the most widely used index that represents the expected number of days or hours of load curtailment. This index is mainly used at the generation adequacy or HL-I level. Reliability metrics commonly used in distribution systems are SAIFI, SAIDI, and CAIDI [9]. The expected energy not supplied (EENS) index is found to be used at all the power systems levels, i.e. generation, transmission and distribution.

Power system resiliency is the ability of the system to withstand or endure extreme events, such as cyber-attacks, and remain functional and/or recover rapidly to avoid further catastrophic repercussions on the power system and severe societal impact on the customers. Evidently, it is important to recognize and analyze the stages that the grid goes through in the occurrence of an extreme event. Ref. [34] proposed a multi-phase trapezoid as shown in Figure 4 that illustrates the various operating stages a power system goes through before, during and after an extreme event. The change in resilience level in these stages construct the three phases that can be identified in the resilience trapezoid of Figure 4. The percentage of load connected is used as a resilience level in this study. Ro shows the pre-disturbance resilient state, where the event has not occurred. The grid's resiliency after the event occurs is given by R_{pd}. It shows the state of the system before any restorative action takes place. As the restorative action takes place and the resiliency index starts to improve, it is assumed that the resilience level restores to R_o. The different phases that a grid undergoes in this process are:

Phase I: It is known as the disturbance progress phase. It lasts from time of event, t_{oe} and end of the event, t_{ee}.

Phase II: It is known as the post-disturbance degraded state. It is the duration between the end of the event, t_{ee} and the start of the restoration process, t_r.

Phase III: It is known as the restorative state of the system. In this phase, restorative action is taken that helps the system to minimize load lost and be back online. It is the duration between the start of the restoration process, t_r and the end of restoration given by T.

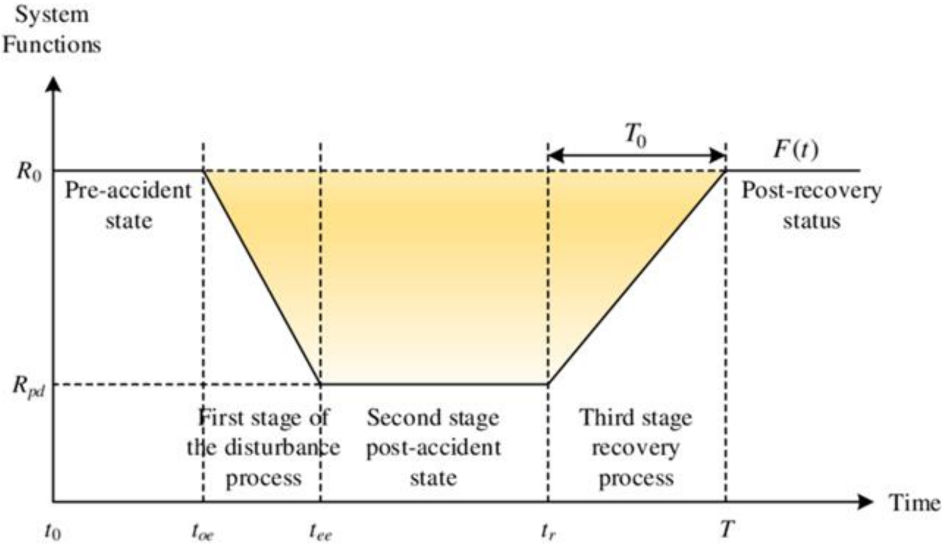

Figure 4 Multi-Phase Trapezoid.

Figure 4 shows the different stages a power goes through as it succumbs to a cyber-attack. Resilience indices shown in Table 1 [11, 16] can be measured at the different trapezoid phases to quantify the impact of the attack at the different phases. The index Φ in (4) quantifies how fast is the system degrades as the disturbance progresses after the occurrence of the attack. It measures the MW load loss per hour. The indices EENSsys and E calculated using (5) and (6) respectively measure the average energy not supplied per load-point and the duration of load curtailment in post disturbance degraded state following the disturbance due to the event. The index E is the duration between the end of the disturbance phase and the start of any restorative action in the grid. The index $\mathit{\Pi}$ obtained from (7) measures how quickly the system can recover from the impact due to the restorative actions. It measures the MW load restored per hour in the system.

Table 1 Equations for Resiliency Assessment.

Phase	Mathematical Expression
Phase I: Disturbance progress	$\Phi = \frac{R_o - R_{pd}}{t_{ee} - t_{oe}}$ (MW/hr) (4)
Phase II: Post disturbance degraded state	$EENS_{sys} = \frac{\sum_{s=1}^{Ns} ENS(s)}{N_S^o}$ (MWhrs/int) (5) $E = t_r - t_{ee}$ (hrs) (6)
Phase III: Restorative state	$\Pi = \frac{R_o - R_{pd}}{T - t_r}$ (MW/hr) (7)

Ns and Nos in (5) are the number of attempted, and successful cyber-attacks respectively. The overall methodology to quantify the reliability and resiliency performance is presented in the flowchart shown in Figure 5. The initial step is to define the power distribution system. This includes identifying the number of buses, sections, loads connected and the load demand of the system. Each component in the system is exposed to failure due to its inherent characteristics.

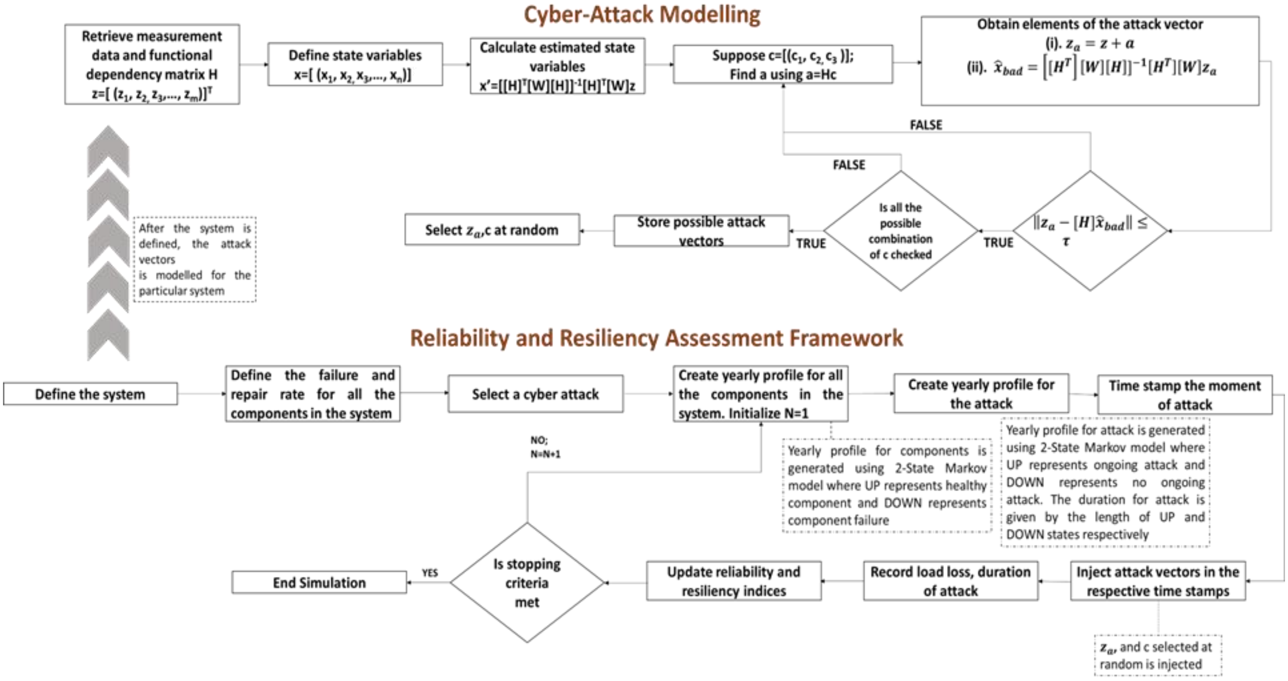
Cyber-Attack Modelling
Retrieve measurement data and functional dependency matrix H $z=[(z_1, z_2, z_3, \dots, z_m)]^T$
Define state variables $x=[(x_1, x_2, x_3, \dots, x_n)]$
Calculate estimated state variables $x'=[[H]^T[W][H]]^{-1}[H]^T[W]z$
Suppose $c=[(c_1, c_2, c_3)]$; Find a using a=Hc
Obtain elements of the attack vector
(i). $z_a = z + a$
(ii). $\hat{x}_{bad} = [[H^T][W][H]]^{-1}[H^T][W]z_a$
FALSE
FALSE
Is all the possible combination of c checked
$\|z_a - [H]\hat{x}_{bad}\| \leq \tau$
TRUE
TRUE
Store possible attack vectors
Select z_a,c at random
After the system is defined, the attack vectors is modelled for the particular system
Reliability and Resiliency Assessment Framework
Define the system
Define the failure and repair rate for all the components in the system
Select a cyber attack
Create yearly profile for all the components in the system. Initialize N=1
Create yearly profile for the attack
Time stamp the moment of attack
Yearly profile for components is generated using 2-State Markov model where UP represents healthy component and DOWN represents component failure
Yearly profile for attack is generated using 2-State Markov model where UP represents ongoing attack and DOWN represents no ongoing attack. The duration for attack is given by the length of UP and DOWN states respectively
NO; N=N+1
Is stopping criteria met
YES
End Simulation
Update reliability and resiliency indices
Record load loss, duration of attack
Inject attack vectors in the respective time stamps
z_a, and c selected at random is injected

Figure 5 Framework for reliability and resiliency evaluation.

The injection of attack vectors, and the record of the aftermath of the system is obtained through a series of steps. First, the system for which the reliability and resiliency study during a cyber-attack needs to be studied is defined. After the system is defined, the topological information of the distribution system is retrieved. This includes measurement data on branches and buses of the network, load demand on the network etc. State estimation is then applied to find the bus angles in the system. Possible attack vectors for the system are created as described in Section 2.1. Then, an attack rate is defined to quantify the frequency in which the system is exposed to the attack vector. For an attack rate, the yearly profile of the attack rate is generated. An attack rate is assumed to exist in only two state: UP state and DOWN state. Up signifying an active cyber-attack and DOWN signifying no such occurrence of cyber-attack for that time.

For any such UP sequence, through randomness, an attack vector is selected and passed through the system. The loss of load, its duration of attack and the moment of time is recorded for analysis. Sequentially, for any DOWN state for a component caused due to its failure rate, the loss on the system is recorded for analysis. The duration of attack is directly going to be dependent on the type of device the FDIAs is planning to penetrate. Therefore, Mean Duration of Attack (MDOA) is modelled using an inverse tangent function over the number of measurement device present in the system to obtain a probabilistic index and weighed over 2 hours to represent the possible duration for such attack. This process is repeated for N no. of years for variation of such attack-rates. Finally, the reliability and resiliency performance of the system is calculated and is elaborated in Results.

The LOLE and the EENS [9] are used in this paper to quantify the impact of cyber-attacks on a test distribution system. The points of time along with the duration in which, the distribution system fails to meet the load demands at particular load points due to inherent failure characteristic of the system component are found and the losses are recorded to obtain the results for a base case i.e. the system without a cyber-attack. The base case is then used for comparison with system performance in the event of cyber-attacks.

3. Case Studies and Result

A number of case studies were carried out to investigate the impact of cyber-attacks on the reliability and resiliency of a distribution system. A 4-bus radial test distribution system as shown in Figure 2 was used in the study. A simple system was intentionally used in this paper to illustrate the comparative impacts on these two system characteristics, the difference between which are not easily understood in the power industry. The methodology can, however, be applied to large and more complex systems with increased computational efforts.

The test system is a simple distribution system with nominal voltage as 12.66 kV, and the total load is 100 MW. L1, L2, and L3 represents load points with 20%, 40% and 40% of the total load respectively. Acceptable bus voltage range is set between 0.9 p.u. to 1.05 p.u. DC power flow is performed to compute line flows. The component reliability data and the load data are taken from [9]. The failure rate of the section and distributor is 0.1 failures per year and 0.2 failures per year respectively. The repair time is 2 hours. Figure 6 shows a typical demand variation profile within a day.

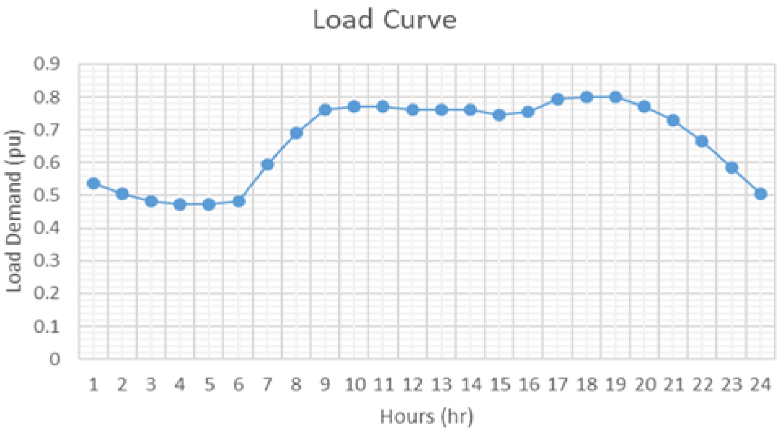

Figure 6 Typical demand variation pattern in 24 hours.

3.1 Impact of Cyber-Attack on System Reliability

This section describes a study done to illustrate the impact of cyber-attack on the reliability indices. The study was repeated with different attack rates to investigate the sensitivity of the attacks s on the reliability indices.

A Monte Carlo simulation was carried out as described in the methodology shown in Figure 4. Figure 7 shows the system LOLE as well as the load point LOLE at the selected attack rates. The index quantifies the expected number of hours of load loss in a year, at the individual load points and at the system level.

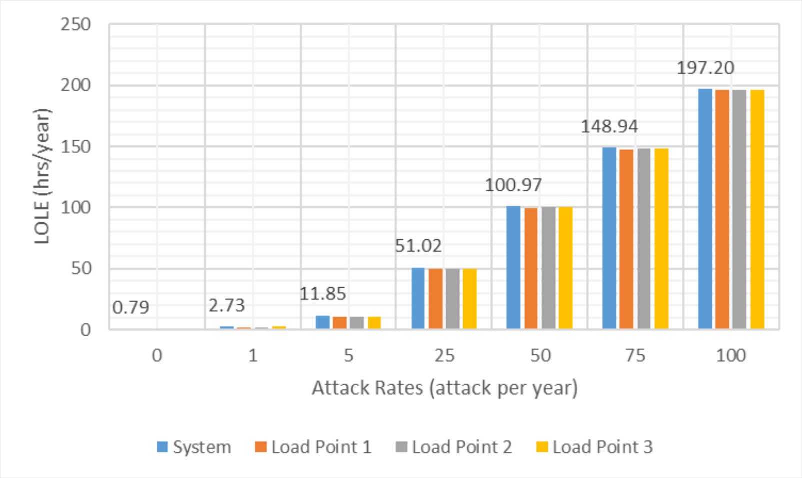

Figure 7 LOLE for different attack rates.

It can be seen that both the system LOLE and the load point LOLE increase significantly, as the attack rate is increased.

Figure 8 shows the resulting EENS for various attack rates in the system.

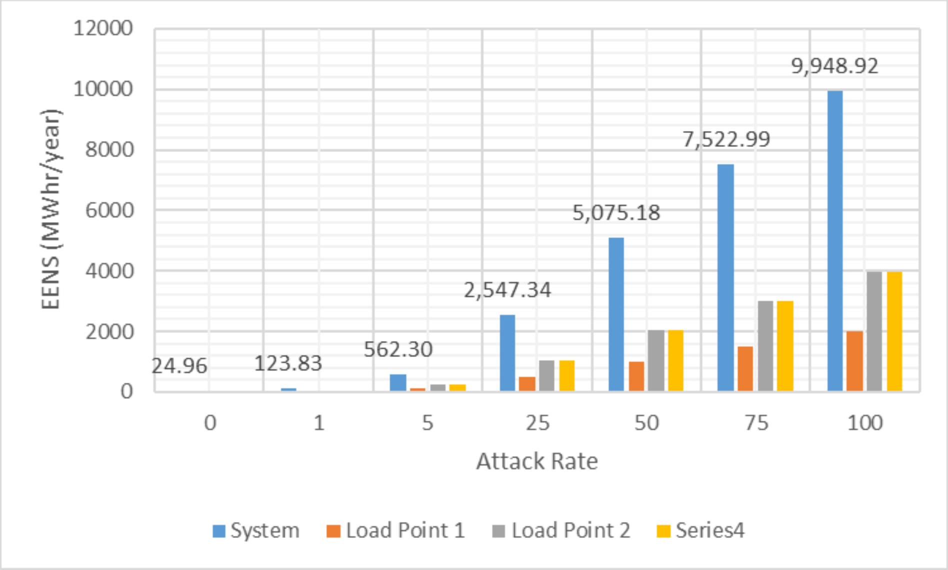

Figure 8 EENS for different attack rates.

It is evident that the loss increases significantly as the attack frequency is increased. The EENS index provides a measure of the magnitude of the losses that can readily be expressed in monetary values. The index is a useful indictor in deciding investment in remedial measures, such as bad-data detection systems to safe-guarding the system.

Figure 7 shows evidence to support the conclusion that, the impact on the probability of trouble is widespread throughout the system and is equal on all the load points. Figure 8 shows that the impact of cyber-attack is dependent on the amount of load lost by the system and the load points. Load points having lower demands show lower impact and load points with higher demands show higher impact of cyber-attack in terms of energy lost. In addition, it is seen that the reliability indices of the system degrades with increasing attack rates while comparing both the probability and the impact of cyber-attack.

The above studies illustrate the impact of cyber-attack frequency on the reliability indices. Cyber-attacks are however considered to be low probability events. With the envisioned transition of power grids into cyber-physical systems, the probability of these events are expected to notably increase in the future. The following study considers two scenarios. Scenario 1 is the current scenario in which cyber-attacks are considered as low probability events. Scenario 2 assumes a future scenario where the power grids are fully integrated cyber-physical systems and cyber-attacks are no longer low-probability events.

It is important to determine the probability distributions of cyber-attacks in the two scenarios in order to evaluate the impact on the system reliability. The actual shape of the distributions can be logically debated at this time due to lack of data for the two scenarios. Many researchers use a Poisson distribution to model rare events. A Poisson distribution with an expectation of 1 attack per year is assumed for Scenario 1 as shown in Figure 9. Uncertainty of random events are often modeled as a Gaussian distribution. The probability distribution of cyber-attacks in Scenario 2 is therefore represented by a normal distribution in this paper. Figure 10 show a 15-step discrete distribution within six standard deviations, assuming a 14% standard deviation about the expectation of 50 attacks per year.

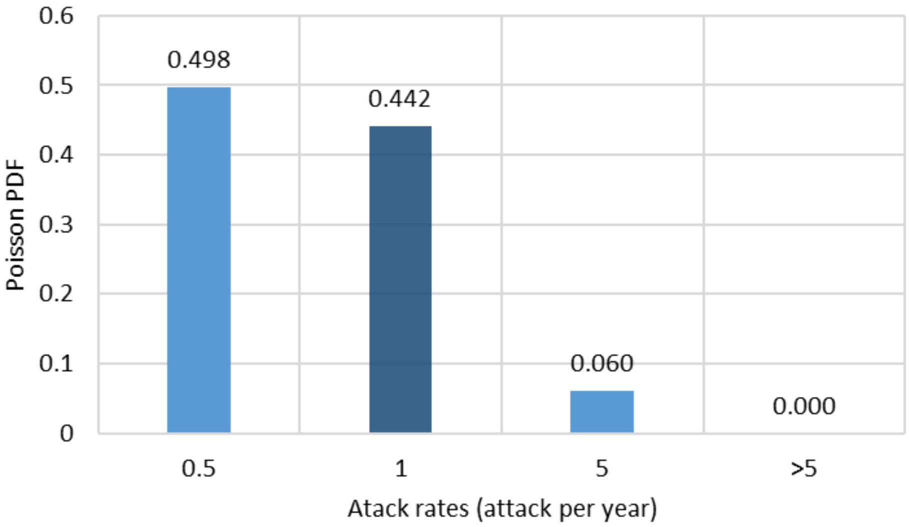

Figure 9 Probability of occurrence of cyber-attack in present day scenario - Scenario 1.

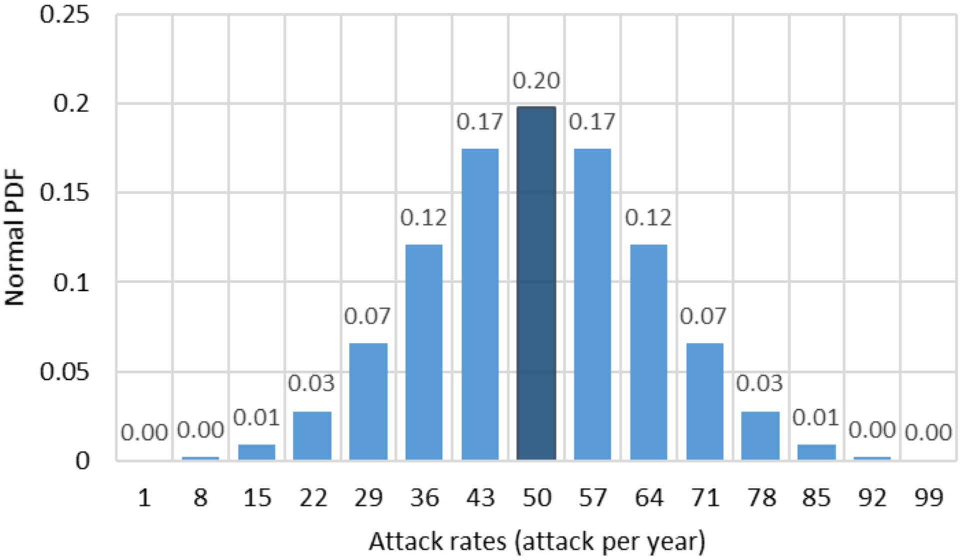

Figure 10 Probability of occurrence of cyber-attack in a future scenario - Scenario 2.

A reliability assessment was done to evaluate the impact of cyber-attacks for the two scenarios, and the system EENS results are shown in Figure 11. For a comparative analysis, the figure also shows the system EENS when cyber-attacks are not considered in the assessment. Figure 11 shows that the consideration of cyber-attack in today's scenario significantly increases the unserved energy in the system. The figure further shows that cyber-attacks have much profound impact on the system reliability in Scenario 2 as power-grids transition into cyber-physical systems. The results clearly point in the direction of growing cyber threats and their devastating reliability impacts as power systems are metamorphosed to fulfill their sustainable goals. This clearly dictates the need for proper investigation of the cyber-physical interdependencies to avoid such scenarios in the future.

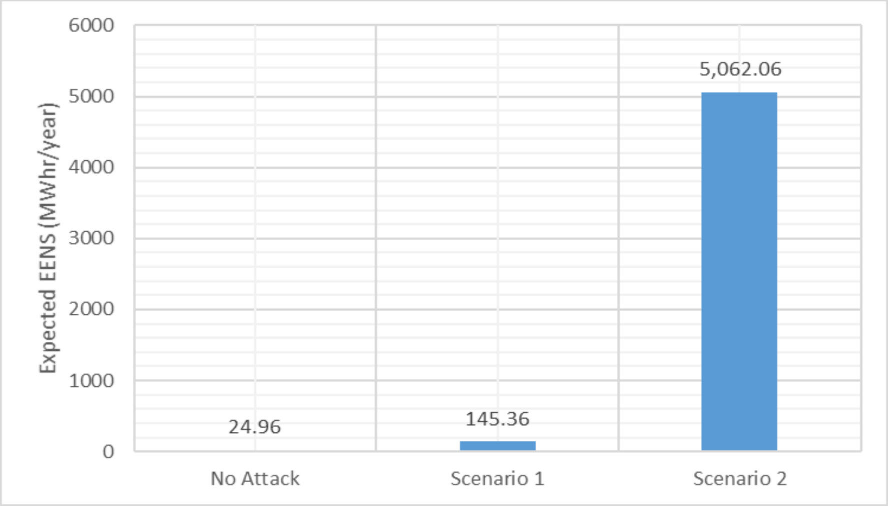

Figure 11 Expected EENS (MWhr/year) for different scenarios.

3.2 Resiliency Assessment in Event of a Grid-Scale Cyber-Attack

This section presents studies done to illustrate the impact of cyber-attack on the system resiliency. The impact of a cyber-attack is first analyzed by comparing the annualized LOLE and EENS indices without and with a single attack consideration. Figure 12 shows that the LOLE indices increase significantly with the cyber-attack and difference is approximately equal to the system down time impact of the cyber-attack. It should be noted that the results presented depend on the input data. If the down time including the restoration time due to such an attack is increased, the difference in LOLE in Figure 12 will increase as well. An analysis of the load point indices in Figure 12 concludes that all the load points are affected by a cyber-attack, and therefore, the LOLE at all the load points are approximately equal and closer in value to the system LOLE. When a system is not subjected to a cyber-attack, the load-point LOLE increases as the load points are located further away from the point of supply. This is because distribution systems are usually operated radially, and the number of components exposed to failure increases with the distance from the supply point.

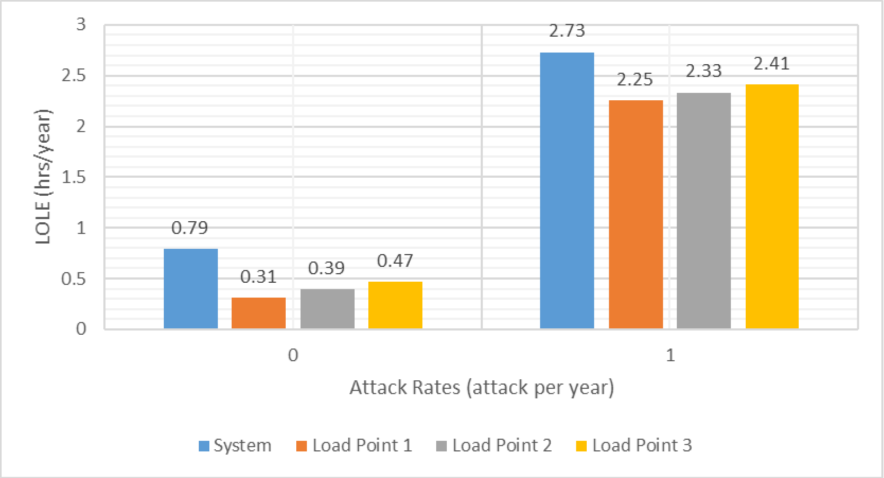

Figure 12 LOLE (hrs/yr) for the system observing zero and one cyber-attack per year.

Figure 13 shows the impact on the EENS index with and without considering the occurrence of a cyber-attack. It can be seen that there is a significant increase in both the load-point and system EENS. The load-point EENS largely depend on the magnitudes of load connected to those points.

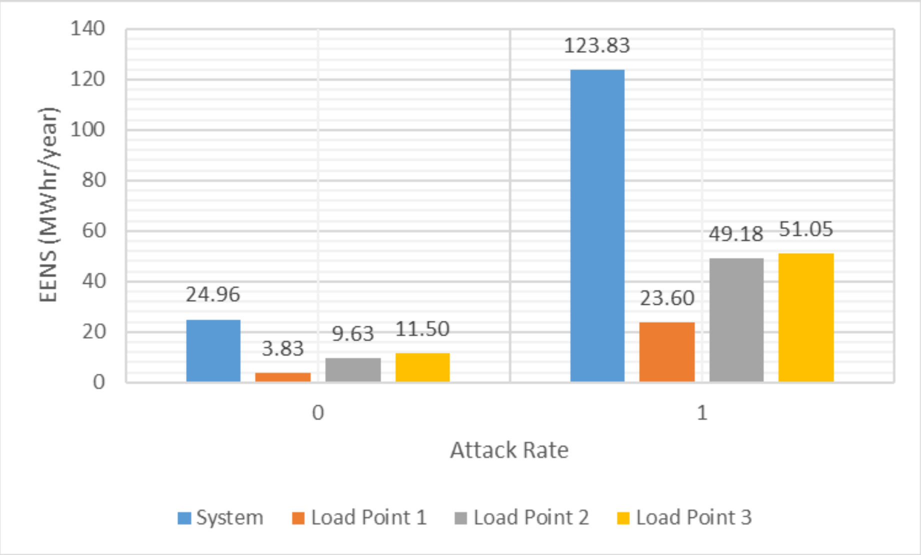

Figure 13 EENS (MWhr/yr) for the system observing zero and one cyber-attack per year.

The expected energy not supplied per interval or EENS (MWhr/int) due to an HILP event has been used as a resiliency metric in published literature. This index alone is not sufficient to describe the resiliency characteristics of a system. The EENS quantifies the magnitude of the impact but does not reflect the duration of the impact or the response of the system to the impact that are important in comprehending the resiliency of the system. The metrics associated with the three phases of a system's response to an HILP event, as shown in Table 1, are evaluated for the system, and the results are shown in Table 2.

Table 2 Resiliency of the system.

Resiliency Metrics		
	Case I	Case II
Φ(MW/hr)	24.84897	24.98939
EENS (MWhrs/int)	188.4839	368.3073
E(hr)	1.824	5.458
Π(MW/hr)	25.47656	25.95405

The following study considers two cases. Case I assumes that the occurrence of a cyber-attack is immediately recognized, and the recovery action follows. However, it often takes considerable time to determine the cause of a system outage. Case II considers an expected delay time of 4 hours to troubleshoot and identify the cyber-attack. The uncertainty around the delay time is represented by a Gaussian distribution. Table 2 shows the results for the two cases using the resiliency indices [11, 26] evaluated at the different impact phases of the system. It can be seen that the rate of system degradation is similar for the two cases as the disturbance progresses. The rate of system recovery in the restorative phase is also approximately equal. This is because the restoration resources in both the cases are the same. The duration of post event degradation state E, however in Case II is significantly higher than that of Case I. The difference is approximately equal to the time taken to identify that the cause of system outage was a cyber-attack. Table 2 shows that the expected energy not supplied EENSsys in Case II is much higher than that of Case I. The delay in starting the restorative action in II results in relatively high energy not supplied at the load points.

While these indices also validate the need for recognition of different stages in case of an attack, the result also infer contrasting achievable benefits from strengthening the infrastructural resiliency through various measures, one of which is described in the following section.

3.3 Inclusion of Cyber-Attack Detection Strategies: Bad-Data Detection Algorithm

A vast majority of research has been done on identifying proactive solutions to cyber-attack as well as on reactive measures [15-20, 25]. One of the solutions is to implement a mechanism to identify the cyber-attack before it can impact the power system and prevent malicious actions to disrupt the continuous flow of power. One of the effective strategies to prevent erroneous data from entering the system is described in [28] and is known as the bad-data detection algorithm. It can be implemented in the energy control center in the operating room as described in Figure 1. This section presents a study to evaluate the reliability and resiliency of a distribution system equipped with a simple yet effective bad-data detection algorithm that helps identify erroneous data due to a cyber-attack. Figure 14 shows the flowchart of the bad-data detection algorithm.

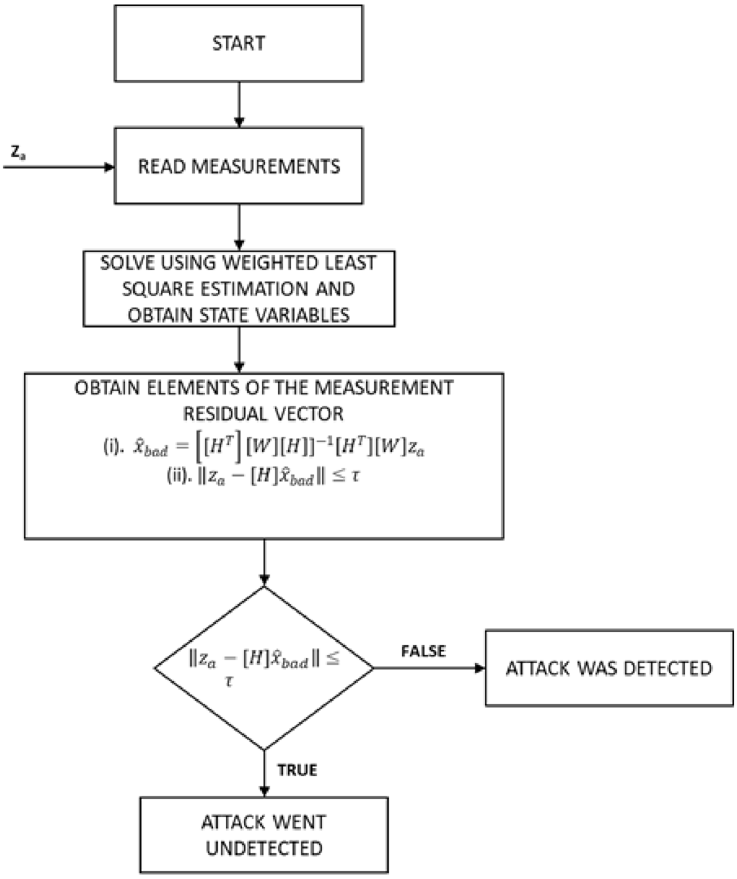
START
z_a
READ MEASUREMENTS
SOLVE USING WEIGHTED LEAST SQUARE ESTIMATION AND OBTAIN STATE VARIABLES
OBTAIN ELEMENTS OF THE MEASUREMENT RESIDUAL VECTOR
(i). $\hat{x}_{bad} = \left[[H^T]\right][W][H]]^{-1}[H^T][W]z_a$
(ii). $\|z_a - [H]\hat{x}_{bad}\| \leq \tau$
$\|z_a - [H]\hat{x}_{bad}\| \leq \tau$
FALSE
ATTACK WAS DETECTED
TRUE
ATTACK WENT UNDETECTED

Figure 14 Bad-data detection algorithm.

A bad-data detection algorithm is based on state-estimation and works by comparing the 2-Norm of the residual vector with a certain threshold. The residual vector is the difference between the observed measurement and the recorded state variable for the system. The threshold is taken from a Chi-squared distribution table as the errors in actual and observed data follows a Chi-distribution. The mathematical expression for the residual vector is expressed in (8).

$$\|z_a - [H]\hat{x}_{bad}\| \leq \tau \tag{8}$$

As discussed earlier, it is assumed that the perpetrators know the complete topo-logical information of the system and can accurately create the [H] matrix. Consequently, any combination of attack vectors that satisfies the condition "a = Hc" is considered a successful vector. The attackers, however, cannot truly map the [H] matrix because of its confidential nature. As [H] contains information only available to the system operator, this secrecy of [H] introduces errors in the [H] model. Any combination of attack vectors that complies with the "a = Hc" condition is passed through a bad data detection algorithm as shown in Figure 14, and only the successful ones are recorded. The recorded vectors and their impacts on the system are evaluated.

The system LOLE results of this study are shown in Figure 15. The results from Figure 7 obtained without the bad-data detection system are also shown for comparison. Figure 15 shows a significant decrease in the LOLE with the implementation of the bad-data detection algorithm.

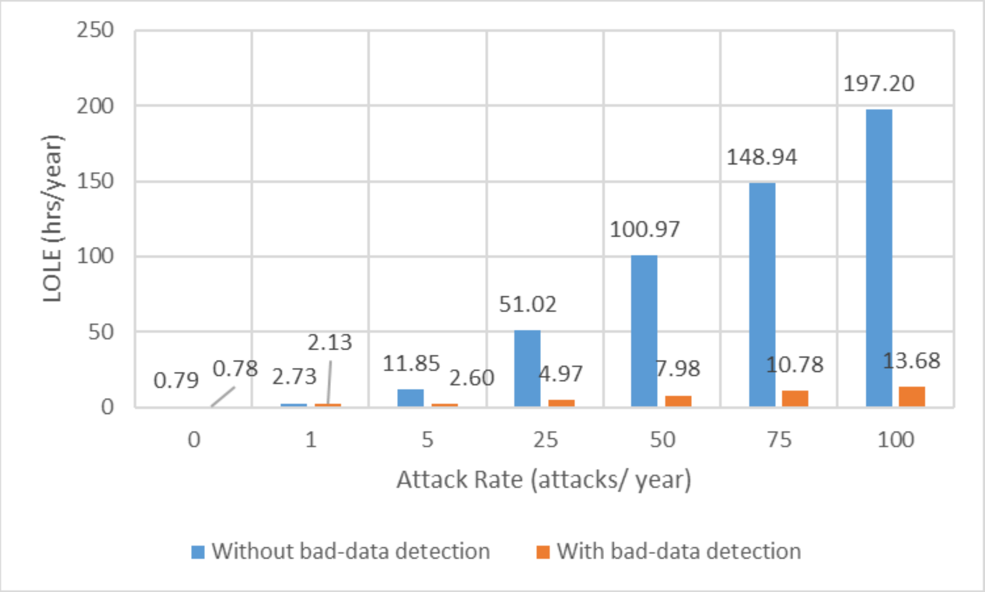

Figure 15 LOLE for different attack rates with and without bad-data detection.

It should be noted that Figure 15 provides only the expected values of the resulting impacts. The distributions of the indices on the other hand can provide detailed information including the probabilities of the best and worst case scenarios. Figure 16 shows the distribution of the loss of load indices for an attack rate of 5/year. It can be seen that with no bad-data detection system, the system will be exposed to a loss of load equal to the mean value with the highest probability. Whereas, the system is most likely to see no outages or very small loss of load if equipped with the detection algorithm.

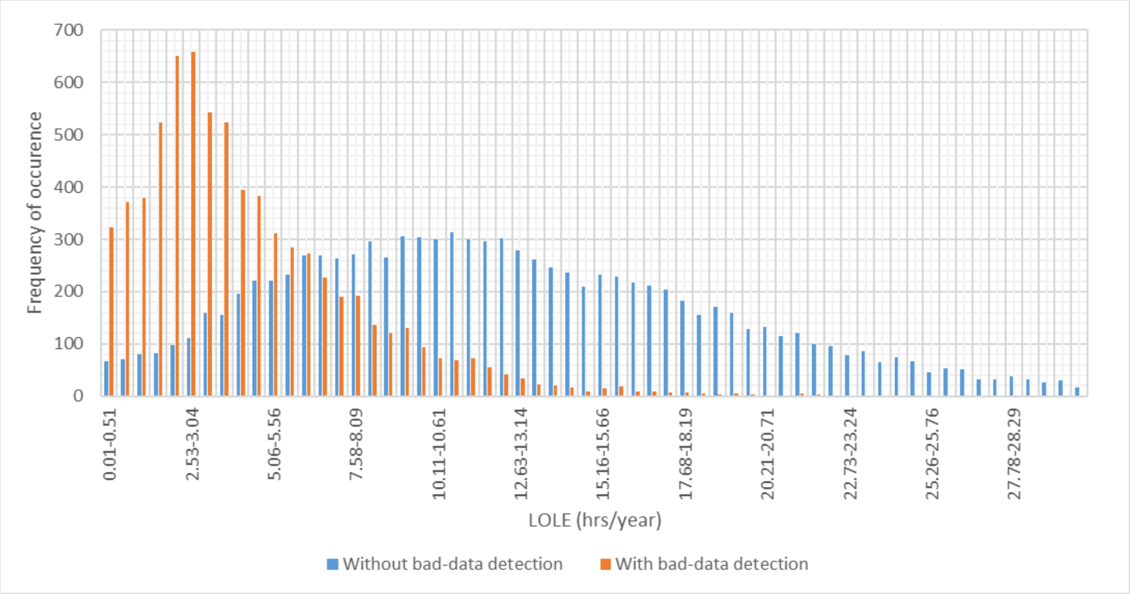

Figure 16 LOLE Distribution for 5 attack/year with and without bad-data detection.

Improving the resiliency of the system is also attributed to different strategies involved in restoring the power to the system. There are numerous strategies that utilities apply in order to mitigate the effect of such event. These strategies are generally either infrastructural or operational in nature. Bad-data detection strategy is one of the most important infrastructural strategy to prevent FDIAs. It helps in identifying false-data beforehand thus preventing any kind of load loss in the system.

Figure 17 shows the multi-phase trapezoid model for the distribution system under a cyber-attack that commences on 24th hour for a particular year, with and with-out the bad-data detection mechanism. It can be seen that in case of a system without bad-data detection, the system experiences a drop of 50% of total load connected, which is significantly greater than the 10% loss of load if a bad-data detection strategy is in place. The three phases can be clearly identified, and the resilience of the system can be assessed. Table 3 shows the resiliency metrics with the bad-data detection, and without the bad-data detection for the two cases described in Table 2.

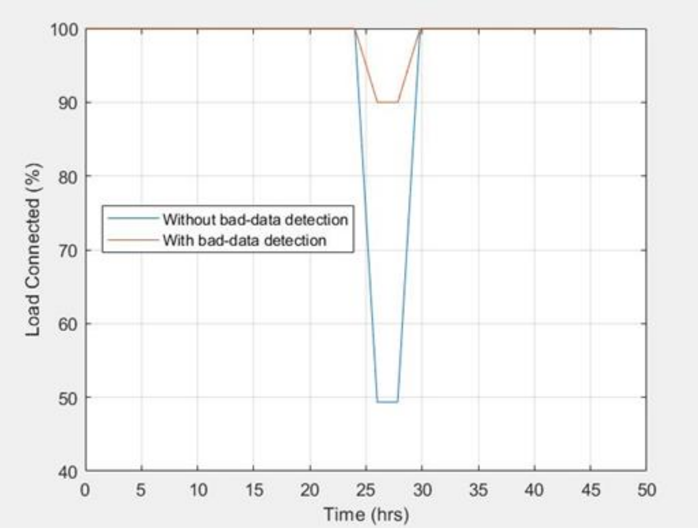

Figure 17 Load Connected (%) in progression of a cyber-attack.

Table 3 Resiliency of the system.

Phase	Expression	Without bad-data detection		With bad-data detection
		Case I	Case II	
Phase I: Disturbance progress	Φ(MW/hr)	24.84897	24.98939	4.983849166
Phase II: Post disturbance degraded state	EENS (MWhrs/int)	188.4839	368.3073	1.127783459
	E(hr)	1.824	5.458	1.995206871
Phase III: Restorative state	Π(MW/hr)	25.47656	25.95405	5.01201161

From Table 2 and Table 3, it is seen that all of the cyber-attacks are not the same. If the system gets a cyber-attack, it depends on identifying the problem and the cause of the problem. It shows that making a system resilient to cyber-attack is different than making a system resilient to a hurricane or a storm, because with cyber-attack, the recovery time can be significantly improved by identifying the problem. In case of hurricane or storm, identifying a problem does not necessarily improve the cyber-attack. Thus, resiliency investment in different type of event is going to be affected in different ways.

4. Conclusions

This paper presents a comprehensive study of the impact of a cyber-attack on the reliability and resiliency of a power distribution system. It presents a unique method to formulate cyber-attacks, and provides a methodology to quantify their impacts. A cyber-attack results in significant power outages as evidenced by the reliability and resiliency metrics presented in the paper. The probability of trouble is widespread throughout the system at all the load points. The frequency and severity of cyber-attacks are expected to rise as power-grids transition into cyber-physical systems. This suggests a need for proper investigation of the cyber-physical interdependencies and appropriate investment in system resilience against cyber-attacks. There is a lack of literature that provides a methodology and suitable modeling techniques to quantify the resiliency and reliability of a modern microgrid equipped with cyber-physical capabilities with the consideration of a false-data injection cyber-attack. Hence, such comparative study has not been done. However, our paper presents a methodology to quantify the implications of cyber-attacks on the reliability and resilience of such microgrids.

The resiliency indices framework- “Φ, E, EENS, Π” provides measures to assess the impact of an extreme event in time sequence at the different stages of a system, and therefrom, quantify the system’s ability to absorb, adapt and recover from the event. The presented results showed that the system degradation increased significantly with the delay in identifying the attack. An automated mechanism to rapidly identify the occurrence of cyber-attacks can enhance system resilience against such attacks. The presented studies also included an infrastructural resiliency enhancement strategy by implementing a bad-data detection algorithm to identify the behavioral changes in the system. The results showed significant improvement in system resiliency from such investment. It should be noted that resiliency investments for different type of HILP events are going to affect their impacts on the power system in different ways. Authorities and regulatory bodies should plan to invest accordingly to develop strategies as economically as possible in order to mitigate the impacts of such attacks and ensure a resilient power grid.

Author Contributions

Rajesh Karki: conceptualization, formal analysis, supervision, review and editing. Binamra Adhikari: methodology, software, detail analysis, writing original draft. All authors have read and approved the published version of the manuscript.

Competing Interests

The authors have declared that no competing interests exist.

References

1. Aleem SA, Hussain SS, Ustun TS. A review of strategies to increase PV penetration level in smart grids. Energies. 2020; 13: 636.
2. Nazir S, Hamdoun H, Alzubi J. Cyber-attack challenges and resilience for smart grids. Eur J Sci Res. 2015; 134: 111-120.
3. 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.
4. Nguyen T, Wang S, Alhazmi M, Nazemi M, Estebsari A, Dehghanian P. Electric power grid resilience to cyber adversaries: State of the art. IEEE Access. 2020; 8: 87592-87608.
5. Whitehead DE, Owens K, Gammel D, Smith J. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. Proceedings of the 2017 70th Annual conference for protective relay engineers (CPRE); 2017 April 03-06; College Station, TX, USA. Piscataway, NJ: IEEE.
6. BBC. Ukraine power cut 'was cyber-attack' [Internet]. London, UK: BBC; 2017. Available from: https://www.bbc.com/news/technology-38573074.
7. Smith R, Barry R. America’s electric grid has a vulnerable back door-and Russia walked through it [Internet]. New York, NY: The Wall Street Journal; 2019. Available from: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.
8. Ratnam EL, Baldwin KG, Mancarella P, Howden M, Seebeck L. Electricity system resilience in a world of increased climate change and cybersecurity risk. Electr J. 2020; 33: 106833.
9. Billinton R, Allan RN. Power-system reliability in perspective. Electron Power. 1984; 30: 231-236.
10. Holling CS. Resilience and stability of ecological systems. Annu Rev Ecol Syst. 1973; 4: 1-23.
11. Gautam P, Piya P, Karki R. Resilience assessment of distribution systems integrated with distributed energy resources. IEEE Trans Sustain Energy. 2020; 12: 338-348.
12. Liu X, Shahidehpour M, Li Z, Liu X, Cao Y, Bie Z. Microgrids for enhancing the power grid resilience in extreme conditions. IEEE Trans Smart Grid. 2016; 8: 589-597.
13. Moreno R, Panteli M, Mancarella P, Rudnick H, Lagos T, Navarro A, et al. From reliability to resilience: Planning the grid against the extremes. IEEE Power Energy Mag. 2020; 18: 41-53.
14. Mahzarnia M, Moghaddam MP, Baboli PT, Siano P. A review of the measures to enhance power systems resilience. IEEE Syst J. 2020; 14: 4059-4070.
15. Kundur D, Feng X, Liu S, Zourntos T, Butler-Purry KL. Towards a framework for cyber-attack impact analysis of the electric smart grid. Proceedings of the 2010 First IEEE international

conference on smart grid communications; 2010 October 04-06; Gaithersburg, MD, USA. Piscataway, NJ: IEEE.

16. Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid. Proc IEEE. 2011; 100: 210-224.
17. Wang W, Lu Z. Cyber security in the smart grid: Survey and challenges. Comput Netw. 2013; 57: 1344-1371.
18. Mitchell R, Chen IR. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv. 2014; 46: 1-29.
19. Inayat U, Zia MF, Mahmood S, Khalid HM, Benbouzid M. Learning-based methods for cyber-attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics. 2022; 11: 1502.
20. Khalid HM, Muyeen SM, Peng JC. Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach. IEEE Syst J. 2019; 14: 2054-2065.
21. Khalid HM, Qasaymeh MM, Muyeen SM, El Moursi MS, Foley AM, Tha'er OS, et al. WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks. IEEE Syst J. 2023; 17: 3950-3961.
22. Ali MZ, Haider SN, Sherazi HA. WAMS operations in modern power grids: A median regression function-based state estimation approach towards cyber-attacks. IET Gener Transm Distrib. 2021; 15: 1-12.
23. Roy SD, Debbarma S. Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid. IEEE Syst J. 2019; 14: 2023-2031.
24. Karimipour H, Dehghantanha A, Parizi RM, Choo KK, Leung H. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access. 2019; 7: 80778-80788.
25. Bahrami M, Fotuhi-Firuzabad M, Farzin H. Reliability evaluation of power grids considering integrity attacks against substation protective IEDs. IEEE Trans Industr Inform. 2019; 16: 1035-1044.
26. Venkataramanan V, Srivastava A, Hahn A. CP-TRAM: Cyber-physical transmission resiliency assessment metric. IEEE Trans Smart Grid. 2020; 11: 5114-5123.
27. Lin H, Chen C, Wang J, Qi J, Jin D, Kalbarczyk ZT, et al. Self-healing attack-resilient PMU network for power system operation. IEEE Trans Smart Grid. 2016; 9: 1551-1565.
28. Pasqualetti F, Dörfler F, Bullo F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. Proceedings of the 2011 50th IEEE Conference on Decision and Control and European Control Conference; 2011 December 12-15; Orlando, FL, USA. Piscataway, NJ: IEEE.
29. Jia H, Shao C, Liu D, Singh C, Ding Y, Li Y. Operating reliability evaluation of power systems with demand-side resources considering cyber malfunctions. IEEE Access. 2020; 8: 87354-87366.
30. Zhang Y, Xiang Y, Wang L. Power system reliability assessment incorporating cyber-attacks against wind farm energy management systems. IEEE Trans Smart Grid. 2016; 8: 2343-2357.
31. Venkataramanan V, Srivastava AK, Hahn A, Zonouz S. Measuring and enhancing microgrid resiliency against cyber threats. IEEE Trans Ind Appl. 2019; 55: 6303-6312.
32. Anshuman ZN, Sajan KS, Srivastava AK. ML-based data anomaly mitigation and cyber-power transmission resiliency analysis. Proceedings of the 2020 IEEE International Conference on

Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm); 2020 November 11-13; Tempe, AZ, USA. Piscataway, NJ: IEEE.

33. Choi IS, Hong J, Kim TW. Multi-agent based cyber-attack detection and mitigation for distribution automation system. IEEE Access. 2020; 8: 183495-183504.
34. Panteli M, Mancarella P, Trakas DN, Kyriakides E, Hatziargyriou ND. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Trans Power Syst. 2017; 32: 4732-4742.
35. Srivastava A, Morris T, Ernster T, Vellaithurai C, Pan S, Adhikari U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Trans Smart Grid. 2013; 4: 235-244.
36. Wood AJ, Wollenberg BF, Sheblé GB. Power generation, operation, and control. New York, NY: John Wiley & Sons; 2013.
37. Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur. 2011; 14: 1-33.