POWER DISTRIBUTION SYSTEM RELIABILITY AND RESILIENCY AGAINST EXTREME EVENTS

A Thesis Submitted to the College of
Graduate and Postdoctoral Studies
In Partial Fulfillment of the Requirements
For the Degree of Master of Science
In the Department of Electrical and Computer Engineering
University of Saskatchewan
Saskatoon, Canada

By

Binamra Adhikari

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying, publication, or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other use of the materials in this thesis in whole or part should be addressed to:

Head of the Department of Electrical and Computer Engineering
57 Campus Drive
University of Saskatchewan
Saskatoon, Saskatchewan S7N 5A9
Canada

OR

Dean
College of Graduate and Postdoctoral Studies
University of Saskatchewan
116 Thorvaldson Building, 110 Science Place
Saskatoon, Saskatchewan S7N 5C9
Canada

ABSTRACT

The objective of a power system is to provide electricity to its customers as economically as possible with an acceptable level of reliability while safeguarding the environment. Power system reliability has well-established quantitative metrics, regulatory standards, compliance incentives and jurisdictions of responsibilities. The increase in occurrence of extreme events like hurricane/tornadoes, floods, wildfires, storms, cyber-attacks etc. which are not considered in routine reliability evaluation has raised concern over the potential economic losses due to prolonged and large-scale power outages, and the overall sustainability and adaptability of power systems. This concern has motivated the utility planners, operators, and policy makers to acknowledge the importance of system resiliency against such events. However, power system resiliency evaluation is comparatively new, and lacks widely accepted standards, assessment methods and metrics. The thesis presents comparative review and analysis of power system resilience models, methodologies, and metrics in present literature and utility applications. It presents studies on two very different types of extreme events, (i) man-made and (ii) natural disaster, and analyzes their impacts on the resiliency of a distribution system. It draws conclusions on assessing and improving power system resiliency based on the impact of the extreme event, response from the distribution system, and effectiveness of the mitigating measures to tackle the extreme event.

The advancement in technologies has seen an increasing integration of cyber and physical layer of the distribution system. The distribution system operators avails from the symbiotic relation of the cyber-physical layer, but the interdependency has also been its Achilles heel. The evolving infrastructure is being exposed to increase in cyber-attacks. It is of paramount importance to address the aforementioned issue by developing holistic approaches to comprehensibly upgrade the distribution system preventing huge financial loss and societal repercussions. The thesis models a type of cyber-attack using false data injection and evaluates its impact on the distribution system. It does so by developing a resilience assessment methodology accompanied by quantitative metrics. It also performs reliability evaluation to present the underlying principle and differences between reliability and resiliency. The thesis also introduces new indices to demonstrate the effectiveness of a bad-data detection strategy against such cyber-attacks.

Extreme events like hurricane/tornadoes, floods, wildfires, storm, cyber-attack etc. are responsible for catastrophic damage to critical infrastructure and huge financial loss. Power

distribution system is an important critical infrastructure driving the socio-economic growth of the country. High winds are one of the most common form of extreme events that are responsible for outages due to failure of poles, equipment damage etc. The thesis models effective extreme wind events with the help of fragility curves, and presents an analysis of their impacts on the distribution system. It also presents infrastructural and operational resiliency enhancement strategies and quantifies the effectiveness of the strategy with the metrics developed. It also demonstrates the dependency of resiliency of distribution system on the structural strength of transmission lines and presents measures to ensure the independency of the distribution system. The thesis presents effective resilience assessment methodology that can be valuable for distribution system utility planners, and operators to plan and ensure a resilient distribution system.

ACKNOWLEDGEMENT

I owe my deepest gratitude to my supervisor Dr. Rajesh Karki for his invaluable guidance, motivation, and useful critiques during my studies at the University of Saskatchewan. His extensive expertise and vast experience were crucial to steer me in the right direction towards the completion of this work. I feel privileged to have had an opportunity to work under his supervision.

My sincere thanks goes to my graduate study professors, Dr. Rama Gokaraju, and Dr. Ha Nguyen for broadening my knowledge in the field of power systems, and statistics.

I am thankful to my colleagues: Mr. Prajjwal Gautam, Mr. Tej Krishna Shrestha, Mr. Mr. Asim Chaulagain, Mr. Safal Bhattarai, Mr. Bikash Poudel, Mr. Kiran Raj Timalsena, Mr. Shandesh Bhattarai, and Mr. Avishek Sapkota for sharing their knowledge and providing valuable suggestions.

I gratefully acknowledge the financial assistance provided by the college of graduate studies and research, the Department of Electrical and Computer Engineering and Natural Sciences and Engineering Research Council of Canada (NSERC) throughout my M.Sc. program.

Lastly, I am thankful to my parents for their encouragement and moral support

DEDICATION

To my beloved parents, ***Babita*** *and* ***Pitambar***

and

To my wonderful sister ***Prastuti***

Without whom none of my success would have been possible

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AGC	Area Generation Control
ASAI	Average Service Availability Index
CDF	Cumulative Distribution Function
CDG	Convention Distribution Generator
CDMP	Cyber-attack Detection and Mitigation Platform
CEA	Canadian Electricity Association
CPRM	Cyber-Physical Resiliency Metric
CP-SAM	Cyber-Physical Security Assessment Metric
DAS	Distribution Automation System
DER	Distributed Energy Resource
DFS	Depth for Search
DoS	Denial of Service
DPUI	Delivery Point Unreliability Index
DSO	Distribution System Operator
EENS	Expected Energy Not Supplied
ERIS	Equipment Reliability Information System
ESP	Electronic Security Perimeter
ESS	Energy Storage Systems
EUE	Expected Unused Energy
FDIA	False Data Injection Attack
GADS	Generating Availability Data System
HILP	High Impact Low Probability
HL	Hierarchical Level
ICT	Information and Communication
IoT	Internet of Things
IPS	Intrusion Prevention System
LOLE	Loss of Load Expectation
MCS	Monte-Carlo System
MDOA	Mean Duration of Attack

MILP	Mixed Integer Linear Programming
NERC	North American Reliability Corporation
NSERC	Natural Sciences and Engineering Research Council of Canada
PBR	Performance Based Regulation
PMU	Phasor Measurement Unit
PV	Photovoltaic
RPS	Reward Penalty Scheme
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Networking
TADS	Transmission Availability Data System
T-SAFI	Transmission System Average Frequency Index
T-SAIDI	Transmission System Average Duration Index
TTC	Time to Compromise
USB	Universal Serial Bus

CHAPTER 1: INTRODUCTION

1.1. Power System Reliability

Power systems serve the function of delivering electrical energy to consumers, as economically as possible, with an acceptable degree of reliability. The electricity generated at generation system is transported to the consumers through the transmission and distribution system facilities. Any random failures observed in this process can translate to huge financial loss and societal discomfort. These issues raise concerns over the reliability of the system and its quantification. The quantification of the degree of reliability has been majorly deterministic. However, deterministic quantification is not able to capture the inherent stochastic nature of the power system. Probabilistic quantification of the degree of reliability can incorporate stochastic behavior and uncertainties in quantitative reliability. Probabilistic power system reliability also provides useful information in system planning and operation to maintain the desired level of supply reliability at an acceptable cost.

A subdivision of power system reliability is shown in Figure 1.1. Adequacy[1] is the study of the existence of sufficient facilities within the system to satisfy the consumer load demand. Security[1]on the other hand is the study of the ability of the system to respond to disturbances that arises within the system.

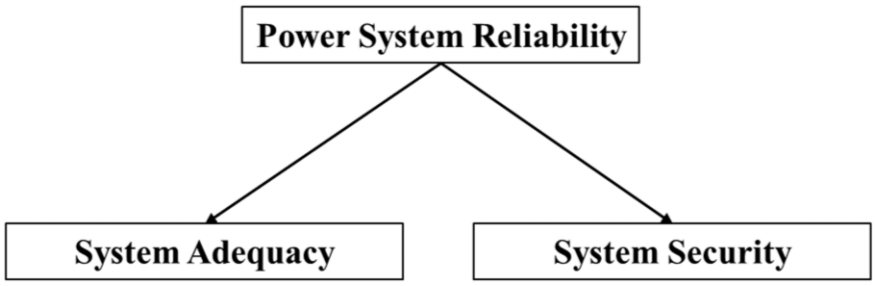

Figure 1.1 Domains of power system reliability

1.1.1. Functional Zones and Hierarchical Levels

A power system comprises of generation, transmission and distribution systems and is complex in nature. The evaluation of power system as a complete unit can be computationally burdensome. The power system is divided to hierarchical levels [2] using the three functional zones as shown in Figure 1.2. The first level or HL I is used to study the generation resources and the ability to satisfy the system demand. The second level or HL II is used to study composite generation and transmission system, and its ability to deliver energy to supply points. The third level (HL III) is used to address the power system, i.e. generation, transmission, and distribution as a complete unit. Predictive HL III reliability study is not done, but past performance reliability is carried out at HL III. Commonly carried out reliability studies based on the functional zones are (i) HL I reliability study, (ii) HL II reliability study, and (iii) Distribution system reliability study.

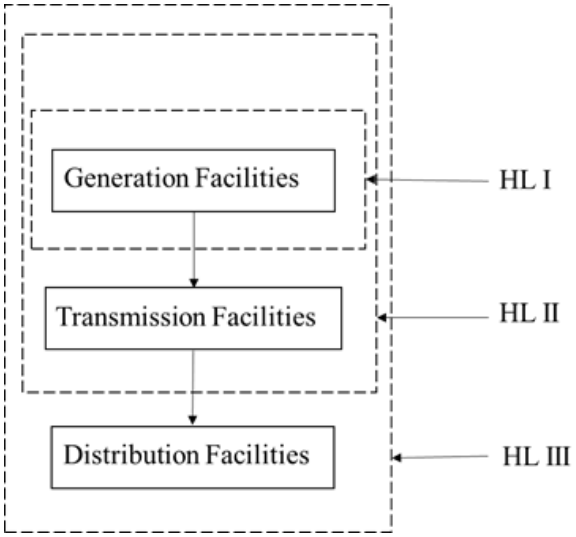

Figure 1.2 Hierarchical levels in power system reliability

There are two main approaches to assess the reliability of a power system. They are done by using analytical and simulation methods [1]. In analytical techniques, the system is represented by a mathematical model, and the reliability indices are evaluated from this model using direct numerical solutions. Unfortunately, assumptions made to simplify the problem in this case can cause the solutions to lose its significance when solving complex systems. Simulation methods on the other hand estimate the reliability indices by simulating the actual process and random behavior of the system. The method theoretically considers all aspects and contingencies inherent in the planning, design, and operation of a power system. Monte-Carlo Simulation are one of the best techniques used for reliability assessment based on simulation.

The simulation can be either random or sequential depending on the type of study required. The random simulation chooses the intervals at random, whereas the sequential simulates the intervals in chronological order. The research work presented in this thesis utilizes both sequential and random Monte-Carlo simulation.

1.1.2. Reliability Assessment of Distribution Systems

The reliability of distribution system can be assessed at both load point and system level. This is done evaluating three fundamental reliability indices. They are failure frequency(λ), average outage duration(r), and the outage probability or unavailability(U). These indices can be used to obtain additional customer oriented and load points indices in order to quantify the reliability of a distribution system. The system average interruption frequency index (SAIDI), system average interruption duration index (SAIDI), and the expected energy not supplied (EENS) are some of the commonly used system indices which can be obtained using (1.1)-(1.3)[1],[3].

$$SAIFI = \frac{\sum \lambda_i N_i}{\sum N_i} \quad (1.1)$$

$$SAIDI = \frac{\sum U_i N_i}{\sum N_i} \quad (1.2)$$

$$EENS = \sum L_{a,i} U_i \quad (1.3)$$

Where, $\lambda_i, U_i, L_{a,i}$, and N_i in (1.1)-(1.3) denote the failure frequency, annual outage time, load connected, and the number of customers of load point i, respectively. These indices can either be calculated using predictive reliability assessment, or from past performance assessment using outage data reported by the utilities.

Distribution systems are generally a part of a vertically integrated power system that connects the customers to the bulk power system [2]. The privatization and deregulation of power industries has transformed the market into a competitive design. As the objectives of the distribution system owners changed from “obligation to serve” to “maximize profits”, initial transformation provided little incentives to maintain the reliability of power supply acceptable to the customers. Many jurisdictions have started to implement different forms of performance based regulation (PBR) to safeguard the customers from high outage costs.

A reward/penalty structure (RPS) is also often incorporated in the PBR. It is based on the reliability performance of the distribution system. Figure 1.3 shows a general representation of RPS, where a selected set of reliability indices for the system are compared against pre-

specified criterion values. Table 1.1 shows the threshold values for the SAIFI and SAIDI indices for some major US utilities [4]. The DSO is rewarded if the reliability index is less than the threshold. Likewise, the DSO is penalized if the reliability index is more than the threshold [5]. There is no reward or penalty in the dead zone. The policy makers set the dead zone, penalty criteria, reward criteria, and the threshold considering the mix of customers served, geography, DSO's performance etc.

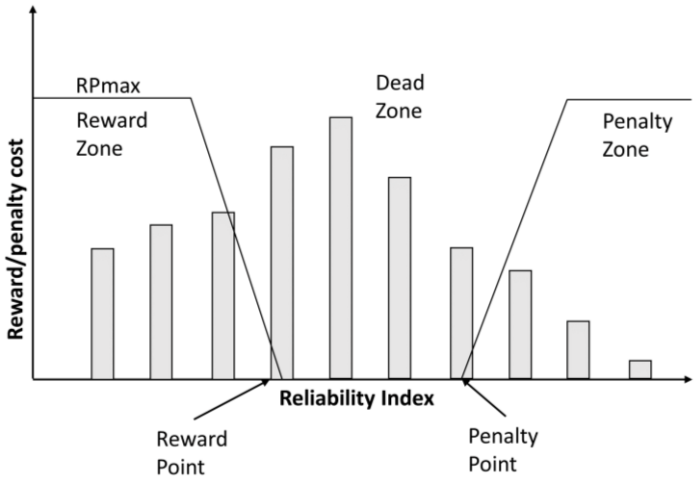

Figure 1.3 General reward/penalty structure

RPS is based on historical values. The mean values of SAIDI or SAIFI is taken and half standard deviation is left on both sides for reward and penalty zones. Some of the standard SAIDI, and SAIFI used in practice is shown in Table 1.1.

Table 1.1 Performance based regulation based on distribution reliability indices

Performance Measure/Utility	Standard
SAIDI	**Minutes**
Boston Edison	108.8
Commonwealth Electric	115.0
Energy Gulf States	158.0
Pacific Gas & Electric	145.0
PublicService Company of Colorado	79.0
San Diego Gas & Electric	52.0
Southern California Edison	55.0
SAIFI	**Number of Interruptions**
Boston Edison	1.040

Central Maine Power	2.000
Commonwealth Electric	1.484
Energy Gulf States	2.600
Maine Public Service.Company	3.100
Pacific Gas & Electric	1.480
San Diego Gas & Electric	0.900

The reliability of the supply of a distribution system to its customers plays an important role in steering the development of the region. It is also responsible for the socio-economic development of the society. Thus, the reliability concerns of the customers are taken into consideration in utility planning and operation. The PBR is a widely implemented mechanism that incentives investment in distribution systems to maintain acceptable reliability. These mechanisms, however, do not penalize DSOs for outages caused by "act of God" events, such as extreme weather, that can have devastating impacts on supply reliability. These events are therefore not considered in routine distribution system reliability studies or in data reporting procedures for RPS compliance. The following subsections describe the impact of these extreme events on distribution systems and the need for the systems to be resilient against such events.

1.2. Impact of Extreme Events on a Power System

Extreme events like hurricane/tornadoes, floods, wildfires etc. are dependent on the geographical peculiarities of the location. These events are responsible for catastrophic damage to critical infrastructures and huge financial losses. Power system is one of the most vulnerable critical infrastructure [6] that has constantly experienced failures due to the frequent occurrence of extreme events. Eight extreme-events related outages have been reported in the United States each with financial losses exceeding one billion U.S. dollars [7]. Thailand experienced an outage in 2013 that lasted for 10 hours and affected 8 million people due to a lightning strike [8]. A severe thunderstorm took place in Sri Lanka that resulted in a power outage, which affected 10 million people and lasted for 16 hours [8]. Table 1.2 is a summary of some of the impacts on distribution system due to climate change.

Table 1.2 Summary of impact on distribution system due to extreme event

Extreme Event	Distribution System

Extreme wind	Equipment damage (poles), changes to vegetation management
Severe floods	Risk of equipment damage
Wildfires	Prolonged system outages, equipment damages, changes to vegetation management
Hurricanes	Equipment damage, changes to vegetation management, cascading failures
Earthquake	Risk of quipment damage, prolonged system outages

The increasing climate change aggravates natural disasters. The occurrence of a particular type of disaster is dependent on the geographical peculiarities of the location. It is also dependent on the seasons. Most of all the earthquakes, and volcanoes occur along the Pacific Ocean's outer edges [9]. The United States has more tornadoes than the rest of the world combined. Landslides are more prone in the springs, whereas wildfire are common in the middle of summer and early fall.

Unlike natural disasters, distribution system are also affected by man-made extreme events. The integration of cyber-layer to the distribution system has introduced many interdependencies that are often exploited for personal gain of the perpetuators. The increased interaction of the cyber-physical layers of distributions system without proper risk evaluation of the vulnerabilities has resulted in the increasing occurrence of cyber-attacks. Ukraine observed such cyber-attack that affected 230 million people and led to an outage of 6 hours [8]. As the distribution system is moving to a more integrated cyber-physical system, distribution system planners and operators must be aware of both kinds of extreme events, and the resources available to them to tackle the events.

1.2.1. Extreme Winds in Power Systems

The National Weather Service of the USA defines extreme wind to be wind gusts higher than 58 mph[10]. Extreme wind of this ferocity and higher can rip apart houses, knock down poles, damage structures and cause threat to life in the vicinity of the event. Distribution systems consist of poles made of wood, steel and concrete carrying overhead lines connecting to hundreds of consumers. The damage to a distribution system can be catastrophic if a high

intensity extreme wind occurs. The outages due to natural disasters as shown in Figure 1.4 represents outages due to extreme winds. The extreme winds knock down poles disconnecting large number of users. The operators on the other hand are at tremendous amount of pressure due to the limited resource available to resume power supply to their customer.

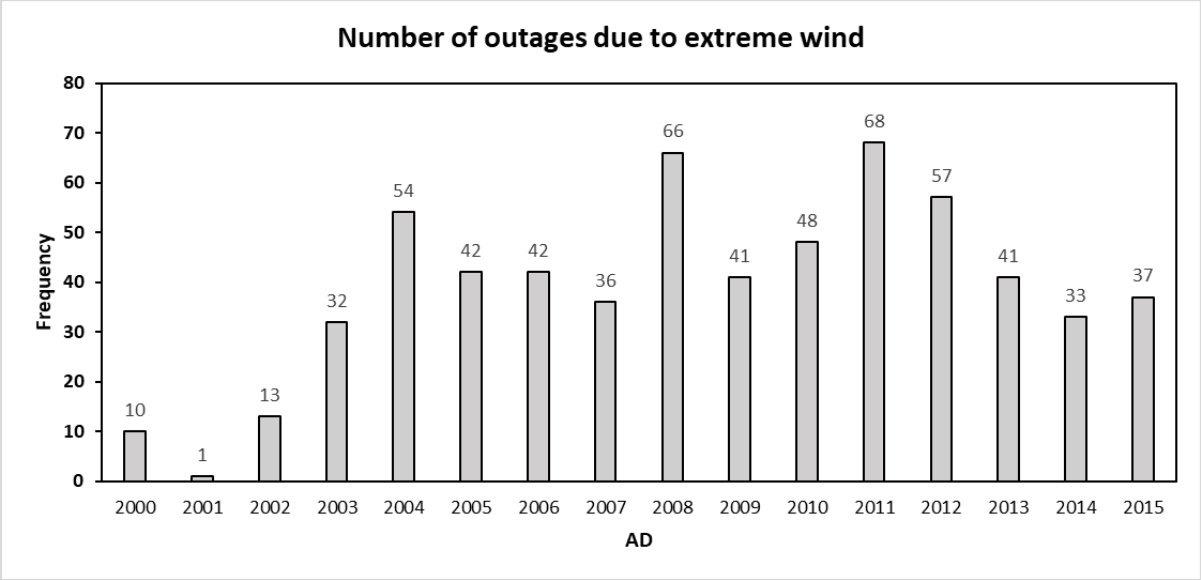

Figure 1.4 Frequency of outages due to extreme wind in the USA from 2000 to 2015

Distribution system reliability performance is usually measured by SAIFI, SAIDI and EENS. The IEEE Std. 1366 [11] described these indices and the type of interruptions that are reported to obtain them. However, utilities do not report outages due to extreme events, and therefore, the impact of extreme events are excluded from the reported reliability indices. Figure 1.7 represents one such comparison of the SAIDI index with and without considering the impact of the extreme windstorm that occurred in Eastern Canada in the year 1998 [12]. It can be seen that there was a ten-fold increase in the annual index due to power outages from the windstorm that resulted in huge economic losses. Although this impact is excluded in annual reliability reporting, the importance of assessing and improving the resiliency of the system to minimize the losses should not be ignored.

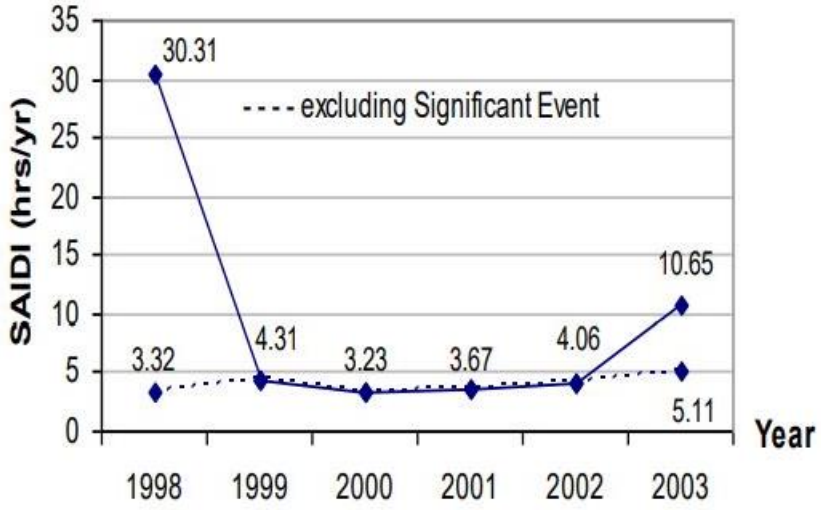

Figure 1.5 The SAIDI index from Annual CEA Report

Extreme winds are directly responsible for equipment damage, and losses to customers due to power outages, there are however other indirect damages as well. It should be noted that there are different categories of electricity consumers, such as industrial loads, commercial loads etc., which drive the region's economy. Prolonged deficit in electricity they receive creates ripples in the economy, whose effects can be seen in the form of price-rise of products or services consumer use, supply deficit of product or services consumer use etc. Both direct and indirect costs associated with an outage due to extreme wind are of concern to utility planners, which is why it is important to envision a reliable and resilient distribution grid to ensure a continuous supply of electricity that can prepare, absorb, adapt and recover from an extreme event.

1.2.2. Increasing Concern for Cyber-Attacks

The performance of modern society heavily relies on the strength of critical infrastructures in the region. Distribution system is an indispensable infrastructure that is responsible for supplying reliable electricity to variety of consumers. Distribution systems all around the globe are gradually transforming into smart-grids, with rapid growth in implementation of advanced sensors, intelligent automation, communication networks and information technologies. The integration of such smart technology with the existing distribution system infrastructure is a symbiotic relationship whose benefits are reaped by the utility operators [13]. The integration of cyber and physical layer provides a microscopic spectacle to observe the delivery of electricity.

Unfortunately, its strength can also be its Achilles Heel. A cyber-physical system introduces numerous access points that are vulnerable to malicious attacks with disastrous repercussions. The access point exploitation can be done through relays, dial-up models, RS-232 or Ethernet. The electronic security perimeter (ESP) generally has a firewall, but sometimes the inter-ESP link maybe wireless or may use leased bandwidth from a third party and can therefore be at risk of penetration. Malware too can be introduced through universal serial bus (USB), or infected software patches. It is also possible that a compromised computer could establish communication with outside attackers. After penetrating the network, the attack can be carried out in numerous ways. There are generally four overarching types of attack that all kinds of cyber-attack fall under [14]. They are reconnaissance, denial of service (DoS), command injection attacks, and measurement injection attacks. Reconnaissance is done before penetration to identify the weak points in the network. DoS and Command Injection Attacks both attack the commands, where DoS breaks the communication links whereas the latter masks the command with false information. Measurement Injection Attacks are also one of the most common form of attacks. The attacks that sends false or modified data by successful penetration of sensors are called are measurement injection attacks. False Data Injection Attacks (FDIA) are a form of this attack which is also explored in this thesis.

The transition of the distribution system to a smarter network has raised concerned over the occurrence and impact of aforementioned issues on the distribution system. These concerns accompanied by recent outages due to suspicious activities call for a resilient grid that can ensure the security of the network. The possible damage cyber-attack causes, and preventive measures against such extreme events are also explored in the thesis.

1.3. Power System Resiliency against Extreme Events

1.3.1. Resiliency and its Essence in Natural Science

The earliest definition of resiliency [15] dates back to 1970 by C.S. Holling where he defined resilience to be ‘the measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist.’ He discussed about resiliency and tied it with stability interpreting them as yin and yang of the ecological systems

Human psychology defines resiliency as the positive adaptation to adversity [16]. A human being is referred as resilient depending on the individual’s ability to cope with stress, and adversity. The definition of resiliency in infrastructural engineering is defined as the ability

to withstand acceptable degradation parameters and to recover within an acceptable time and costs [17]. The definitions may vary across different disciplines but the overarching essence has always been observed in different fields of natural science. Resiliency is the property that defines the ability of the system to prepare, absorb, and recover from any external event.

1.3.2. Power System Resiliency

Power system resiliency is the ability of a system to prepare, absorb, adapt and recover from extreme events. As global warming is rising, the increasing occurrence of natural extreme events has surprised and raised concerns over the resiliency of power system [18]. Each outage that a utility faces translates to huge financial loss, and societal discomfort [16]. Figure 1.6 shows the number of outages observed due to hurricane/tornadoes, floods, high winds, and cyber-attack between 2000-2015 [19].

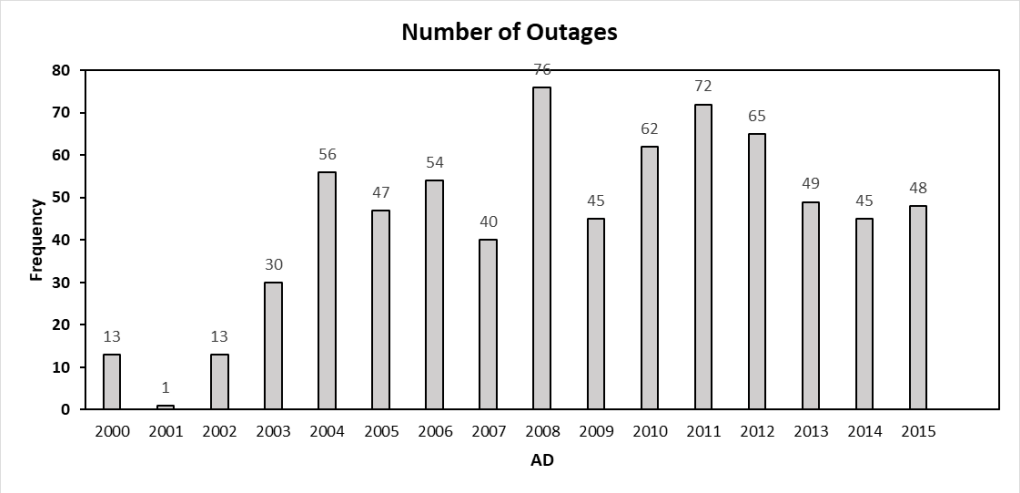

Figure 1.6 Number of blackouts observed from 2000 to 2015

The increasing outage is of concern to many utility planners and operators. These outages are not only responsible for financial losses, but are also responsible for the degradation of the distribution system infrastructure. Figure 1.7 shows the power outages causes from 1965 to 2012 [20]. The data suggests the importance of evaluating the resiliency of power systems against natural disasters, cyber-attacks, vandalism and other causes not routinely incorporated in annual reliability assessments.

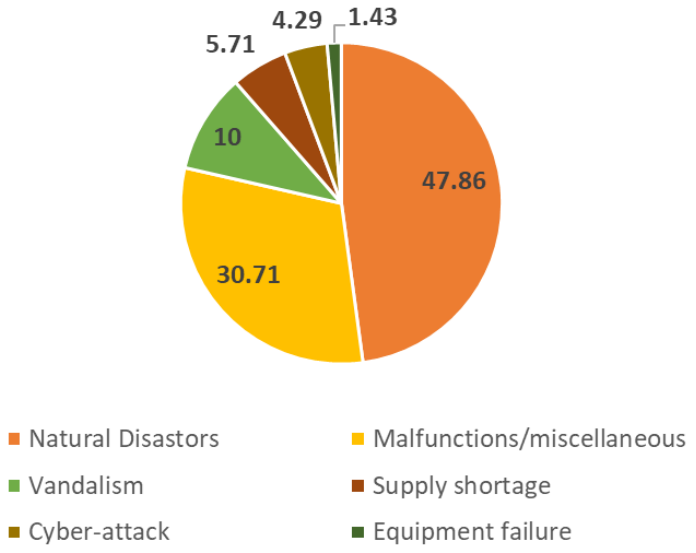

Figure 1.7 Power outage causes reported between 1965 to 2012

The increasing occurrence of cyber-attacks has raised concerns over the interdependency of the cyber and physical layer of the distribution system. In 2000, the Supervisory Control and Data Acquisition (SCADA) system of the sewage control system in Australia[21] was compromised. A cyber-attack penetrated a computer network at a nuclear plant in U.S[21]. Iran's nuclear fuel facility was attacked by a Stuxnet worm in 2010 [21] As stated earlier, the occurrence of these kind of extreme events and their mitigation strategies are not generally incorporated in routine reliability studies during the planning phase of utilities. The utilities lack a unifying framework to assess the resiliency of their systems against extreme events, and to decide appropriate investment strategies to withstand or mitigate their impacts in order to minimize the losses from such events.

1.4. Research Motivation and Objectives

Increase in outages of the distribution system due to increase in occurrence of natural and man-made extreme events like hurricane/tornadoes, flood, wildfire, landslides, storms, high winds, cyber-attack has raised public concerns as they result in significant economic losses to a society. Historical reports show that 80% of power outages experienced by customers are originated from the distribution system [22]. The performance of distribution system in extreme events has raised concern for the utility planners and operators. Moreover,

the degradation of equipment during extreme events has raised question over the strength, and adaptability of the distribution system

Routine reliability evaluations ensure outages are minimized but do not incorporate the occurrence of extreme events. There are market mechanisms in place to ensure utilities invest in minimizing outages but they cannot hold utilities accountable for outages caused by extreme events as these are external variables that do not reflect the performance of the utility. It is also too costly to invest with the objective to withstand such extreme events. The statistics show that these events have very low probabilities, which is also the reason it has gathered less attention from utilities in the past. However, the aftermath of extreme events on distribution system suggests that the distribution system is in need of comprehensive assessment frameworks, upgrade of policies, and deployment of necessary strategies to address the operating reliability of the system during extreme events.

The need for the operating reliability of the system that is catered for extreme events, and quantifies the adaptability of the distribution system has birthed resiliency. However, being in its infancy, resiliency has ambiguous approaches, and definitions. The unequivocal need for resilient distribution system has diverged into different streams, and brought confusion among utility planners and operators [18]. Many utility planners and operators are aware of the risk unprecedented extreme events have on the existing distribution system but do not have the necessary means, framework, policies and resource in place to tackle the extreme events.

Resiliency has spurred research interests among plethora of researchers in power systems. This has brought awareness among academia and industries in the field. However, being in its infancy, resiliency studies face ambiguous approaches, and interpretations. The unequivocal need for resilient distribution system has diverged into different streams, and brought confusion among utility planners and operators **Error! Reference source not found.**. Many utility planners and operators are aware of the risk of unprecedented extreme events on the existing distribution systems but do not have the necessary means, framework, policies and resource in place to properly assess, quantify and utilize the results to make appropriate decisions. Each extreme events like cyber-attack, hurricane/tornadoes, floods, wildfires are different, and has different consequences on the distribution system. The extreme event affecting a particular jurisdiction is also dependent on the geographical peculiarities, and the demographics of the place. Extreme winds are one of the most common form of natural disasters affecting North American regions. Moreover, as the world is transitioning into smart grid, the occurrence of cyber-attacks has considerably increased and raised concerns among power utilities and operators. Resiliency against these extreme events are important for

sustaining economic development and minimizing societal losses, but a gap can be felt as no common framework exits with quantitative indices that can be useful to utilities to make balanced investment decisions to achieve a reliable and resilient distribution system.

The thesis aims to provide a clear and concrete definition of resiliency, and discuss the challenges and opportunities of reliability and resiliency based on recognized research articles and reports. The thesis aims to develop a framework for resiliency assessment, quantify the impact on the distribution system, and provide strategies for resiliency enhancement, considering two different types of extreme events i.e. cyber-attack and extreme winds. The models are developed with the aim to provide a unifying framework that encompasses all of the properties of resiliency, along with guidelines for achieving a resilient distribution system. The specific objectives of the research work are summarized below:

- Development of clear and concise differences between reliability and resiliency, and its studies in the distribution system
- Development of a novel methodology to model cyber-attacks for analysis based on state-estimation
- Development of distribution system resiliency assessment model to assess the impact of FDIA, a type of cyber-attack with the help of expected EENS for cyber-attack
- Development of novel resilience evaluation framework including probabilistic extreme event model, resilience enhancement model, and resilience assessment model in presence of infrastructural and operational strategies, for a distribution system facing extreme wind

1.5. Thesis Organization

This manuscript-style thesis is organized into five chapters. All the chapters, except the first and the last, are papers submitted to technical publication. This section briefly describes the different chapters within the organization of this thesis.

Chapter 1 provides an overview of power system reliability and resiliency. It introduces power system, and the reliability studies done in power system. It discusses about the increasing modernization of the grid, and the reliability concern associated with it. It also presents studies to prove the increasing occurrence of extreme events on the distribution system. The chapter then moves ahead to show the present day distribution system, and its inability to face the extreme events. It then discusses about resiliency, and the importance of resiliency in the distribution system to protect the grid from natural and man-made extreme

events. The motivation for the research work and the objectives set in the thesis are also presented in Chapter 1.

Chapter 2 is extracted from the paper titled “Power System Reliability and Resilience: A Comparative Analysis of Challenges and Opportunities”. This paper has been presented in International Conference on Electric-Vehicle, Smart-Grid and Information Technology, ICESI 2020. This paper presents the foundation of reliability studies and some of the reliability practices until date. It presents the foundation of resiliency by establishing various literatures done to bring resiliency in distribution system. It then talks about the confusion between reliability and resiliency, presenting works done that claims resiliency studies but is more on the side of reliability, and vice versa. The paper then ends with a clear distinction between reliability and resiliency, and the need for resiliency in power systems.

Chapter 3 is a paper titled “Reliability and Resiliency Implications of Cyber-Attacks in Distribution Systems” submitted to the *IEEE Transactions on Smart Grid*. The paper starts by discussing the increasing modernization of the distribution system. The paper presents a comprehensive study of the impact of a cyber-attack on the reliability and resiliency of a distribution system. It presents a unique method to formulate cyber-attacks, and provide methodologies to quantify their impacts. It also includes an infrastructural resiliency enhancement strategy by implementing a bad-data detection strategy to identify the behavioral changes in the system. The study observes the response of the system on both the cases and draws definitive conclusions on the need of resiliency in modernizing distribution system.

Chapter 4 is a paper titled “Distribution system resiliency enhancement strategies against extreme wind”. The paper starts by discussing the present condition of the distribution system. It then moves ahead to discuss the increasing occurrence of extreme wind, and its impact on the distribution system. The paper develops an efficient framework to model the impact of extreme wind on the distribution system, and quantifies the resiliency in the system with the proposed indices. The paper discusses infrastructural and operational resilience strategies, and elaborates the impact of these strategies in the system facing extreme wind. The paper also discusses the use of DERs in improving the resilience of the system.

Finally, Chapter 5 presents the summary and conclusions of the thesis.

1.6. References

[1]. R. Billinton and R. N. Allan, Reliability evaluation of power systems, 2nd ed., Plenum Press, 1994

[2]. Billinton, Roy, and Ronald N. Allan. "Power-system reliability in perspective." Electronics and Power 30.3 (1984): 231-236.

[3]. Billinton, Roy, and Ronald Norman Allan. Reliability evaluation of engineering systems. New York: Plenum press, 1992.

[4]. Davis, Ron. "Acting on performance-based regulation." The Electricity Journal 13.4 (2000): 13-23.

[5]. R. Billinton and Z. Pan, "Historic performance-based distribution system risk assessment,"

[6]. IEEE Trans. Power Del., vol. 19, no. 4, pp. 1759-1765, Oct. 2004 E. Bartholameuz, H. Nazir and G. Doluweera, "Climate Impacts on Canada's Electricity Systems," Canadian Energy Research Institute, Calgary, AB, Study No. 196, 2021. URL: https://ceri.ca/assets/files/Study_196_Full_Report.pdf

[7]. Li, Zhiyi, et al. "Networked microgrids for enhancing the power system resilience." Proceedings of the IEEE 105.7 (2017): 1289-1310.

[8]. Haes Alhelou, Hassan, et al. "A survey on power system blackout and cascading events: Research motivations and challenges." Energies 12.4 (2019): 682.

[9]. National Geographic Society, "Plate tectonics and the Ring of Fire," National Geographic Society, 09-Oct-2012. [Online]. Available: https://www.nationalgeographic.org/article/plate-tectonics-ring-fire. [Accessed: 07-Feb-2022].

[10]. N. O. A. A. US Department of Commerce, "Wind threat defined," National Weather Service, 26-Feb-2021. [Online]. Available: https://www.weather.gov/mlb/wind_threat. [Accessed: 07-Feb-2022].

[11]. IEEE Guide for electric power distribution reliability indices, IEEE Std. 1366-2003.

[12]. R. Karki, Class Lecture, Topic: "Distribution System Reliability", Department of Electrical and Computer Engineering, University of Saskatchewan, Saskatoon, Dec, 2021.

[13]. Arghandeh, Reza, et al. "On the definition of cyber-physical resilience in power systems." Renewable and Sustainable Energy Reviews 58 (2016): 1060-1069.

[14]. Srivastava, Anurag, et al. "Modeling cyber-physical vulnerability of the smart grid with incomplete information." IEEE Transactions on Smart Grid 4.1 (2013): 235-244.

[15]. Holling, Crawford S. "Resilience and stability of ecological systems." Annual review of ecology and systematics 4.1 (1973): 1-23.

[16]. Doorn, N., Gardoni, P., & Murphy, C. (2019). A multidisciplinary definition and evaluation of resilience: The role of social justice in defining resilience. Sustainable and Resilient Infrastructure, 4(3), 112-123.

[17]. Wied, Morten, Josef Oehmen, and Torgeir Welo. "Conceptualizing resilience in engineering systems: An analysis of the literature." Systems Engineering 23.1 (2020): 3-13.

[18]. Panteli, Mathaios, and Pierluigi Mancarella. "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies." Electric Power Systems Research 127 (2015): 259-270.

[19]. Mukherjee, Sayanti, Roshanak Nateghi, and Makarand Hastak. "Data on major power outage events in the continental US." Data in brief 19 (2018): 2079.

[20]. Bie, Zhaohong, et al. "Battling the extreme: A study on the power system resilience." Proceedings of the IEEE 105.7 (2017): 1253-1266.

[21]. Liang, Gaoqi, et al. "A review of false data injection attacks against modern power systems." IEEE Transactions on Smart Grid 8.4 (2016): 1630-1638.

[22]. Chowdhury, A. and D.O. Koval, Value-based distribution system reliability planning. IEEE Transactions on Industry Applications, 1998. 34(1): p. 23-29

CHAPTER 2: POWER SYSTEM RELIABILITY AND RESILIENCE: A COMPARATIVE ANALYSIS OF CHALLENGES AND OPPORTUNITIES

2.1. Abstract

Power system reliability is a well-defined subject of study in engineering practice with established quantitative metrics, regulatory standards, compliance incentives and jurisdiction of responsibilities. Growing concerns over severe power outages due to catastrophic events such as hurricanes, floods, ice storms, earthquakes, geomagnetic disturbances, cyber-physical attacks, which are not considered in routine reliability evaluation have motivated power utilities and policymakers, and regulators to acknowledge the importance of system resilience against such events. In contrast to reliability study, power system resilience is a relatively new area of study lacking widely accepted standards, assessment methods or metrics. This paper presents comparative reviews and analysis of power system resilience models, methodologies, and metrics being currently proposed and discussed in available literature and utility applications.

2.2. Introduction

The objective of a power system has conventionally been to provide electricity to its customers as economically as possible with an acceptable level of continuity and quality [1]. With the growing concerns on the adverse environmental impacts of electricity generation, the environmental sustainability is also recognized as an important objective. Power outages are inevitable, and can result in significant adverse economic and social impacts to the end users as well as to the utility supplying the power. Therefore, regulatory authorities must ensure that power utilities continuously make adequate investment in their systems to provide reasonable assurance of supply reliability to their customers such that the overall societal cost is minimized. Such investment decision requires routine reliability assessment during system planning and operation. Power system reliability is a well-defined subject of study in

engineering practice with established quantitative metrics, regulatory standards, compliance incentives and jurisdiction of responsibilities.

Reliability studies, in general, do not consider the effects of very low probability events such as hurricanes, floods, ice storms, earthquakes. The accountability of such "Act of God" events are ignored in many other applications as well. Such events, however, cause severe power outages resulting in huge financial and societal losses, and are recognized as high impact low probability (HILP) events. For example, Hurricane Sandy in 2012 caused severe power outages for millions of people in the US north-eastern states. In 2011, 4 million customers suffered power outage for more than seven days due to an earthquake in Japan. A snowstorm in southern China in 2008 left 14.6 million customers without power. These statistics show that the extreme weather events are occurring more frequently. Moreover, within the envisioned framework of smart-grid, future power systems are expected to function as cyber-physical dependent systems deploying increased automation and smart technologies that utilize information from widely distributed and complexly interlinked components and sub-systems. These power systems will be vulnerable to malfunction of such interlinked components or processes, which can occur due to random hardware/software failures, and also from malicious cyber-attacks. These can also lead to widespread power outages. There is no consensus on whether these events should be included in reliability assessment, and regulatory requirements. But no one would disagree that future power systems should not only be able to economically deliver reliable power supply to electricity consumers while meeting environmental commitments, but also be adequately resilient to withstand or recover from widespread outages caused by natural disasters, inherent inter-related malfunctions and potential malicious attacks. Resilience, in context of a power system, is a relatively new area of study lacking widely accepted standards, assessment methods or metrics.

2.3. Power System Resiliency

The increased interest in the resiliency of power systems against HILP events has spurred research and related investigative work within the power utilities and associated organizations. Such activities carried out through independent and collaborative approaches have led to somewhat fuzzy understanding of the term "resilience" and its utility in power system planning and operation. It is not surprising that different stakeholders of energy systems have their individual perspective of resiliency. Moreover, as the concept of resiliency has become the forefront for creating an adaptive, sustainable environment, various definitions has

emerged. Addressing the dynamic behavior of resilience that a system portrays, [2] defined resiliency as the measure of persistence of system and of their ability to absorb change and disturbance, and still maintain the same relationship between population and state variable. With the aim of addressing resiliency at an asset/facility level and regional/community level, resiliency is defined as the ability of an entity - asset, organization, community, region - to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance [3]. The Presidential Policy Directive 21 has defined resilience as, "The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents" [4]. The concept of resilience has been interpreted from different perspectives. There are, however, certain similarities in the definitions that have been used to describe power system resiliency. Some of the definitions are shown in Table 2.1

Table 2.1. Power system resiliency definitions over the years

Date	Description	Reference
2011	Resilience is the capacity of an energy system to tolerate disturbance and to continue to deliver affordable energy services to consumers. A resilient energy system can speedily recover from shocks and can provide alternative means of satisfying energy service needs in the event of changed external circumstances.	[5]
2011	The resilience of a system to a class of unexpected extreme perturbations is defined as the ability of this system to (i) gracefully degrade its function by altering its structure in an agile way when it is subject to a set of perturbations of this class and (ii)quickly recover it once the perturbations ceased	[6]
2013	Robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event	[7]
2016	Resilience is the system's ability to endure disturbing events in two ways: by absorbing disturbances	[8]

Date	Description	Reference
	(“absorbing potential”) and by recovering from disturbances (“recovery potential”). Resilience implies that the system can absorb disturbances, adapt to the new parameters, and recover fast enough to mitigate the effects of the disturbing event.	
2016	Resiliency includes the ability to harden the power system against—and quickly recover from—HIGH-IMPACT, LOW-FREQUENCY events	[9]
2018	The ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event	[10]

The definition of power system resiliency over the years has metamorphosed into the attribute of a system that reflects its ability to withstand high-impact, low probability event, and recover from the consequent situation. Power system resilience is associated with the impact on the system whereas power system reliability is often catered for evaluating the impact on customers. Power system reliability and resiliency albeit being related to power outages differ in the causes that result in an outage. Power system resiliency is focused on creating a system that can remain functional on the occurrence of such event and recover rapidly to avoid further catastrophic repercussions on the power system and severe societal impacts on the customer. The fundamentals of both reliability and resiliency are concerned with planning and operation to minimize the overall societal cost. In an electrical market, there are well-established reliability reward/penalty measures and governing frameworks, such as those accepted by NERC in the North American jurisdictions. It can be argued if similar performance based incentive models should be established to stimulate investment in system resiliency.

The proper functioning of modern society heavily relies on the electric grid. On the contrary, there are significant documented articles from [11, 12] that demonstrate an increasing rise of unprecedented events; both natural and man-made, to conclude that the present-day power systems are ill-prepared to adapt to the increased disruptions due to extreme events.

Changing climatic conditions are primarily associated with these outages but increasing technological complexity and interconnectedness have greatly exacerbated the severity of these outages [13]. Recent years has also seen significant advancement in sensors, automation, communication network, and information technologies. The integration of these technologies has introduced increasing interconnections and interdependencies between the cyber and physical components of the grid [8]. This has resulted in an increase in cyber intrusion access points [14]. Reference [8] discusses the in-depth ramifications of the technological interconnectedness in the electric grid. The importance of resiliency in the coming years is reflected by the report from [15] where two major findings were observed through the data collected from various utilities in the NERC region. Extreme weather events were seen to be leading contributors in transmission and generation, followed by the increase in evolving cyber and physical threats.

Reliability and resiliency are related characteristics of a power system, and the distinction between the two are often vague. However, there is limited reported work that intends to provide clarification with comparative analysis between reliability and resiliency. Power system reliability is an extensively researched and quantifiable subject matter. On the contrary, resiliency related research and applications are relatively immature, and lacks widely acceptable quantifiable framework to evaluate this behaviour. Nevertheless, the electric grid remains susceptible to the events possibly resulting in disastrous consequences. The development of a proper framework, policies that address these issues is imperative. In this regard, the paper presents a comparative analysis of reliability and resilience models and metrics and their practices aiming to clarify the similarities and distinctions between them.

2.4. Reliability Practices

Power system reliability is well-established and widely accepted practice by power system planners, operators, regulatory authorities, and policymakers. In general, power system reliability is subdivided into two basic aspects of system adequacy and system security. Adequacy refers to the existence of sufficient facilities within the system to satisfy customer load demand, whereas, system security relates to the ability of the system to respond to the disturbances arising within that system [16]. A large amount of research has been done focusing on the adequacy assessment of power system as it contributes to optimal investment decisions in energy recourses and infrastructure of the utilities [33]. Generally, adequacy assessment is categorized in terms of their application in the the different hierarchical levels (HL) of

generation, transmission and distribution facilities of the power system as shown in Figure 2.1 [1]. The assessment of power system reliability has two approaches: deterministic and probabilistic. Deterministic approaches, such as the (N-1) criteria often result in widely inconsistent risks in comparable systems and scenarios [1]. System behaviour being stochastic in nature is more accurately assessed using probabilistic methods.

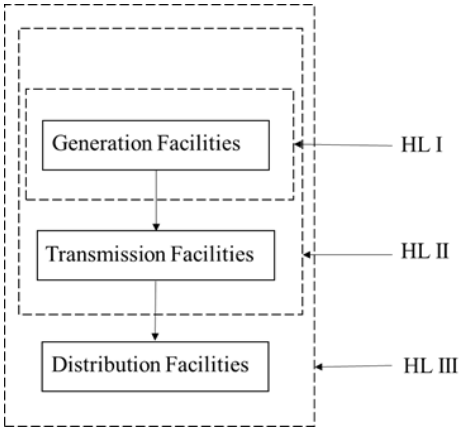

Figure 2.1 Hierarchical Levels of Power System

Table 2.2 describes the reliability evaluation tasks at various levels, and the quantitative metrics that are widely used by utilities [16, 17]. The loss of load expectation (LOLE) and the expected unused energy (EUE) are widely used probabilistic reliability indices at the HL I level. These indices are widely used in adequacy studies for generation planning. The LOLE is the expected number of days of load curtailment in a given period. The EUE is the expected energy that will not be supplied by the system due to load curtailment. The transmission-SAIFI (T-SAIFI), transmission-SAIDI (T-SAIDI), and delivery point unreliability index (DPUI) are some of the indices used to measure the adequacy of a bulk system. The T-SAIFI is the average frequency of power interruptions at the bulk load delivery point. The T-SAIDI is the expected number of hours of power outage at a delivery point of the bulk system. The DPUI reflects the overall bulk electricity system performance in terms of a composite index of unreliability expressed in system minutes in a year [18]. Reference [17] defines the reliability indices that are commonly used by the utilities for distribution system reliability evaluation. The system average interruption frequency index (SAIFI), system average interruption duration index (SAIDI), and the average service availability index (ASAI) are the commonly used sustained interruption indices for a distribution system. The SAIFI indicates how often the average customer experiences a sustained interruption over a predefined period [17]. The ASAI is the probability that a customer connected to the distribution system is interrupted. The SAIDI is the ASAI expressed in hours per year. In the North American jurisdictions, the NERC is

responsible for developing reliability standards to which all bulk-power system owners, operators, and users must comply. The NERC uses violation risk factor and violation severity level as defined in [15] to define penalty, and is responsible for taking necessary actions to ensure the necessary steps are taken by all of the participating bodies to maintain the reliability standard of a power system.

Table 2.2. Reliability Evaluation and Indices

Evaluation	Description	Indices Used
HL I or Generation Adequacy	Ability of the overall generating system to satisfy the system demand in a period under study	LOLE, EUE
HL II or Bulk System Reliability	Ability of the system generation and transmission system to generate and deliver the required power at the bulk load points	T-SAIFI, T-SAIDI, DPUI,
Distribution System Reliability	Ability of the distribution system to satisfy the connected loads	SAIFI, SAIDI, ASAI

An accurate reliability evaluation requires relevant and reliable data of the system behaviour. Utilities maintain logbooks of various types of data associated with the system operation, specific performance, repair and maintenance. Many utilities are aware of data collection schemes for reliability evaluation, and participate in reliability data compilation and reporting activities, such as the equipment reliability information system (ERIS) of the Canadian Electricity Association (CEA). Power utilities in the United States participate in providing generation and transmission reliability data respectively through the Generating Availability Data System (GADS) and the Transmission Availability Data System (TADS) within their NERC jurisdictions. The NERC and CEA have well-established data collecting and reporting systems that annually publish and disseminate power system reliability data.

2.5. Overlapping Area between Reliability and Resiliency

Resilience studies are mainly scoped to assess the adverse effects of high-impact, low probability events, such as extreme weather events, on power systems. It should, however, be noted that past literature is available in reliability modelling of extreme weather events and the impact on system reliability. In fact, IEEE 346 standard categorizes weather conditions into

three types namely: normal weather, adverse weather, and major storm disaster [17] to provide guidelines in reliability assessment incorporating extreme weather events. Reference [19] uses a 2-state model where the weather alternates between normal and severe conditions and their failure rates are evaluated using the Markov process. Reference [20] explore the use of a 3-state model and observe the change in the failure rate and repair time by subjecting the variables to a change in the percentage of failures that occurs in different weather conditions. Reference [21] highlight the effect of adverse weather conditions on transmission and distribution lines using consumer and load-oriented reliability indices and a 3-state weather model.

In addition to the reliability research reported above, recent literature also includes work done on the resiliency of power systems in extreme weather conditions. Reference [22] introduces a closed-loop distribution system restoration tool. It discusses achieving resiliency as a closed-loop process where data obtained from the weather forecast, system fragility assessment, SCADA, etc. is interpreted through a probabilistic estimation function indicating damage of the grid that is fed in the framework. Reference [23] provides a quantitative framework for resiliency evaluation of distribution system against extreme events using parameters like the probability of the number of hazard events that occur annually, the severity of hazard event, duration of a hazard event, and its impacts on the grid. The resiliency is expressed in percentage and does not express the consequences of an event but rather focuses on possibilities of disruption and its modelling. Reference [24] shows how increased automation in a distribution system can improve its resiliency. Several switches are replaced by remote-controlled switches and an extreme event is simulated to support the argument projected by the paper. The difference in these systems is reflected through indices like SAIFI and SAIDI. These are however well established reliability indices, and their use in resiliency studies often creates ambiguity in their applications. A large number of articles are available in published literature that overlap the domains of reliability versus resiliency studies, and make use of models and indices across these two domains. This creates not only confusion among researchers and industry personnel working in these areas, but also shows conceptual gaps in the contribution and utility of many such works. It can be argued that the lack of unifying regulations or articulated policies that distinguish between reliability and resiliency has misguided many researchers and utilities.

The technological evolution of the electric grid over the years is transitioning into a cyber-integrated network. 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 various access points that are vulnerable

to malicious attack with- disastrous repercussions. The largest blackout in Ukrainian power system due to cyber-attack was reported in the year 2015 [25]. One of the earliest known cyber-attack dates back to 2010 where “Stuxnet worm” attacked the SCADA system of a nuclear power plant in Iran [26]. Exploring and resolving the nature of this problem requires a pragmatic approach. It is necessary to evaluate the reliability of the cyber-physical power system to minimize failures introduced by the increase in interconnectedness between the cyber and physical layers of the power system. Reference [28] proposes a vulnerability index to demonstrate the impact of an Aurora Attack. Reference [29] expresses reliability and availability to be the features that gives a measure of resiliency. The ambiguous approach to resiliency has produced various articles that demonstrate this confusion between reliability and resiliency. A coherent understanding in difference between assessing reliability and resiliency of low-probability, high-impact events is required. Therefore, it is imperative to develop policies and regulations that attempts to clearly distinguish between reliability and resiliency, and provides distinct guidelines for researchers and industry experts to work and produce useful outcomes in the respective domains.

2.6. Resilience Trends

The various definitions of resilience imply the need to understand the behaviour of the system before, during, and after an extreme detrimental event. Energy system planners, operators, and regulatory authorities have struggled to anticipate such events, and to make the power system more resilient to these events. It is not economically feasible to provide a comprehensive upgrade to the entire power system in order to make it completely disaster-resistant [11]. Most power systems operate adhering to the (N-1) contingency complying with the established reliability guidelines. However, high-impact low-probability events have unanticipated repercussions in the electric grid resulting in an (N-X) contingency scenario [14]. Resiliency aims to address these issues, providing alternative means to the utilities to face such events. However, a comprehensive understanding of the behavior of the power system is required to come up with any conclusions to make the power system adequately resilient. So, it is imperative to recognize the stages that the grid goes through in the occurrence of an extreme event. The multi-phase resilience trapezoid model shown in Figure 2.2 [31] is used by many researchers to assess the resilience of power system in different stages of the event, and is also identified by the IEEE as a temporal resilience diagram [10].

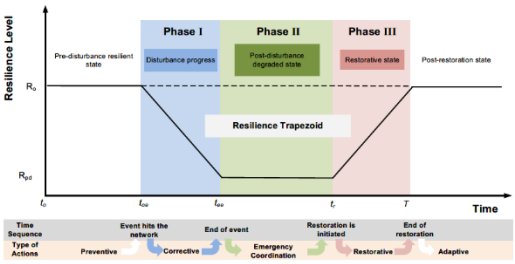

Figure 2.2 Multi-phase resilience trapezoid

There has been an appreciable amount of research work to assess the resilience of power systems. These works are broadly categorized under qualitative and quantitative evaluation of the power system.

2.6.1. Qualitative Resiliency Evaluation

Majority of the work done in qualitative resiliency assessment of power system involve two basic tasks of analysing the system in light of the extreme event(s) and assessing its capabilities to withstand or recover from such events, before producing an evaluation framework [11]. The capabilities include strategies that complement the resilient behaviour of the system, such as infrastructure endurance, preparedness, and resources for mitigation, response, and recovery. Qualitative assessment of resiliency has been performed using different evaluation frameworks, some examples being a matrix-based scoring methodology, and a checklist for questionnaires. Some of these evaluation frameworks are discussed in this section.

Reference [8] identifies resilience assessment to be a three-stage process where the system is first identified before carrying out a vulnerability analysis. The three stages are “before”, “during”, and “after” the extreme disturbance event in chronological order. After performing the vulnerability analysis of the system, the recovery and absorbing potential is assessed. Reference [13] propose a matrix-based evaluation approach for the resiliency of power system. It incorporates the tasks associated with the four stages of an extreme event identified by [33], namely plan/prepare, absorb, recover and adapt. The qualitative assessment methodologies can serve as useful references in the development of quantitative resiliency evaluation frameworks.

2.6.2. Quantitative Resiliency Evaluation

A majority of quantitative evaluation of resiliency is event-specific and does not intend to cover all possible extreme events, or their impacts on the entire power system. Both the absolute and the relative metrics have been used to quantify system resilience. Reference [30] state that a resiliency metric should be a probabilistic assessment of the consequences to extreme events. Reference [31] developed a new resilience measurement index called ΦΛΕΠ (pronounced as "flep") to capture the degradation of the power system in each of the three phases of an extreme windstorm event as shown in Figure 3. The Φ, and Λ is a measure of how fast and how low the resilience has dropped on the occurrence of an event. The E measures the extensity of the post-disturbance degraded state and the Π measures the promptness in recovering the network. Reference [27] used a simulation-based method to quantify resiliency and also identified the improvements using microgrids and DERs. Reference [32] quantified the resilience of a distribution network using three metrics namely the expected probability of interruption, expected outage duration and expected energy not served during the extreme event. Their resilience evaluation framework embedded a wind-induced extreme event generating model, damage assessment model and an optimal restoration model utilizing DER. Utilities face a difficult time dealing with unexpected power outages. Infrastructure reinforcements, such as strengthening the transmission poles and using underground cables, contribute to improve the resiliency but cannot always prevent unprecedented failures. There are critical load points that rely on a continuous supply of power. Utilities have explored alternatives like microgrid operation, utilization of distributed energy resources to maintain an uninterruptible supply of load. However, different deployment techniques for load restoration or the time required for restoration translates into different financial scenarios that the utilities have to look into. There are various literature in this particular area that contributes to quantitatively evaluating resiliency. Reference[11] discusses in-depth about the effectiveness of the proposed load restoration framework in creating a resilient grid.

Resiliency enhancement strategies differ in their applications. In the occurrence of an extreme event, there are different strategies involved that focus on the operational and infrastructural aspects in restoring the power system to its normal state. Strategies involving reconnecting the consumer with electricity before the affected part being repaired generally play out in practical scenarios suggesting a clear distinction between infrastructural and operational resilience.

Operation resiliency is more concerned with the task at hand. This includes reducing the magnitude and frequency of outages and customers affected. Infrastructural resilience focuses on planning measures for infrastructure hardening. Table 2.3 and Table 2.4 show examples of key strategies and remedial measures that can be taken to improve operational resilience and infrastructural resilience respectively in a power system [34-36].

Table 2.3. Operational resilience strategies and measures

Strategies	Remedial Measures
Maintaining supply to consumers with alternate options	Application of Microgrids and DER Installation of portable and mobile power generators Proper mobilization of on-site crews
Minimizing adverse impacts during the the extreme event	Optimizing load restoration, time-to-restoration framework Accurate extreme event modelling

Table 2.4 Infrastructural resilience strategies and measures

Strategies	Remedial Measures
Increasing structural strength and robustness	Equipment repair/maintenance Strengthening poles/towers Replacing overhead lines with underground cables
Increasing resistivity of power system preserving individual component functionality	Vegetation management Elevating substation to prevent floods

2.7. Opportunities and Challenges

Resiliency and reliability concepts in a power system have definitive distinctions despite having relevant fundamentals. Resiliency studies focus on all high-impact, low probability events that are normally excluded from reliability calculations [10]. During the resiliency assessment of a power system, the sequential impacts and the remedial measures to be taken during the transition between the states following an extreme event are particularly of interest [10]. Reference [30] proposed a decision-control architecture that would provide future

system states or trajectories differentiating itself from reliability metrics. The assessment is done for events that are highly uncertain in nature and result in (N-K) contingencies [11]. Moreover, investment decisions differ according to the need of the utility considering reliable or resilient options.

Reference [8] has identified the lack of sophistication to observe the interdependency between the system levels and the integration of concepts of Internet of Things (IoT) with distributed energy resources to be the major challenges during assessing the resiliency of a cyber-physical system. One of the major challenges in resiliency evaluation also remains the modelling of extreme events due to lack of historical data [8] related to these events or the usability of the data for future prediction given the event's stochastic nature.

Recognizing the increase of renewable energy mostly connected as distributed generation, [9] has revised a series of IEEE standards for distributed energy resources (DER) interconnection and interoperability with the grid. However, there is lack of unifying regulation and policies that are required to facilitate the interconnection of micro grid along with guidance for overcoming resilience oriented challenges in power systems [35]. A comprehensive understanding of the behavior of the participants of the market is required to provide short-term and long-term resilient strategies. The technological revolution and privatization of the energy market have skewed the interest of utilities towards financial benefits. With the increase in the penetration of renewables and the advent of the cyber-physical grid, a challenge will be the study of consumer-behavior and unbiased formulation of policies and mechanisms that adhere to the rudimentary concepts of reliability and resiliency and provides a check and balance with counteractive penalty measures.

2.8. Conclusion

The increase in high impact, low probability events, and its effect on the grid have been observed and accepted by power system planners, operators, regulatory authorities, and policymakers. This calls for a unanimous understanding of the fundamentals of power system resiliency and the development of standards and frameworks that all of the utilities can comply with. Power system resilience metrics should not only be a reflection of the state of the system but should also be able to capture the time duration and extremity of the event. This paper provides a review of the definition and governing principles of resilience in the power system. The increasing interconnectedness and advent of the cyber-physical era and its effect on the grid are also discussed. In distinctions between reliability and resiliency, it is important to

address the previous works done in light of the evaluation of the reliability of the power system in extreme events that at the present have fallen under the scope of resiliency. Power system resiliency evaluation greatly depends on the type of event and as event are recognized as high impact, low probability events, it is difficult to obtain abundant data. Even if such data is available for a specific extreme event, it is likely unusable considering the nature of the events. It is also understood that an increase in energy literacy on an individual level and better interactions with the utilities at a communal level can help overcome challenges associated with anticipating consumer's response and their responsibilities as a part of a resilient grid. An appropriate definition and common understanding of resilience and the relationship between reliability and resilience is imperative and will help the development of resilience models and metrics contributing to building reliable and resilient power system that delivers electricity with acceptable quality, continuity, and environmental compliance.

2.9. References

[1]. R. Billinton en R. N. Allan, “Power-System Reliability in Perspective.”, IEE Review, vol 30, no 3, pp 231–236, 1984.

[2]. C. S. Holling, “Resilience and stability of ecological systems”, Annual review of ecology and systematics, vol 4, no 1, pp 1–23, 1973.

[3]. L. Carlson et al., “Resilience: Theory and Applications”, Anl/Dis-12-1, no January, pp 1–42, 2012.

[4]. P. P. Directive, “Critical infrastructure security and resilience. PPD-21, Released February 12, 2013”. 2013

[5]. M. Chaudry et al., “Building a resilient UK energy system”, 2011.

[6]. L. Mili en N. V. Center, “Taxonomy of the characteristics of power system operating states”, in 2nd NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop, 2011, pp 13–15.

[7]. M. Keogh en C. Cody, “Resilience in regulated utilities. National Association of Regulatory Utility Commissioners (NARUC)(2013)”. 2021.

[8]. R. Arghandeh, A. Von Meier, L. Mehrmanesh, en L. Mili, “On the definition of cyber-physical resilience in power systems”, Renewable and Sustainable Energy Reviews, vol 58, pp 1060–1069, 2016.

[9]. EPRI Staff, “Electric Power System Resiliency”, Electric Power System Research Institute (EPRI), 2016.

[10]. A. Stankovic, “The definition and quantification of resilience”, IEEE PES Industry Technical Support Task Force: Piscataway, NJ, USA, pp 1–4, 2018.

[11]. Z. Bie, Y. Lin, G. Li, en F. Li, “Battling the Extreme: A Study on the Power System Resilience”, Proceedings of the IEEE, vol 105, no 7, pp 1253–1266, 2017.

[12]. Y. Lin, Z. Bie, en A. Qiu, “A review of key strategies in realizing power system resilience”, Global Energy Interconnection, vol 1, no 1, pp 70–78, 2018.

[13]. P. E. Roege, Z. A. Collier, J. Mancillas, J. A. McDonagh, en I. Linkov, “Metrics for energy resilience”, Energy Policy, vol 72, pp 249–256, 2014.

[14]. A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, en U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information”, IEEE Transactions on Smart Grid, vol 4, no 1, pp 235–244, 2013.

[15]. “2020 state of reliability - NERC.” [Online]. Available: https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf. [Accessed: 17-Feb-2022].

[16]. R. Billinton en R. N. Allan, Reliability Evaluation of Power Systems, 1984.

[17]. IEEE Guide for Electric Power Distribution Reliability Indices. IEEE Std, 1366, 2003.

[18]. BC Hydro, “F2019 Annual Reporting of Reliability Indices.” [Online]. Available: https://www.bchydro.com/content/dam/BCHydro/customerportal/documents/corporate/regulatory-planning-documents/regulatory-filings/rra/2019-05-15-f05-f06-directive-26-f2019.pdf. [Accessed: 17-Feb-2022].

[19]. D. P. Gaver, F. E. Montmeat, en A. D. Patton, “Power system reliability I-measures of reliability and methods of calculation”, IEEE Transactions on Power Apparatus and Systems, vol 83, no 7, pp 727–737, 1964.

[20]. R. Billinton, J. Acharya “Consideration of multi-state weather models in reliability evaluation of transmission and distribution systems”, May, pp 619–622, 2005

[21]. R. Billinton en G. Singh, “Application of adverse and extreme adverse weather : modelling in transmission and distribution system reliability evaluation”, pp 115–120, 2006.

[22]. C. Chen en B. Chen, “Modernizing distribution system restoration to achieve resiliency against extreme weather events”, in 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP), 2018, pp 895–896.

[23]. N. T. Bazargani and S. M. T. Bathaee, “A general framework for resiliency evaluation of radial distribution system against extreme events,” Electrical Engineering (ICEE), Iranian Conference on, 2018.

[24]. Y. Xu, C.-C. Liu, K. P. Schneider, en D. T. Ton, “Toward a resilient distribution system”, in 2015 IEEE Power & Energy Society General Meeting, 2015, pp 1–5.

[25]. “Sans ICS,” SANS Industrial Control Systems Security Blog | Confirmation of a Coordinated Attack on the Ukrainian Power Grid | SANS Institute, 24-Jan-2022. [Online]. Available: https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/. [Accessed: 17-Feb-2022].

[26]. D. Kushner, “The real story of stuxnet”, IEEE Spectrum, vol 50, no 3, pp 48–53, 2013.

[27]. S. Chanda en A. K. Srivastava, “Defining and Enabling Resiliency of Electric Distribution Systems with Multiple Microgrids”, IEEE Transactions on Smart Grid, vol 7, no 6, pp2859–2868, 2016.

[28]. M. Zeller, “Myth or reality—Does the aurora vulnerability pose a risk to my generator?”, in 2011 64th Annual Conference for Protective Relay Engineers, 2011, pp 130–136.

[29]. E. Al-Ammar and J. Fisher, "Resiliency assessment of the power system network to cyber and physical attacks," 2006 IEEE Power Engineering Society General Meeting, 2006, pp. 7 pp.-, doi: 10.1109/PES.2006.1709089.

[30]. J.-P. Watson et al., “Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States”, Sandia national laboratories, Albuquerque, tech. rep, 2014.

[31]. Panteli, M., Mancarella, P., Trakas, D. N., Kyriakides, E., & Hatziargyriou, N. D. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Transactions on Power Systems, vol 32 no 6, pp 4732-4742, 2017.

[32]. P. Gautam, P. Piya, en R. Karki, “Resilience assessment of distribution systems integrated with distributed energy resources”, IEEE Transactions on Sustainable Energy, vol 12, no 1, pp 338–348, 2020.

[33]. I. Linkov et al., “Measurable resilience for actionable policy”. ACS Publications, 2013.

[34]. F. H. Jufri, V. Widiputra, en J. Jung, “State-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies”, Applied Energy, vol 239, pp 1049–1065, 2019.

[35]. Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, en Y. Al-Turki, “Networked microgrids for enhancing the power system resilience”, Proceedings of the IEEE, vol 105, no 7, pp 1289–1310, 2017.

[36]. A. Stankovic, “The definition and quantification of resilience”, IEEE PES Industry Technical Support Task Force: Piscataway, NJ, USA, pp 1–4, 2018.

CHAPTER 3: RELIABILITY AND RESILIENCY IMPLICATIONS OF CYBER-ATTACKS IN DISTRIBUTION SYSTEMS

3.1. 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. The evolving infrastructure is now susceptible to an alarming increase in natural and manmade extreme events that are responsible for wide-scale outages. 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 reliability and resiliency of a 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 reliability and resiliency assessment methodologies to conduct similar studies.

3.2. 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(Security DAS) 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 over-arching 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 [13]. Moreover, a reliable system may not necessarily be resilient [14]. Therefore, it is necessary to make a detailed assessment of the reliability and resiliency of the system against particular events

separately. There is some interesting research that sheds some light on the area of detection of possible cyber-attacks in the system. Reference [15] 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. Reference [16] 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). Reference [17] 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 [18] 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 [19], which used Software-defined Networking (SDN) reconfiguration mechanism to isolate compromised PMUs and connect uncompromised PMUs. [20] 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 measurements 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 cyber-attacks on the reliability and resiliency of power systems. Reference [21] 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. Reference [22] 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). Reference [23] 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. Reference [24] presents two tools; SyncAED 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 [23]. Reference [25] proposes a cyber-security enhanced Distribution Automation System (DAS) that can identify the anomalies in data and help mitigate them in a distribution system. Reference [8] proposed a multi-phase trapezoid as shown in Fig. 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. Three distinct phases can be visualized in the multiphase 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 [26]. Motivated by the need for quantitative assessment of distribution system followed by a holistic approach from both reliability and resiliency perspectives, this paper presents a case study of a radial distribution system in event of a cyber-attack and assess its states from both reliability and resiliency point of view. Contributions of this paper are as follows:

- A novel methodology to model cyber-attacks for analysis based on state estimation
- A novel reliability assessment methodology to assess the impact of False Data Injection Attacks (FDIAs) on the system

3.3. Methodology

3.3.1. 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 [27]:

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. An individual can compromise a device within an ESP intentionally 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 3.1 shows the information flow between the various operational functions for a section within an energy control center computer system [28]. 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 [28].

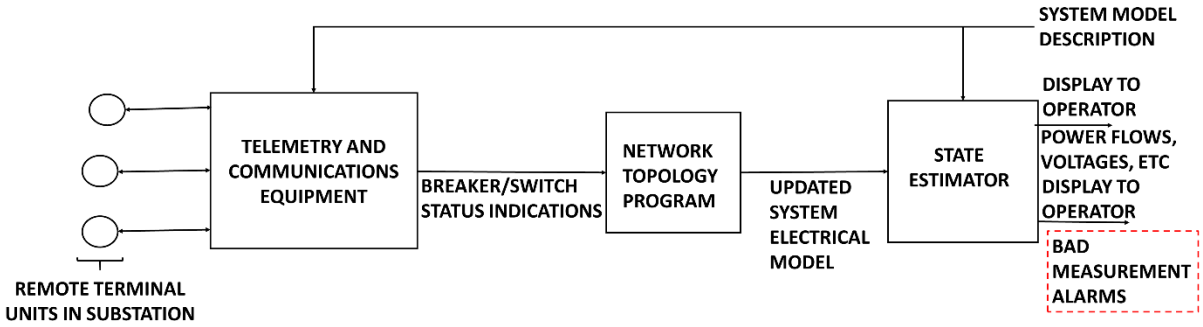

Figure 3.1 A section of energy control center system security flowchart

In this work, the distribution system is modelled as a graph G consisting of nodes or vertices V and edges E as shown in (3.1). The buses, sections, load points, circuit breakers and fuses are treated as nodes, whereas, the edges are the connections between the nodes.

$$G = \{V, E\} \tag{3.1}$$

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 [29] 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:

$$z = h(x) + e \tag{3.2}$$

where $z = [(z_1, z_2 \dots \dots, z_m)]^T$ denotes measured data, $x = [(x_1, x_2 \dots \dots, x_n)]^T$ denotes system states, $e = [(e_1, e_2 \dots \dots, e_m)]^T$ denotes measurement noise that follows a Gaussian distribution with zero mean. h(x) is a m by n 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 $\hat{x}$ is expressed in (3.3).

$$\hat{x} = [[H]^T[W][H]]^{-1}[H]^T[W]z \tag{3.3}$$

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 [30], it is evident that

an attack vector that complies, $a = Hc$ where $z_a = z + a$ will go undetected. For the test system shown in Figure 6, $x = [(x_1, x_2, x_3)]^T$ represents bus angles at bus 2,3 and 4 respectively and $z = [(z_1, z_2, z_3)]^T$ denotes the measured data. Bus 1 is assumed to be the slack bus. For, any $c = [(c_1, c_2, c_3)]^T$, $a = [(a_1, a_2 \dots\dots, a_7)]^T$ is calculated using $a = Hc$, and z_a is found. It's $z_a - Hx_{bad}$ is smaller than the threshold which is why the infected data is not detected in the system. Upon multiple iterations, it was found that, the possible load loss occurred between [0, 10] for all the values of c. All the possible iterations for c is carried out and the load loss for the combination of c, state variable x, injected error a, and the measured data z is recorded. Figure 3.2 represents some of the load loss keeping c_1 constant and varying c_2 and c_3. The hill, z-axis represents the load lost and x and y-axis represents c_2 and c_3.

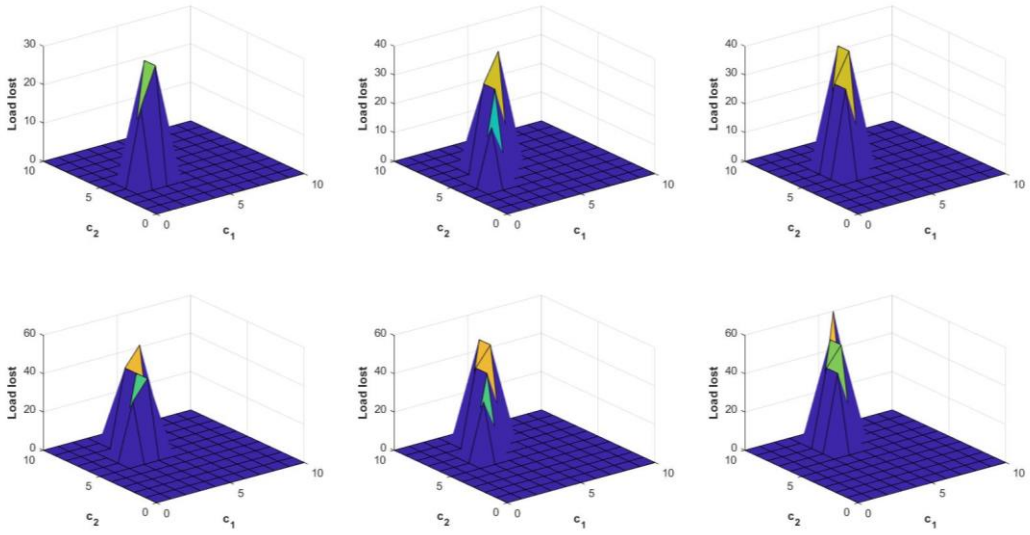

Figure 3.2 Possible losses in the system due to FDIA

3.3.2. 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. Reference [26] proposed a multi-phase trapezoid as shown in figure 3 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 3. 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, toe and end of the event, tee. Phase II: It is known as the post-disturbance degraded state. It is the duration between the end of the event, tee 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 3.3 shows the different stages a power goes through as it succumbs to a cyber-attack.

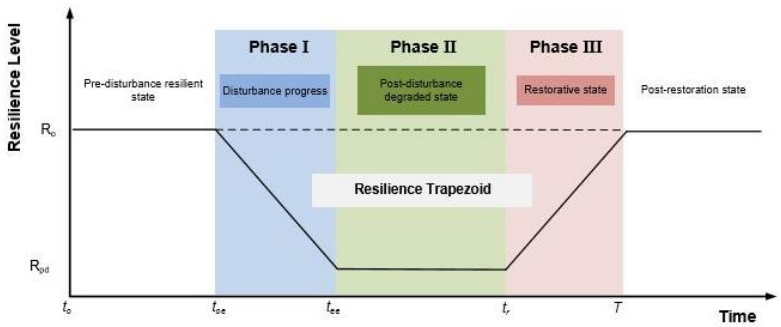

Figure 3.3 Multi-phase trapezoid

Resilience indices shown in Table 1 [12], [26] can be measured at the different trapezoid phases to quantify the impact of the attack at the different phases. The index ϕ 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 $EENS_{sys}$ and E calculated using equations from Table 3.1 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 Π obtained from Table 3.1 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. Ns and Nos in I 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 3.4.

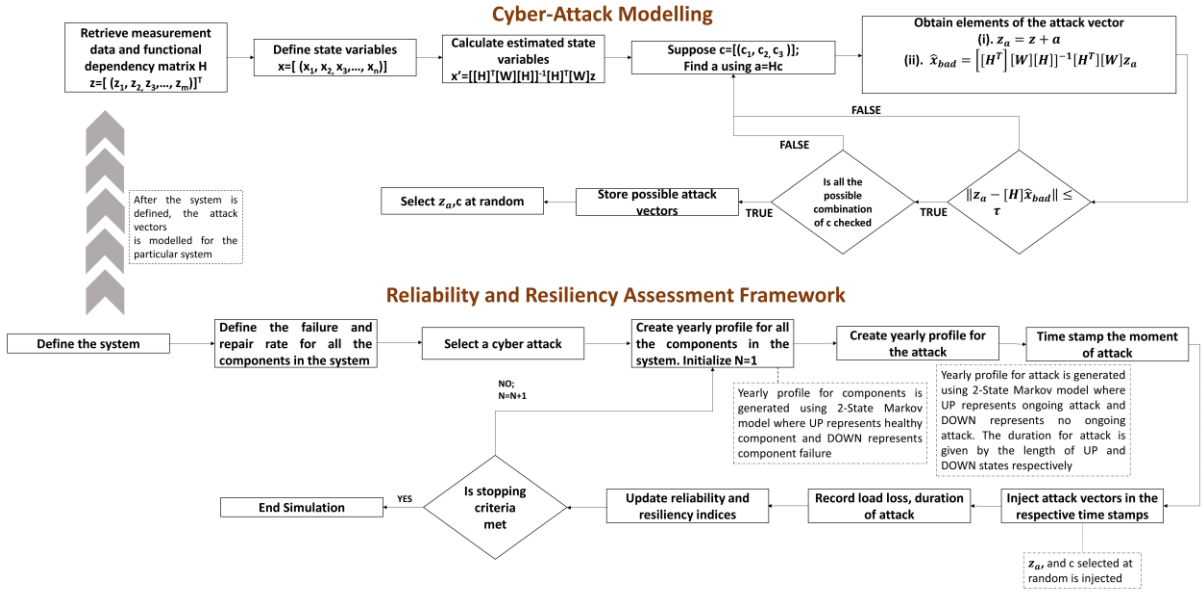

Figure 3.4 Framework for reliability and resiliency evaluation

Table 3.1 Equations for resiliency assessment

Phase	Mathematical expression
Phase I: Disturbance progress	$\Phi = \frac{R_o - R_{pd}}{t_{ee} - t_{oe}} (\frac{MW}{hr})$

Phase II: Post disturbance degraded state	$EENS_{sys} = \frac{\sum_{s=1}^{Ns} ENS(s)}{N_s^o}$ $E = t_r - t_{ee}$
Phase III: Restorative state	$\Pi = \frac{R_o - R_{pd}}{T - t_r} (\frac{MW}{hr})$

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. 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 is created as described in Section 3.3. The distribution system is then exposed to one such attack vector chosen in random. The frequency in which the system is exposed to the attack vector is defined by attack rate. 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 particular time. A sequence for a year for any such attack-rate is generated. 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 number of years for variation of such attack-rates. Finally, the reliability and resiliency performance of the system is calculated and is elaborated in Results.

3.4. Case Studies and Results

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 3.5 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 3.6 shows a typical demand variation profile within a day.

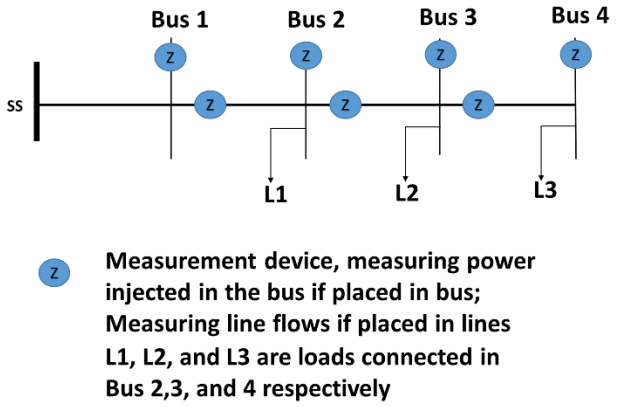

Figure 3.5 Distribution system test network

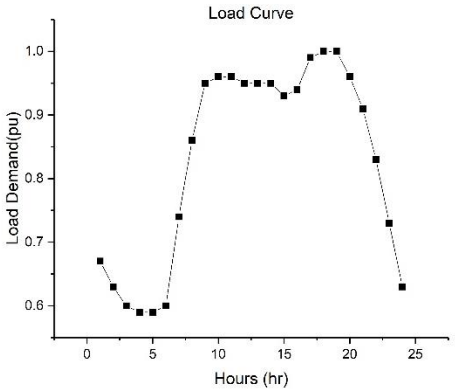

Figure 3.6 Typical demand variation in 24 hours

3.4.1. 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 3.4. Figure 3.7 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. It can be seen that both the system LOLE and the load point LOLE increase significantly, as the attack rate is increased.

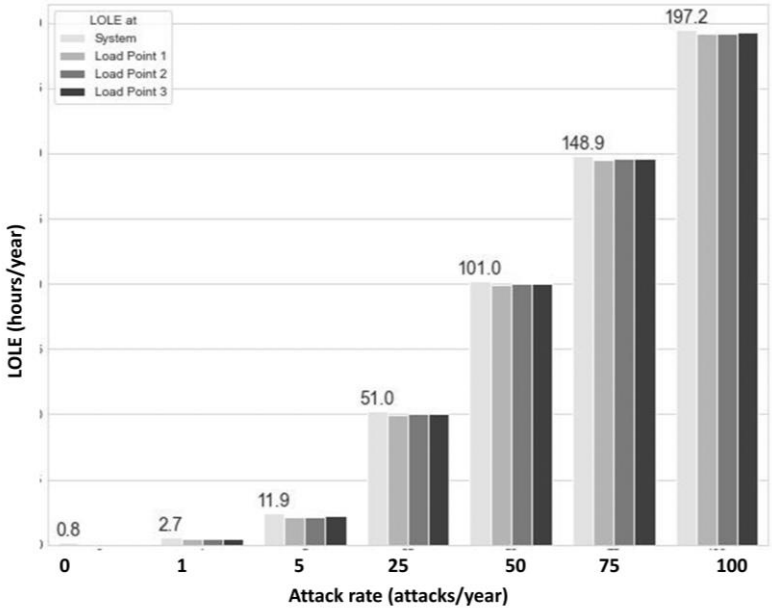

Figure 3.7 LOLE for different attack rates

Figure 8 shows the resulting EENS for various attack rates in the system. 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 indicator in deciding investment in remedial measures, such as bad-data detection systems to safe-guarding the system. Figure 3.7 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 3.8 shows that the impact of cyber-attack is dependent on the amount of load lost by the system and the load points.

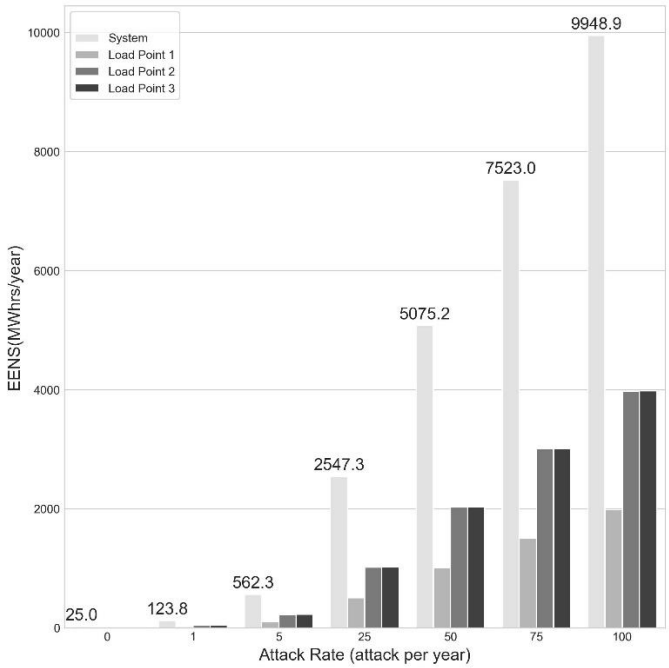

Figure 3.8 EENS for different attack rates

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 3.9. 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 3.10 show a 15-step discrete distribution within six standard deviations, assuming a 14% standard deviation about the expectation of 50 attacks per year. 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 3.11. For a comparative analysis, the figure also shows the system EENS when cyber-attacks are not considered in the assessment. Figure 3.11 shows that the consideration of cyber-attack in today's scenario significantly increases the unserved energy in the system.

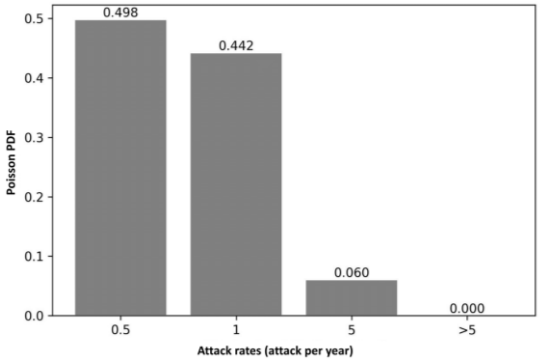

Figure 3.9 Probability of occurrence of cyber-attack in present day scenario-Scenario 1

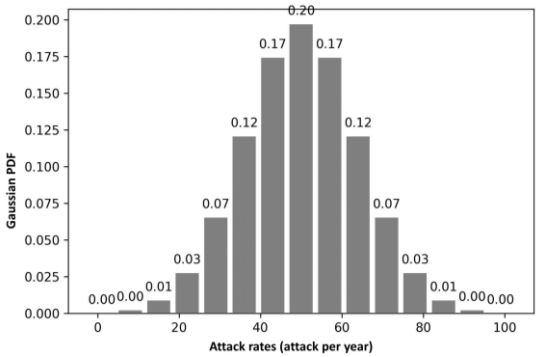

Figure 3.10 Probability of occurrence of cyber-attack in a future scenario-Scenario 2

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.

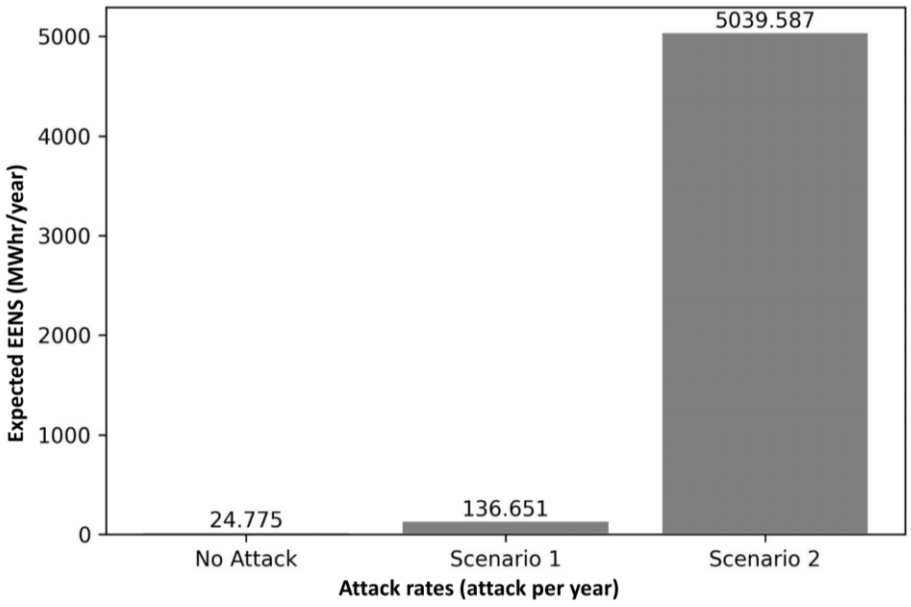

Figure 3.11 Expected EENS (MWhr/year) for different scenarios

3.4.2. 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 3.12 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 3.13 will increase as well. An analysis of the load point indices in Figure 3.12 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.

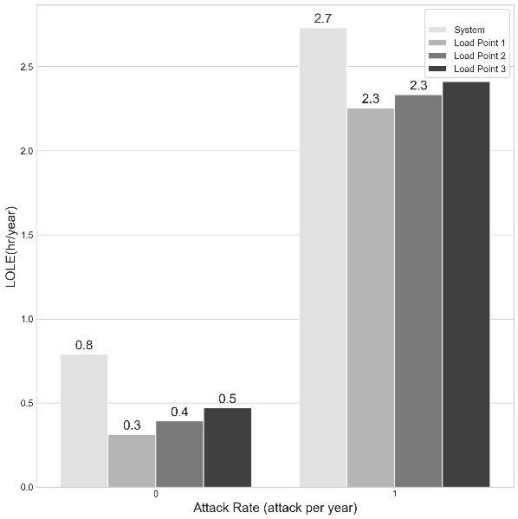

Figure 3.12 LOLE (hrs/yr) for the system observing zero and one cyber-attack per year

Figure 3.13 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.

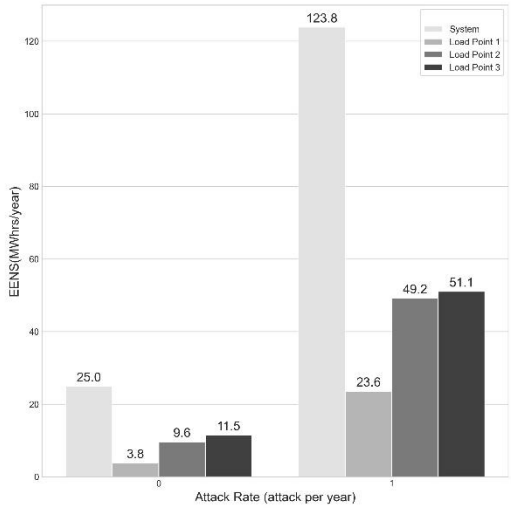

Figure 3.13 EENS(MWhrs/yr) for the system observing zero and one cyber-attack per year

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

Figure 3.3, are evaluated for the system and the results are shown in Table 3.2. The following study considers two cases. Case A 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 B 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 3.2 shows the results for the two cases using the resiliency indices evaluated at the different impact phases of the system.

Table 3.2 Resiliency of the system for Case A and Case B

	Case A	Case B
Φ (MW/hr)	24.85	25.99
EENS (MWhr/int)	188.48	368.30
E (hr)	1.82	5.46
Π (MW/hr)	25.47	25.95

Table 3.2 shows the results for the two cases using the resiliency indices 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 B is significantly higher than that of Case A. The difference is approximately equal to the time taken to identify that the cause of system outage was a cyber-attack. Table 3.2 shows that the expected energy not supplied $EENS_{sys}$ in Case B is much higher than that of Case A. The delay in starting the restorative action in Case B 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 sections.

3.4.3. 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 3.1. 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 3.14 shows the flowchart of the bad-data detection algorithm. A bad-data detection algorithm is based on state-estimation and works by com-paring 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 (4):

$$\|z_a - H\hat{x}_{bad}\| \leq \tau \tag{3.4}$$

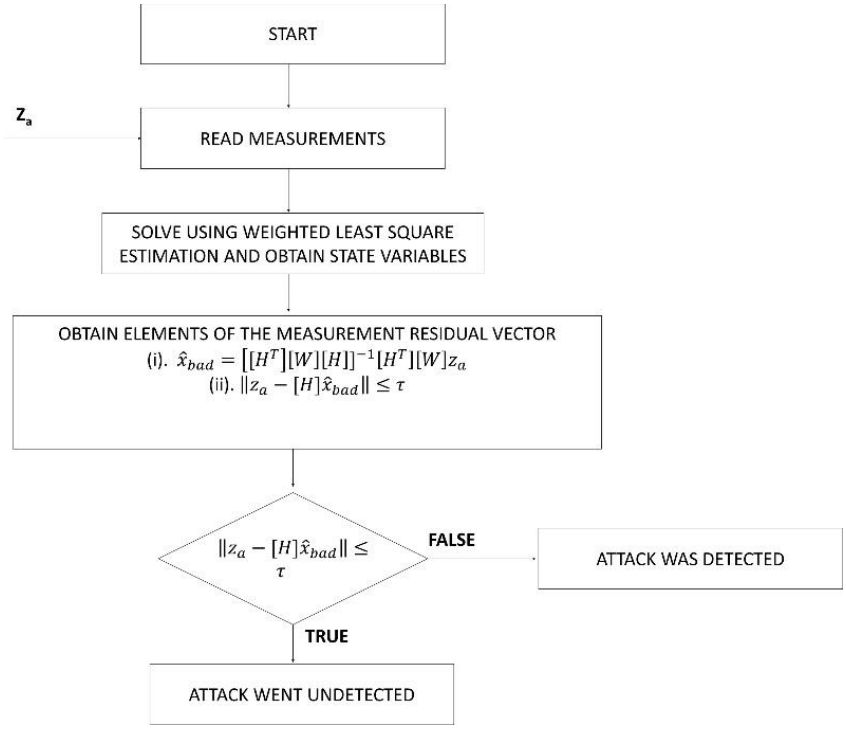

Figure 3.14 Bad-data detection algorithm

As discussed earlier, it is assumed that the perpetrators know the complete topological 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 3.14, 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 3.15.

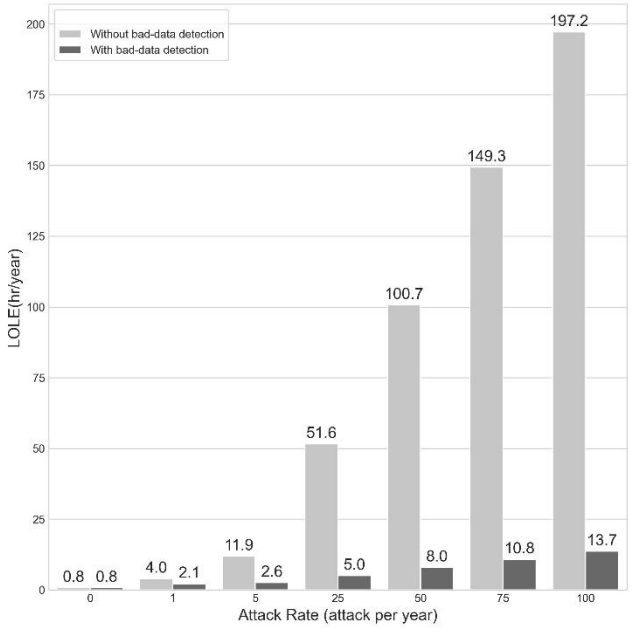

Figure 3.15 LOLE for different attack rates with and without bad-data detection

The results from figure 7 obtained without the bad-data detection system are also shown for comparison. Figure 3.15 shows a significant decrease in the LOLE with the implementation of the bad-data detection algorithm. It should be noted that Figure 3.15 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 3.16 shows the distribution of the loss of load indices for an attack rate of 5/year.

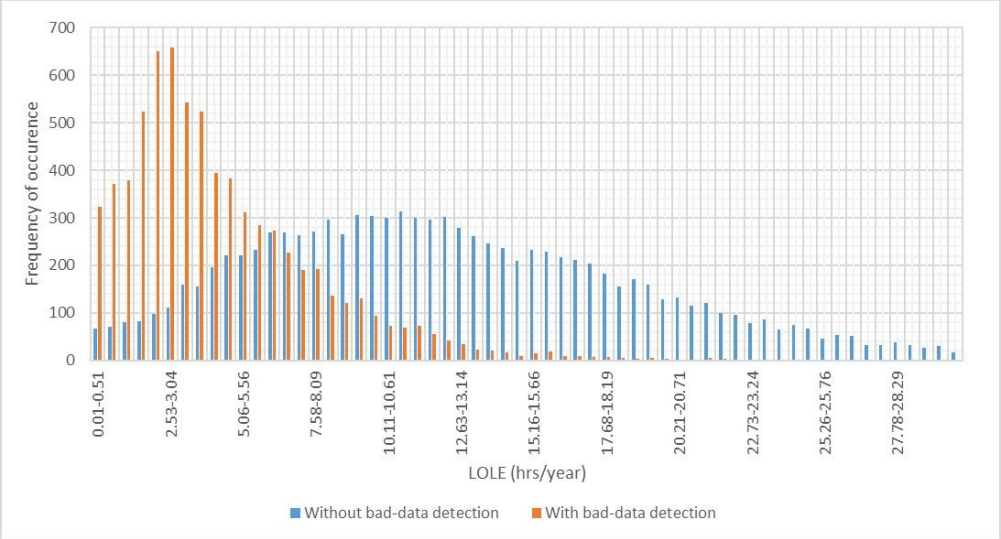

Figure 3.16 LOLE distribution for 5 attack/year with and without bad-data detection

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. 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 3.17 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 3.3 shows the resiliency metrics with the bad-data detection, and without the bad-data detection for the two cases described in Table 3.2.

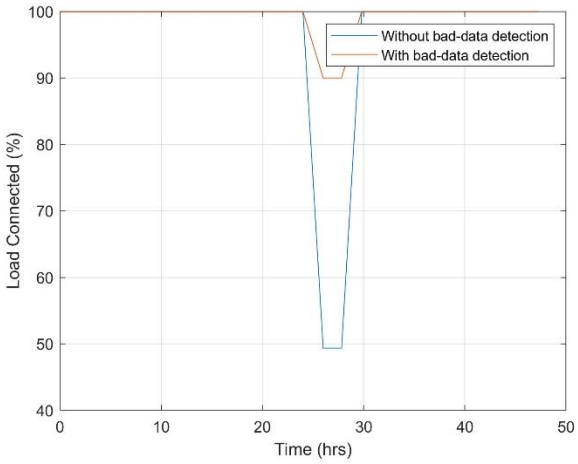

Figure 3.17 Load connected (%) in progression of a cyber-attack

From Table 3.2 and Table 3.3, 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.

Table 3.3 Resiliency of the system with and without bad-data detection

Phase	Expression	Without bad-data detection		With bad-data detection
		Case A	Case B	
Phase I: Disturbance progress	Φ (MW/hr)	24.85	24.98	4.98
Phase II: Post disturbance degraded state	EENS (MWhr/int)	188.48	368.30	1.13
	E (hr)	1.82	5.45	1.99
Phase III: Restorative state	Π (MW/hr)	25.47	25.95	5.01

3.5. 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.

The resiliency indices framework- "ϕ, E, EENS, Π" pro-vides 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.

3.6. Reference

[1] Sk Abdul Aleem, SM Hussain, and Taha Selim Ustun. A review of strategies to increase pv penetration level in smart grids. Energies, 13(3):636, 2020.

[2] Sajid Nazir, Hassan Hamdoun, and Jafar Alzubi. Cyber attack challenges and resilience for smart grids. European Journal of Scientific Research, 2015.

[3] Reza Arghandeh, Alexandra Von Meier, Laura Mehrmanesh, and Lamine Mili. On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews, 58:1060–1069, 2016.

[4] Tien Nguyen, Shiyuan Wang, Mohannad Alhazmi, Mostafa Nazemi, Abouzar Estebsari, and Payman Dehghanian. Electric power grid resilience to cyber adversaries: State of the art. IEEE Access, 8:87592– 87608, 2020.

[5] David E Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In 2017 70th Annual Conference for Protective Relay Engineers (CPRE), pages 1–8. IEEE, 2017.

[6] Ukraine power cut 'was cyber-attack'. BBC.

[7] Rebecca Smith and Rob Barry. America's electric grid has a vulnerable back door–and russia walked through it. The Wall Street Journal, 10, 2019.

[8] Elizabeth L Ratnam, Kenneth GH Baldwin, Pierluigi Mancarella, Mark Howden, and Lesley Seebeck. Electricity system resilience in a world of increased climate change and cybersecurity risk. The Electricity Journal, 33(9):106833, 2020.

[9] Roy Billinton and Ronald N Allan. Power-system reliability in perspec¬tive. Electronics and Power, 30(3):231–236, 1984.

[10] Crawford S Holling. Resilience and stability of ecological systems. Annual review of ecology and systematics, 4(1):1–23, 1973.

[11] Xindong Liu, Mohammad Shahidehpour, Zuyi Li, Xuan Liu, Yijia Cao, and Zhaohong Bie. Microgrids for enhancing the power grid resilience in extreme conditions. IEEE Transactions on Smart Grid, 8(2):589–597, 2016.

[12] Prajjwal Gautam, Prasanna Piya, and Rajesh Karki. Resilience assess¬ment of distribution systems integrated with distributed energy resources. IEEE Transactions on Sustainable Energy, 12(1):338–348, 2020.

[13] Maedeh Mahzarnia, Mohsen Parsa Moghaddam, Payam Teimourzadeh Baboli, and Pierluigi Siano. A review of the measures to enhance power systems resilience. IEEE Systems Journal, 14(3):4059–4070, 2020.

[14] Rodrigo Moreno, Mathaios Panteli, Pierluigi Mancarella, Hugh Rudnick, Tomas Lagos, Alejandro Navarro, Fernando Ordonez, and Juan Carlos Araneda. From reliability to resilience: Planning the grid against the extremes. IEEE Power and Energy Magazine, 18(4):41–53, 2020.

[15] Siddhartha Deb Roy and Sanjoy Debbarma. Detection and mitigation of cyber-attacks on agc systems of low inertia power grid. IEEE Systems Journal, 14(2):2023–2031, 2019.

[16] Hadis Karimipour, Ali Dehghantanha, Reza M Parizi, Kim-Kwang Raymond Choo, and Henry Leung. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access, 7:80778–80788, 2019.

[17] Mahdi Bahrami, Mahmud Fotuhi-Firuzabad, and Hossein Farzin. Reliability evaluation of power grids considering integrity attacks against substation protective ieds. IEEE Transactions on Industrial Informatics, 16(2):1035–1044, 2019.

[18] V Venkataramanan, A Srivastava, A Hahn, et al. Cp-tram: Cyber-physical transmission resiliency assessment metric. IEEE Transactions on Smart Grid, 11(6):5114–5123, 2020.

[19] Hui Lin, Chen Chen, Jianhui Wang, Junjian Qi, Dong Jin, Zbigniew T Kalbarczyk, and Ravishankar K Iyer. Self-healing attack-resilient pmu network for power system operation. IEEE Transactions on Smart Grid, 9(3):1551–1565, 2016.

[20] Fabio Pasqualetti, Florian Dorfler, and Francesco Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In 2011 50th IEEE Conference on Decision and Control and European Control Conference, pages 2195–2201. IEEE, 2011.

[21] Heping Jia, Changzheng Shao, Dunnan Liu, Chanan Singh, Yi Ding, and Yanbin Li. Operating reliability evaluation of power systems with demand-side resources considering cyber malfunctions. IEEE Access, 8:87354–87366, 2020.

[22] Yichi Zhang, Yingmeng Xiang, and Lingfeng Wang. Power system reliability assessment incorporating cyber attacks against wind farm energy management systems. IEEE transactions on smart grid, 8(5):2343–2357, 2016.

[23] Venkatesh Venkataramanan, Anurag K Srivastava, Adam Hahn, and Saman Zonouz. Measuring and enhancing microgrid resiliency against cyber threats. IEEE Transactions on Industry Applications, 55(6):6303– 6312, 2019.

[23] Zhijie Nie Anshuman, K Sadanandan Sajan, and Anurag K Srivastava. Ml-based data anomaly mitigation and cyber-power transmis¬sion resiliency analysis. In 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), pages 1–6. IEEE, 2020.

[24] In-Sun Choi, Junho Hong, and Tae-Wan Kim. Multi-agent based cyber attack detection and mitigation for distribution automation system. IEEE Access, 8:183495–183504, 2020.

[25] Mathaios Panteli, Pierluigi Mancarella, Dimitris N Trakas, Elias Kyri-akides, and Nikos D Hatziargyriou. Metrics and quantification of operational and infrastructure

resilience in power systems. IEEE Transactions on Power Systems, 32(6):4732–4742, 2017.

[26] Anurag Srivastava, Thomas Morris, Timothy Ernster, Ceeman Vel-laithurai, Shengyi Pan, and Uttam Adhikari. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Transactions on Smart Grid, 4(1):235–244, 2013.

[27] Allen J Wood, Bruce F Wollenberg, and Gerald B Sheblé. Power generation, operation, and control. John Wiley & Sons, 2013.

[28] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1):1–33, 2011.

[29] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security, 14(1), 2011

CHAPTER 4: DISTRIBUTION SYSTEM RESILIENCE ENHANCEMENT STRATEGIES AGAISNT EXTREME WIND

4.1. Abstract

The objective of a power system is to provide electricity to its customers as economically as possible with an acceptable level of reliability while safeguarding the environment. Power system reliability assessments are routinely performed to ensure adequate system resources and reliable operation using well-established methods, quantitative metrics, regulatory standards and compliance incentives in the jurisdictions of responsibilities. The alarming increase in the occurrence of extreme events, which are not included in routine reliability evaluation, has raised growing concerns due to the catastrophic impacts of these events on distribution systems. The potential economic losses due to prolonged and large-scale outages have motivated utility planners, operators, and policy makers to acknowledge the importance of system resiliency against such events. Power system resiliency however, lacks widely accepted modeling frameworks, standards, assessment methods and metrics. The paper presents a resilience assessment framework, along with quantifiable metrics to assess the resiliency of a distribution system against extreme winds, which is among the most common form of natural disasters affecting the North American region. The paper assesses the effectiveness of infrastructural and operational resilience enhancement strategies. The effectiveness of preventive and corrective strategies are also analyzed on a test distribution system.

4.2. Introduction

The conventional distribution system fed from a centralized power supply system is rapidly transforming into a decentralized and relatively independent network structure with increasing penetrations of distribution energy resources (DERs). The evolving infra-structure of distribution systems are exposed to considerable increase in man-made extreme events, such as cyber-attacks, and natural disasters such as earthquake, hurricanes/tornadoes, floods, ice

storms extreme winds [1] etc., that cause prolonged and/or wide-scale power outages. The proliferated exposure of distribution system to extreme events has emphasized the importance of resiliency studies. Extreme winds are known to affect distribution systems the most due to their topological and operational characteristics [2]. The distribution network succumbing to extreme winds sustain considerable damage to the infrastructures and often require lengthy and costly restoration processes. Existing approaches to planning a reliable distribution system account for random com-ponent outages, generation variations, load uncertainties and the capability of the distri-bution network to satisfy the customer demands, but do not incorporate high impact low probability (HILP) events in routine applications. The impending degradation of structural integrity and the potential magnitude of economic losses due to such damages and power outages have highlighted the need for resilient distribution systems. Power system resiliency studies, however, do not yet have established frameworks, metrics, and regula-tory standards that are widely accepted by the electric utilities [3]. Moreover, ambiguous approaches in envisioning a resilient grid is bringing surging concerns on the authenticity and credibility of the applications of such approaches.

A limited amount of literature can be found on power system resilience against extreme winds. Min Ouyang et al. [4] provide realistic fragility model to assess the resiliency using % of load connected. Reference [5] provides effective optimization algorithm that maximizes the service time of critical loads. Authors in [6] found that significant im-provement in resiliency can be made with the help of microgrids. Efficient automated switching for microgrids/DERs operations are proposed in [7] and tested on a 34-bus and 123-bus system. Authors in [8],[9],[10] model extreme wind on a bulk system. Infrastruc-ture based resilience assessment is done assessing the status of infrastructures after an event in [8], in comparison with [9],[10] which uses EENS to calculate resiliency. Ref [11] validates the efficient approach of graph theory in modelling a distribution network, and shows that microgrids can be used to ensure a flexible and resilient distribution network. An effective crew management strategy to ensure a resilient distribution system is demonstrated by [12] on the IEEE-34 bus. Reference [13] includes the geographical extensivity of extreme wind in the study. Optimal restoration of distribution grid consid-ering the switching operations and DERs/microgrids in the aftermath of extreme wind are proposed in [5,8,11,14-19].

Reference [8] proposes a resilience index called ΦΛΕΠ (pronounced as “flep”) to assess the degradation of a power system following an extreme event. Reference [20] uses a simulation-based method to quantify resiliency and also identifies the improve-ments using microgrids and DERs. Reference [21] quantify the resilience of a distribution network using

three metrics namely the expected probability of interruption, ex-pected outage duration and expected energy not served during the extreme event. Their re-silience evaluation framework embedded a wind-induced extreme event generating mod-el, damage assessment model and an optimal restoration model utilizing DER. Bie et al. [22] presents an in-depth discussion on the effectiveness of the proposed load restoration framework in creating a resilient grid.

A considerable amount of literature is present on the judicious utilization of DERs/microgrids and their switching operations to ensure the critical load points are re-stored quickly. However, ambiguity in identification of infrastructural and operational measures to ensure resiliency in distribution system, and lack of information on the ap-propriate steps to implement remedial measures in the the planning and operating phas-es are observed in many literatures. The impact of transmission line fragility on the resili-ency of the distribution network is also an important aspect not yet investigated, as the re-siliency of a distribution system cannot be guaranteed without a resilient delivery network feeding the system.

System resilience evaluation methods should have the ability to incorporate the un-certainties and correlations in the performance of different type of strategies for improving resilience. It should be able to identify between an infrastructural and operational strategy and assess the worth of the strategies in order to make proper investment decisions. It is extremely difficult to encompass all of these factors into an analytical model and validate them. A sequential Monte-Carlo simulation (MCS) can be used to observe the behavior of the system chronologically throughout the period of study, but it becomes computational-ly burdensome due to the need to employ large simulation samples, and carry out load flow and optimization algorithms for each simulated event. This paper presents the de-velopment of novel resilience evaluation framework including probabilistic extreme event model, resilience enhancement model, and resilience assessment model incorporating in-frastructural and operational strategies, and integrates them using a MCS framework that preserves relevant time-varying dependencies of the various stochastic parameters in the system. A non-sequential MCS is chosen over sequential MCS for computational efficien-cy.

Infrastructural strategies, such as pole hardening, are modelled with the help of fra-gility curves [10]. Its impact on distribution system is studied using the proposed resili-ence assessment model. The resilience assessment model observes the load supplied be-fore, during and after an extreme event and creates a load profile to quantify its resiliency. The availability of repair personnel and its impact on resiliency of the distribution system is also evaluated using the proposed framework. The application of DERs is also facili-tated and studied in the proposed resilience assessment framework. A graph-theory based search algorithm is used to

find the affected load points and identify segments that can operate under islanded microgrid mode. An optimization problem based on mixed inte-ger linear programming (MILP) is formulated to minimize the energy curtailment due to outages.

4.3. Distribution system resiliency assessment framework

The development of the proposed distribution system resiliency assessment framework is presented in this section. The framework is based on the system response curve shown in Figure 4.1, which is also known as a resilience trapezoid [1]. On the x-axis of Figure 4.1, t_o represents the time before the occurrence of the extreme wind when the system is working under normal conditions. The extreme wind event starts at the time t_{se}, and the impact begins to change the operating condition of the system. This is designated as Phase I in Figure 4.1. Extreme wind can tear down poles, damage overhead lines and outdoor equipment causing load loss in the system. This increasing load loss, or infrastructural damage caused by the extreme wind is represented by the drop in resilience level between the times t_{se} and t_{ee}, the later represents the end of the extreme wind event. Phase II or post-disturbance degraded state represents the time interval after the extreme wind subsides and before the restorative measures are deployed. At this phase, the operators start assessing the damage in order to decide how to restore the supply to the critical and other loads in the affected areas. This requires identification and assessment of the problem, and planning of restoration measures in order to minimize the losses.

Restorative actions can include deployment of DERs to supply the loads, and deployment of crewmen to repair damaged poles, lines and related equipment. These actions gradually restore service to the curtailed loads, which translates to a decrease in load loss, and an increase in the resilience level as shown by the positive slope in Phase III of the figure. Phase III or the restorative state is the time interval between t_{sr}, the start of restorative actions and t_{er}, the end of the restorative actions.

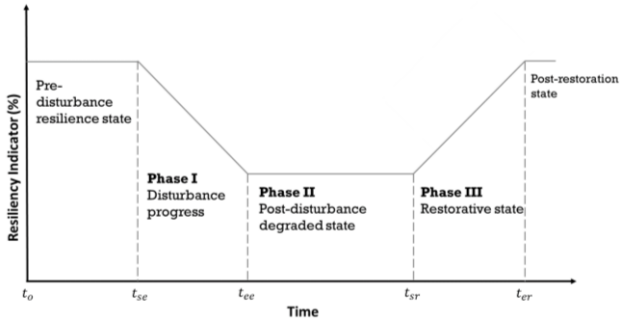

Figure 4.1 Typical resilience trapezoid

The resiliency of a system can be improved through different strategies. Each of these measures produce a different response in the system. Therefore, in order to provide the distinction, the strategies are categorized into two types: (i) Long-term infrastructural planning, and (ii) Short-term operational strategies. Pole hardening using stronger materials to increase the strength of poles, under-grounding cables are some of the long-term preventive strategies to achieve a resilient grid against extreme wind. These strategies can be relatively costly and are to be decided during the planning phase, but provide proactive solution to the problem. Investment in DERs is another example of a long-term infrastructural planning. Short-term operational strategies includes strategies like deployment of crewmen, efficient operation/management of DERs etc. These strategies provide corrective action and reduce the outage time due to extreme wind.

Each of these strategies react differently and therefore produce different results in the distribution system resilience enhancement. The paper, therefore, models and studies each strategy independently. A quantitative assessment of resilience is done for each study after the associated changes are made in the distribution system. The system resilience profile is studied for improvement or degradation, and conclusions are drawn on the effectiveness of the strategies using appropriate quantitative indices. The following subsection describes the main steps involved in modelling the wind and the system responses, and the impact on the distribution system incorporating the remedial strategies. The proposed indices are used to assess the effectiveness of the strategies.

4.3.1. Extreme wind modelling

The “duration” of the event and the “profile” of the wind speed during the event are the two key mathematical features considered in extreme wind modeling. The ”duration” refers to the time span of the extreme wind. It can range from a few hours to a few days. This paper models the duration using exponential approximation. Exponential distribution is approximated based on historical data of outages associated to wind events to estimate the mean duration of the outage times [23]. The data in [23] contains wind event duration for power outages associated with extreme wind from the year 2000 to 2016. This estimation is then used to randomly generate the duration of extreme events in hours using the ‘*exprnd*’ function in MATLAB. The “profile” represents the wind speed throughout the duration of the extreme

wind event. The profile is generated using a Gumbel distribution, also known as the extreme-I distribution.

Equation (4.1) shows the cumulative distribution function (CDF) of the Gumbel distribution. The symbol μ and β in (4.1) are the location and scale parameters of the Gumbel distribution, respectively. Wind speed samples (w_n) are generated from the inverse transform of Equation (4.1) using MATLAB. Equation (4.2) shows the output of the extreme wind model. The variable n in Equation (4.2) is the duration in hours obtained from exponentially fitting the historical data, and w_i gives the wind speed for the ith hour of the event.

$$F(x, \mu, \beta) = e^{-e^{\frac{x-\mu}{\beta}}} \tag{4.1}$$

$$W = \{w_1, w_2, \dots, w_n\} \tag{4.2}$$

4.3.2. Impact assessment on the distribution system due to extreme wind

The distribution system components exposed to an extreme wind event can fail depending on the severity of the event and the structural fragility of the elements. A generic structural fragility of a distribution pole is shown in Figure 4.5. This figure is mathematically expressed by the empirical equation (4.3) which is utilized to evaluate the failure probability of distribution poles FP_{pl}. These values are then used to calculate the failure probability of line segments, FP_{ij} using Equation (4.4). The variable *pl* represents a pole, and *ij* represents the line segment between bus *i* and bus *j* respectively.

$$FP_{pl} = 0.0001 \times \exp[\, 0.0421 \times V_w] \tag{4.3}$$

$$FP_{ij} = 1 - \prod_{pl=1}^{NP_{pl}} (1 - FP_{pl}) \tag{4.4}$$

The failure status for each line segment of the distribution system is then determined using uniform random numbers. The random number x_{line} is compared with probability of failure of each line segment obtained from Equation (4.3) and Equation (4.4). The status of individual line segment is then evaluated using Equation (4.5).

$$\gamma_{ij}^{line} = \begin{cases} 1\,; & if\ x_{line}(=\cup\,(0,1)) \leq\ FP_{ij} \\ 0\,; & otherwise \end{cases} \tag{4.5}$$

The information is then utilized to identify the unhealthy and healthy sections of the distribution grid. A depth-first search (DFS) algorithm, based on graph theory [24] is used in this paper to assess the load points affected after an extreme event, and identify the healthy and unhealthy sections of the network. The information regarding the status of the distribution

system elements is provided by the DFS. After an extreme event, the load points may reside in one of the following three states; (i) Grid-connected mode, (iii) Islanded mode, and (iii) Failed Mode. The main utility supplies the segment in the grid-connected mode. The healthy part of the network is supplied by DERs in the islanded mode. In the failed mode, the load point is not be supplied by the main grid or DERs. It is assumed that fully reliable circuit breakers/reclosers are equipped with sectionalizers on both sides for fault isolation.

4.3.3. Restoration mechanism of the distribution system after an extreme event

This section describes the restoration mechanism of the distribution system after an extreme event. Restoration mechanism depends on the state of the system, available resources and the restoration strategy decided for implementation. Preventive strategy and corrective strategy are two strategies studied in this paper. Preventive strategy aims to strengthen the system such that it rides through an extreme wind with minimal or no damages. Corrective strategy aims to provide measures to mitigate the losses by managing and deploying the operational resources at the time of an extreme wind. Pole hardening and investment in DERS are the long-term preventive strategies, whereas managing available DERs and deployment of repair crew are the operational corrective strategies considered in the study.

Preventive strategy can avoid or minimize damages, but may still need repair in the system. The repair takes place for the failed line segments in the system. Corrective strategies too sustain damages in the line segments and follow the same principle. Both the strategies follow the same restoration mechanism. The restoration time depends on the magnitude of repair and the number of repair crew deployed. The repair times of components are assumed to be exponentially distributed. The repair time *rt* for a component, such as a line segment, is calculated using Equation (4.6), where m is the mean time to failure of the component and U is an uniformly distributed random number between 0 and 1.

$$rt = -\frac{1}{\mu}\ln(U) \tag{4.6}$$

The mean time to repair is based on one repair personnel being deployed for the repair of of a faulty line segment. The restoration time is then calculated based on repair time of individual segments, number of line segments damaged and repair personnel available as depicted in Figure 4.2. The variable *f* and *rp* represents number of failed segments and number of repair personnel respectively.

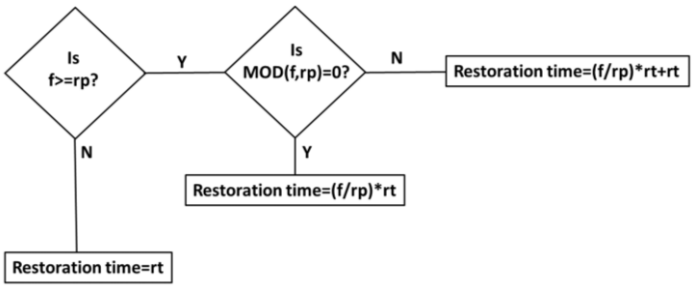

Figure 4.2 Logic diagram for restoration time

The modes in which the load points reside following an extreme wind event are first identified. The load points in the islanded and failed mode needs restoration. The buses connecting these load points are identified and then sorted on the basis of priority. The critical loads have priority over the non-critical loads in the restoration process. The time required for restore each bus depends on the number of load points restored. A restoration profile for each of the bus in the distribution system is obtained, which contains amount of load restored in each hour.

4.3.4. Modelling of operating strategies with DERs

This section details the MILP based optimization problem formulated for islanded microgrids. Table 4.1 includes the notations used in the optimization.

Table 4.1 Notations used in optimization

$i/j, ij, p, c,$ e, m	Indices of bus, line section, PV, CDG, ESS, and islanded microgrids, respectively
$\Omega_B, \Omega_{IJ}, \Omega_{PV},$ $\Omega_{CDG}, \Omega_{ESS}, \Omega_M$	Set of bus, line section, PV, CDG, ESS, and islanded microgrids, respectively
$t/\ T$	Index and total estimated outage time
$pr_{CDG,}\ pr_{ESS},$ pr_{PV}	Operational cost of CDG, ESS and PV, respectively ($/MWhr)
pr_i^{lc}	Penalty cost for load curtailment for load at bus i ($/MWhr)
$LC_{a,i}(t), LC_{r,i}(t)$	Active and reactive load curtailed at bus i, time t (MW and MVAR)
$\eta_{e,i}^c, \eta_{e,i}^d$	Charging and discharging efficiency of ESS at bus i, respectively (%)
$V_i(t), \theta_i(t)$	Voltage magnitude and phase angle at bus i, time t (p.u.)
$P_{c,i}(t), Q_{c,i}(t)$	Active and Reactive power from CDG at bus i, time t (MW and MVAR)

$P_{p,i}(t)$	Active power from PV at bus i, time t (MW)
$P_{ij}(t), Q_{ij}(t)$	Active and Reactive power flowing between line ij at time t (MW and MVAR)
$PD_i(t), QD_i(t)$	Active and reactive power demand at bus i, time t (MW and MVAR)
$P^d_{e,i}(t), P^c_{e,i}(t)$	Discharging and charging power associated with ESS at bus i, time t (MW)
$Q_{e,i}(t)$	Reactive power from ESS at bus i, time t (MVAR)
$SOC_{e,i}(t)$	State of Charge of ESS at bus i, time t (MWhr)
$\gamma^c_{e,i}(t)$	Binary variable representing charging status of ESS at bus i for period t (1 for charging, 0 otherwise)
$\gamma^d_{e,i}(t)$	Binary variable representing discharging status of ESS at bus i for period t (1 for discharging, 0 otherwise)
$\overline{P_{p,i}(t)}$	Maximum available power from PV at bus i, time t (MW)
$\overline{X}, \underline{X}$	Maximum and minimum limit of parameter X, respectively (X=active/reactive power of DERs, charging/discharging power of ESS, SOC of ESS, bus voltage magnitude/phase angle)

The implementation of DERs is based on [21]. The nodal power injected to the grid is represented by (4.7)-(4.8). P,Q and ΔV represents the column vector of active power, reactive power, and incremental voltage from the nominal value at each bus.

$$P = G'\Delta V - B'\theta \tag{4.7}$$

$$Q = -B''\Delta V - G'\theta - B_{sh} \tag{4.8}$$

The admittance matrix is given by Y = G + **j**B, where each element in ith row and jth column is shown by $Y_{ij}=G_{ij}$ + **j**B_{ij}. G'_{ij}, B'_{ij}, B''_{ij}, and B_{sh} are obtained from (4.9)-(4.12)

$$G'_{ij} = \begin{cases} -G_{ij}\,; & if\ i \neq j \\ \sum_{\substack{k\in\Omega_{BN} \\ k\neq i}} G_{ik} & if\ i = j \end{cases} \tag{4.9}$$

$$B'_{ij} = \begin{cases} -B_{ij}\,; & if\ i \neq j \\ \sum_{\substack{k\in\Omega_{BN} \\ k\neq i}} B_{ik} & if\ i = j \end{cases} \tag{4.10}$$

$$B''_{ij} = \begin{cases} -B_{ij}\,; & if\ i \neq j \\ 2B_{i0} + \sum_{\substack{k\in\Omega_{BN} \\ k\neq i}} B_{ik} & if\ i = j \end{cases} \tag{4.11}$$

$$B_{sh} = \left[B_{10}, B_{20}, \ldots B_{io}\,, B_{N_B 0}\right]^T \tag{4.12}$$

Where the shunt susceptance of bus i is given by B_{io}; the set of network buses and the total number of network buses is denoted by Ω_{BN} and N_B respectively.

An optimization problem is formed with an objective of minimizing the load curtailments over the duration of restoration time calculated from Figure 4.2. The objective function shown by (4.13) considers the load restoration priority based on the penalty cost for the curtailment of load points.

$$\boldsymbol{Min.} \quad \sum_{t=1}^{T} \sum_{i \in \Omega_B} LC_{a,i}(t) \times pr_i^{lc} + P_{p,i}(t) \times pr_{CDG} + P_{e,i}(t) \times pr_{ess} + P_{c,i}(t) \times pr_{CDG} \tag{4.13}$$

The objective function in (4.13) is subjected to the constraints (4.14)-(4.30), where $\forall i \in \Omega_B, \forall ij \in \Omega_{IJ}, \forall t \in T$. The multi-period AC power flow equality constraints for load balance for the islanded microgrid is given in (4.14)-(4.15). The capacity constraints of line sections are described in (4.16)-(4.19). Note that the linearized AC load flow equations utilized in (4.14)-(4.17) are based on (4.7)-(4.12). In (4.20)-(4.21), the nodal voltage magnitude and phase angle constraints are detailed. The state of charge (SOC) update and minimum/maximum SOC allowed for ESS are represented in (4.22)-(4.23). The charge/discharge rates of the ESS are enforced in (4.24)-(4.26), where the binary variables are used to ensure ESS either charge or discharge at a time. The maximum and minimum value of active and reactive power from the conventional DG (CDG), Photovoltaic arrays (PV), and ESS are considered in (4.27)-(4.30).

$$-P_{c,i}(t) - P_{p,i}(t) + P_{e,i}^{c}(t) - P_{e,i}^{d}(t) + \sum_{j \in \Omega_B} G'_{ij}\, \Delta V_j - \sum_{j \in \Omega_B} B'_{ij}\theta_j - LC_{a,i}(t) = -P_{D,i}(t) \tag{4.14}$$

$$-Q_{c,i}(t) - Q_{e,i}(t) - \sum_{j \in \Omega_B} B''_{ij}\, \Delta V_j - \sum_{j \in \Omega_B} G'_{ij}\theta_j - B_{sh_i} - LC_{r,i}(t) = -Q_{D,i}(t) \tag{4.15}$$

$$P_{ij}(t) = \left(\Delta V_i - \Delta V_j\right) G_{ij} - \left(\theta_{ij} - \theta_{ij}\right) B_{ij} \tag{4.16}$$

$$Q_{ij}(t) = -\left(\Delta V_i - \Delta V_j\right) B_{ij} - \left(\theta_i - \theta_j\right) G_{ij} \tag{4.17}$$

$$\underline{P_{ij}} \leq P_{ij}(t) \leq \overline{P_{ij}} \tag{4.18}$$

$$\underline{Q_{ij}} \leq Q_{ij}(t) \leq \overline{Q_{ij}} \tag{4.19}$$

$$\underline{V_i} \leq V_i(t) \leq \overline{V_i} \tag{4.20}$$

$$\underline{\theta_i} \leq \theta_i(t) \leq \overline{\theta_i} \tag{4.21}$$

$$SOC_{e,i}(t) = SOC_{e,i}(t-1) + \eta_{e,i}^{c} \times P_{e,i}^{c}(t) - \frac{P_{e,i}^{d}(t)}{\eta_{e,i}^{d}} \tag{4.22}$$

$$\underline{SOC_{e,i}} \leq SOC_{e,i}(t) \leq \overline{SOC_{e,i}} \tag{4.23}$$

$$\gamma_{e,i}^{c}(t) \times \underline{P_{e,i}^{c}} \ \leq P_{e,i}^{c}(t) \ \leq \gamma_{e,i}^{c} \times (t)\overline{P_{e,i}^{c}} \tag{4.24}$$

$$\gamma_{e,i}^{d}(t) \times \underline{P_{e,i}^{d}} \ \leq P_{e,i}^{d}(t) \ \leq \gamma_{e,i}^{d}(t) \times \overline{P_{e,i}^{d}} \tag{4.25}$$

$$\gamma_{e,i}^{c}(t) + \gamma_{e,i}^{d}(t) \leq 1 \tag{4.26}$$

$$\underline{P_{c,i}} \leq P_{c,i}(t) \ \leq \overline{P_{c,i}} \tag{4.27}$$

$$\underline{Q_{c,i}} \leq Q_{c,i}(t) \ \leq \overline{Q_{c,i}} \tag{4.28}$$

$$\underline{P_{p,i}} \leq P_{p,i}(t) \ \leq \overline{P_{p,i}(t)} \tag{4.29}$$

$$\underline{Q_{e,i}} \leq Q_{e,i}(t) \ \leq \overline{Q_{e,i}} \tag{4.30}$$

4.3.5. Resilience assessment model

The flowchart of the proposed framework is shown in Figure 4.3. At first, the distribution system to be studied is defined. The load demand, line parameters, protection settings, DER ratings and all other associated input data for the system and its components are obtained. As mentioned before, the study in this paper considers two types of strategies, (i) Long-term infrastructural planning and (ii) Short-term operational strategy. A strategy to be studied is chosen, and changes are made in the distribution system accordingly. For example, if the application of pole hardening is to be studied, changes are made in the parameters of structural fragility for the simulation. The graph network of the distribution system is generated to facilitate an efficient damage assessment model. An extreme wind event as discussed in Section 4.3.1 is generated. The damage assessment due to the extreme wind is done using (4.3)-(4.5). The restoration of the affected load points takes place after the extreme wind subsides. The restoration time is calculated from Figure 4.2 and the restoration profile for the system is obtained as described in Section 4.3.3.

A non-sequential Monte Carlo simulation based program is developed on MATLAB to simulate the extreme event, and perform the resiliency evaluation for different strategies. The load profile for the system before, during and after an event is obtained. The resiliency metrics are then evaluated based on the load profile of the system and the mitigating effects of the remedial strategies are observed and analyzed.

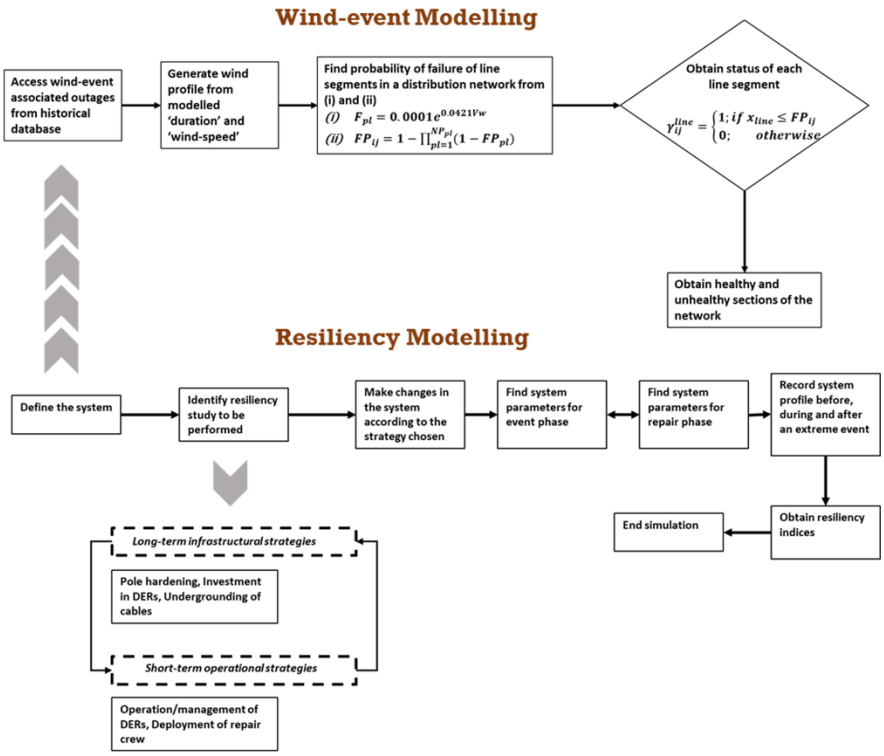

Figure 4.3 Flowchart of the proposed framework

4.4. Application of the proposed resiliency framework

When an extreme wind event occurs, the distribution network operators try to manage the resources available to them with the aim of minimizing load lost considering options with least economic stress. The avaibility of these resources during an event depends on prior resilience planning of the system. The different investment decisions will result in different resilience performance of the system as the various resilience metrics are impacted in different ways. The following sections investigagte different investment options and strategies to improve distribution system resiliency and present case studies. The extreme wind impact studies are carried out the on the IEEE 69 bus test system shown in Figure 4.4.

The nominal voltage of the test system is 12.66 kV, and the total load is 3.80 MW and 2.69 MVAR. The critical loads comprise 1.02 MW and 0.72 MVAR and their locaitons are shown in the Figure 4.4. The acceptable bus voltage range is set as 0.9 p.u. to 1.05 p.u. The power ratings of ESS, PV and CDG are shown in Table 4.2**.** The charging and discharging efficiency of ESS is taken as 0.95 each, and the rated discharge duration is 6 hour. Advance notice of extreme winds are generally available with reasonable time to allow some degree of preparedness, such as storing energy in ESS connected to the system. The initial SOC of ESS are therefore assumed to be 80% of the rated capacity. It is assumed that the DERs form the

largest possible microgrid and the protective devices accordingly facilitates the formation of microgrid. The reactive power limit for the CDG and ESS are assumed as +-70% of the rated MW capacity. The operational cost of convential DG is $0.28/kWhr [24]. The operational cost associated with PV and ESS are neglected. Penalty costs of $500/MWhr and $200/MWhr are used for critical and non-critical loads respectively.

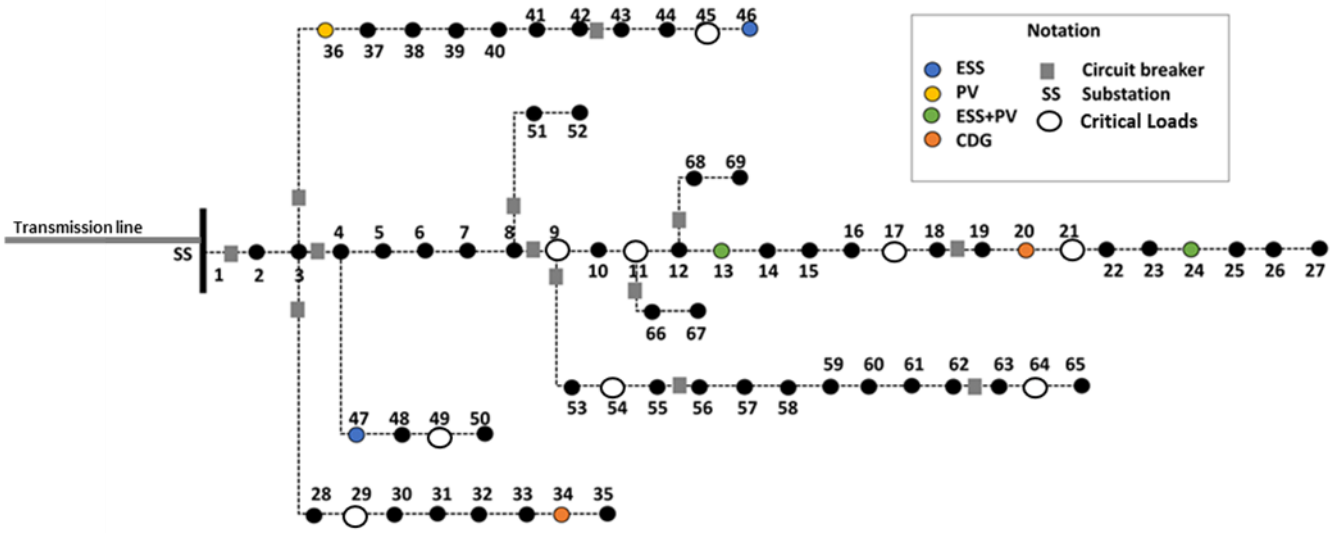

Figure 4.4 IEEE 69 bus test distribution network

Table 4.2 Details of DERs used in the network

Type of DERs	Bus No.	Rated capacity (MW)
ESS	13,24	0.15
	46	0.075
	47	0.4
	54	0.05
PV	13,24	0.15
	36	0.075
	49	0.2
	54	0.05
CDG	20	0.10
	34	0.05
	64	0.25

An extreme wind profile is generated using Equation (4.1) and (4.2). Wind speed samples are generated using the MATLAB function ‘evinv’. The average wind speed for

extreme wind is taken as 58 mph, with the scaling parameter of 8 mph for the Gumbel distribution. The duration of the extreme wind event is randomly generated for each simulation.

A program was developed based on non-sequential Monte-Carlo simulation implemented in MATLAB R2019a. The program was used for data-analysis and resiliency index calculation in the following studies.

4.4.1. Infrastructural resiliency assessment

This section investigates the distribution system resiliency due to change in infrastructure hardness, mainly the fragility of the distribution system poles that support the overhead lines. These poles can have different structure design, such as single-pole, H-frame, and can be made from different materials, such as wood, steel or concrete. The different designs and materials have different fragilities, and show different levels of resilience in the case of an extreme event.

When the distribution poles are exposed to high winds, the withstanding capacity of the poles depend on their structural integrity. Some of the poles sucuumb to the strong winds and fall down, whereas others may not. The number of damaged poles depends on the wind speed and the structural integrity of the material used to construct the poles. The lines supported by the damaged poles cannot supply the load, and the system suffers load loss. The different levels of resiliency shown by the poles and their collective impact on the resiliency of the distribution system is examined by facilitating different cases studies. Case B considers the distribution lines supported by routinely maintained wooden poles, and is considered as the base case study. Case A assumes a case where the wooden poles are not routinely maintained due to budget constraints, and therefore, exposed to considerable wear and tear over the years. The poles are assumed to be 30% more fragile than the base case. Case C assumes the distribution system has steel poles due to investment in infractural hardness. The poles are assumed to be 30% more robust than the base case. Figure 4.5 shows the fragility curves for the three cases. The fragility curves are matematically expressed in Equation (4.31).

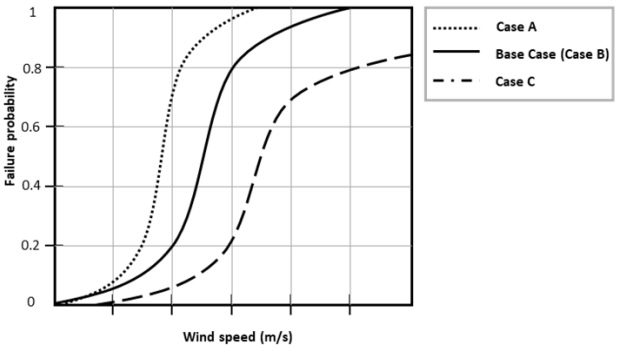

Figure 4.5 Fragility curve for distribution and transmission network

This study assumes the test system in Figure 4.5 does not include the DERs. The mean time to repair for each line segment in distribution network is assumed to be 5 hrs. It is assumed that 20 crewmen are available for repair.

$$p_{f,dist\_poe}(W_s = x_i) = 0.0001e^{0.0421x_i} \quad (4.31)$$

Figure 4.6 represents the resilience profile of the test system for cases A, B and C. It can be seen that the resilience profile obtained closely resembles the charatertistics of the resilince trapezoid in Figure 4.1. Figure 4.6 shows that all three cases succumb to the extreme wind event and follow similar degradation profile under the wind subsides. Case C, however, has the least number of poles damaged, and therefore, recovers faster than the other two cases. Case A has distribution poles with the weakest fragility curve, and therefore shows the poorest performance among the three cases in restoring the system. The effectiveness of load restoration strategy as discussed in Section 4.3.3 is also verified, as critical loads are first restored, followed by the non-critical loads.

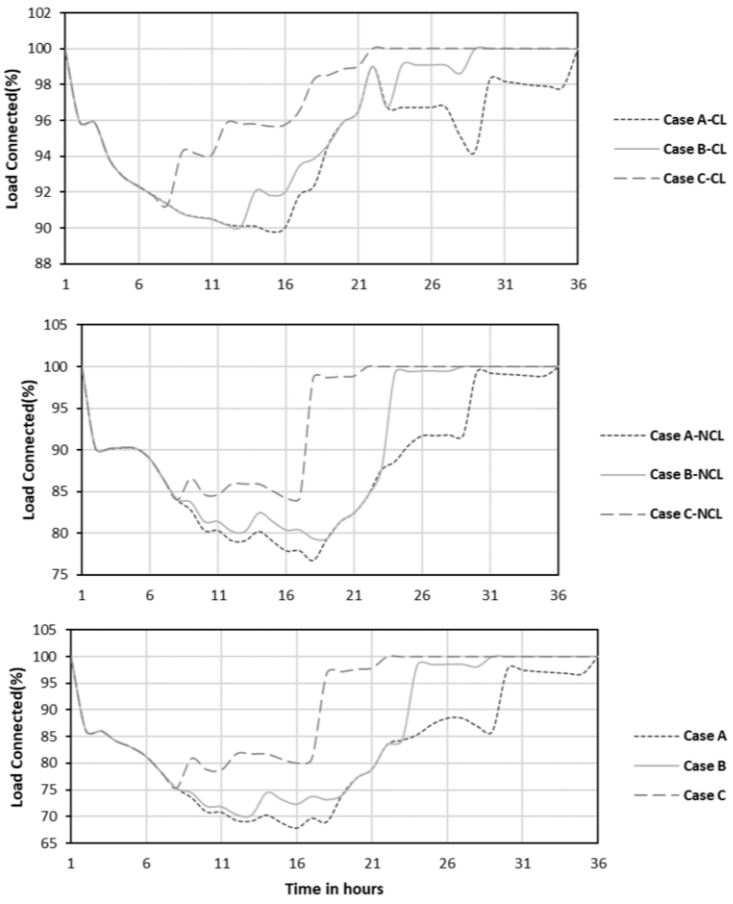

Figure 4.6 Resilience profile for Case A, B and C

It should be noted that extreme winds with high peaks are less probable than extreme winds with moderate peaks. Another study was done to compare the resiliency of Case B and C in which the extreme wind event peaks at 30 mph. . The resilience profile for the two cases are shown in Figure 4.7. In contract to the previous study, the degradation in Phase I of the resilience profile are not the same for the two cases when the extreme wind is slighlty moderate. The figure shows that the steel poles in Case C are able to withstand and ride through the event up to a certain point and degrade less severly that Case B with the wooden poles. The restoration in Case C is much faster than Case B due to fewer failures in system elements.The resutls from these studies provide evidence that investment in using proper guide wires to increase the strength of the poles, or using stronger materials for distribution poles can help achieve a more resilient distribution grid.

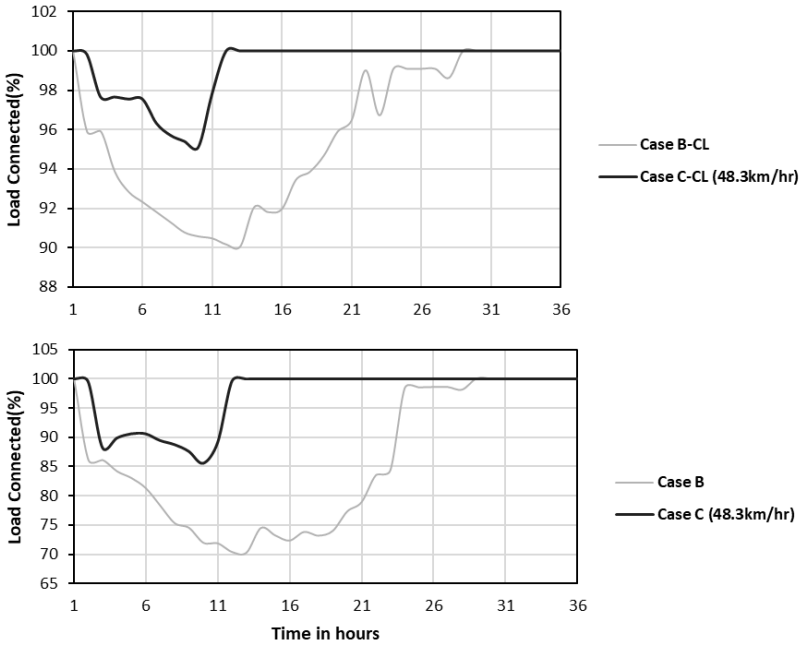

Figure 4.7 Resilience profile for different wind speeds

Figure 4.8 shows the response in terms of loads lost per hour of critical loads considering materials of different structural fragility of distribution poles during extreme wind. The figure shows that, the poorer the fragility of the poles, the faster load is lost in an extreme wind. This is because, poor structural fragility increases number of failed poles, increasing number of failed lines in a distribution system, which translates to load loss in those areas. Case C(30mph) referes to Case C in which the extreme wind peaks at 30 mph, and experiences the slowest load loss among other cases. This is because very few number of poles are damaged as most of them ride through the extreme event. The results show that hardening poles is a preventive strategy that ensures a resilient distribution network.

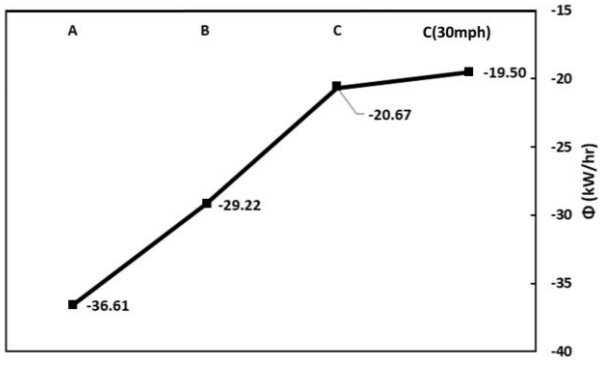

Figure 4.8 Φ response of different cases in event phase

Repair personnel repair the damaged poles, line segments and other comoponents and restore the load in the system. The impact of the avaibility of repair personnel on distribution system resiliency against extreme wind is investigated by carrying out three case studies on the

test system. Case B, D and E consider 20, 5 and 100 repair personnel respectively. Case E envisions a national rapid response team that can be immediately dispatched to locations that are under the threat of extreme wind events. Figure 4.9 shows the resilience profile of the distribution network for the three cases.

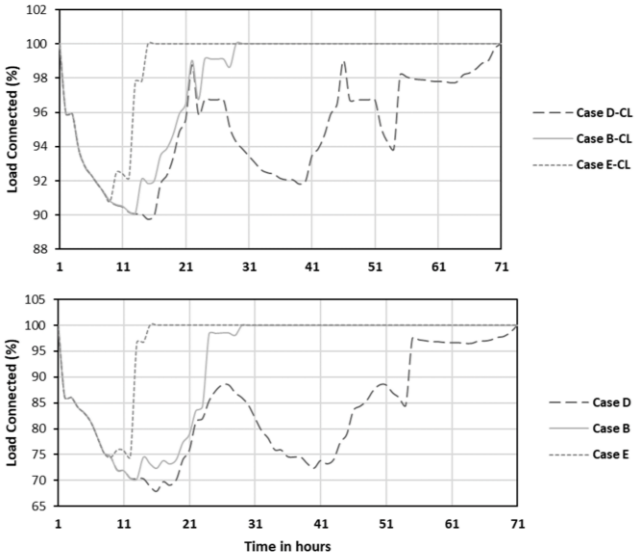

Figure 4.9 Resilience profile for Case D,B and E

Case E has the best resilience profile among all three cases. Case D shows the worst performance, as case D is assumed to have least amount of repair personnel. Increasing repair personnel decreases the restoration time of the system . The second and third dip observed is due to the load profile for 2nd day as the extreme event lasted for more than 24 hours. Figure 4.9 shows that the recovery of the network can be greatly improved if needed amount of repair personnel can be made available. Figure 4.10 shows the recovery rate, Π (kW/hr) of all three cases. The results of Figure 4.10 shows that Case E makes the fastest recovery among the three cases. A rapid response team filled with repair personnel should prove to be an efficient operational strategy against extreme winds.

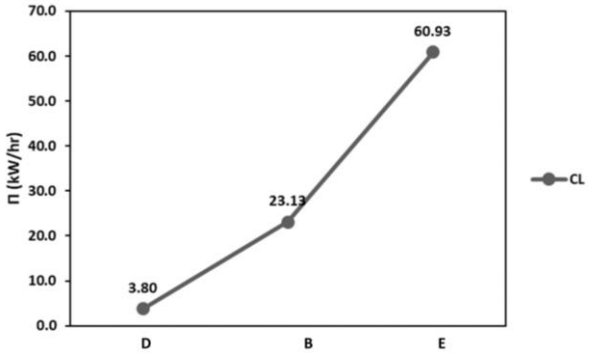

Figure 4.10 Π(kW/hr) for Case D,B and E

Table 4.3 shows the EENS (MWhr/int) summarizing all of the cases involving infrastructural recovery strategies.

Table 4.3 EENS (MWhr/int) for different infrastructural recovery strategies

Cases	EENS (MWhr/int)
A	54.64
B	39.41
C	24.41
D	59.38
E	35.53

Among different infrastructural measures, using materials of higher structural fragility for distribution poles shows that least amount of energy is lost. The results associated with the number of repair personnel quantifies the benefits of hiring additional personnel, and can be used to make hiring decisions.

While the study results from the implementation of different remedial strategies improves the resilience of the distribution network, it is important to consider the scope of the strategies discussed. Case E aims to improve resiliency by providing better response strategies, but does not provide a scenario where the network can withstand an extreme event. Case C provides results to show that investment in using material of higher structural fragility is an effective proactive strategy, and provides scenarios where the system is unaffected by extreme winds of lower intentisites which in fact are more probable in occurrence. Case E is not proactive in nature, and is a corrective strategy while case C is a preventive strategy. Each strategy has a different response from the system, and therefore, it is important to make a balanced investment decisions to ensure a resilient distribution network.

4.4.2. Operating strategies with DERs

This section assesses the change in resiliency of the system with the application of DERs. DERs form microgrid where possible, and ensure continuity of power, when the power from the utility supply fails. In this way, DERs help in restoring power to the isolated section of the network, reducing the overall load lost in the system. In this study, case F is facilitated

with DERs in the network that form an islanded microgrid when possible. The type of DERs present and the power supplied is given in Table 4.1. Case F is compared with the base case, Case B which does not include DERs. The result shown in Figure 4.11 shows that the system incorporated with DERs has better resiliency profile than the system with no DERs in place. Figure 4.12 shows the recovery rate, Π(kW/hr) for the two cases.

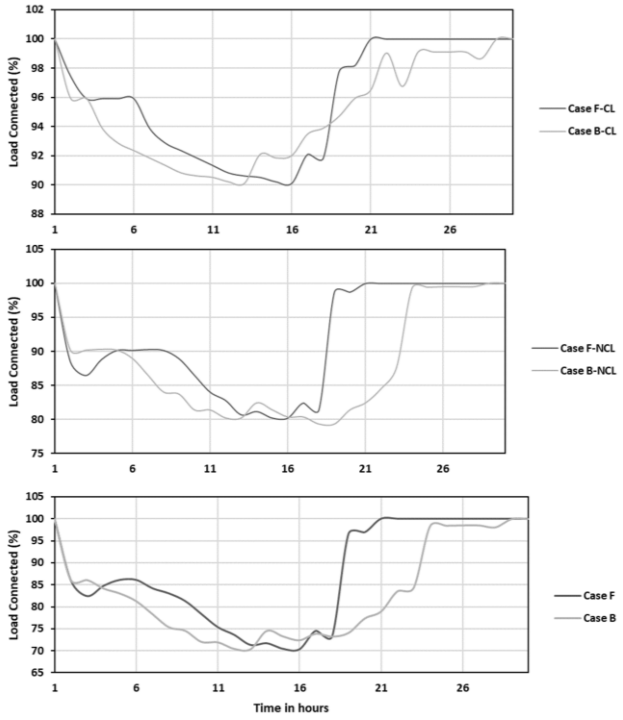

Figure 4.11 Resilience profile for Case F and B

Figure 4.12 also agrees with the conclusions made from Figure 4.11. The system with Figure 4.12 also agrees with the conclusions made from Figure 4.11. The system with DERs shows faster restoration than the system with no DERs in place. DERs also makes the system independent and increases the flexibility of the system, as it ensures continious supply of load if the transmission line fails. DERs can be an effective strategy that provides faster response to the system that has succumbed due to extreme winds ensuring load supply forming microgrids.

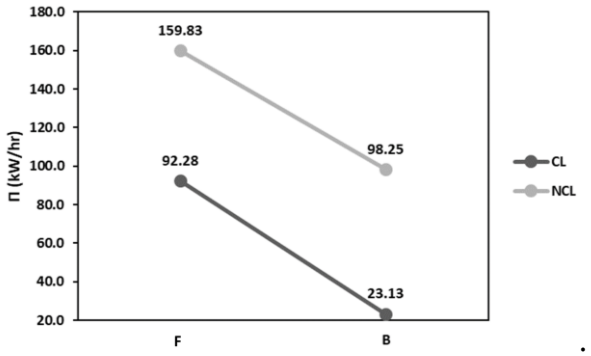

Figure 4.12 Π(kW/hr) for Case F and B

A network with DERs has the fastest recovery among all of the cases, suggesting that network with DERs are more resilient than others. However, inclusion of DERs in a network requires additional financial burden to the authorities, that can sometimes outweigh the benefits of having DERs. It should however be noted that the DERs can only supply power to the load points if the poles and lines responsible to the power delivery are intact. It is therefore important to have a proper balance in the invesetment in DERs and in pole hardening. Studies as presented in this paper can be carried out on the system to determine the impacts of such investments and make a rational decision. The investment in pole hardening alone cannot mitigatge power outatges from extreme wind events if the upstream transmission feeders are not hardened for the same objectives.

4.4.3. Transmission line fragility and its impact on distribution system resiliency

A resilient distribution network will not suffice if the transmission network is not resilient enough against extreme winds. It is therefore important to consider the impact of transmission line fragility on distribution system resiliency. The upstream transmssion line feeding the test system is shown in Figure 4.4. The transmission lines in the vicinity of the distribution system would also be exposed to the extreme wind event that affects the distribution system. The scope of this study is to understand the impact of the fragility of the transmission line on distribution system.

This section models the fragility of transmission network poles using emperical equation derived from [[1]]. Equation (4.32) gives the equation for structural fragility of transmission network poles, where x_i is assumed to be the wind speed at any duration of time for which the failure probability of the pole is to be obtained..

$$p_{f,txn}(W_s = x_i) = 2 * 10^{-7} e^{0.0834 x_i} \quad (4.32)$$

The study considers two cases. Case B-txn is the base case considering the exposure of the transmission line to the extreme events. Case G assumes that the poles are 30% more fragile due to lack of maintenance from wear and tear Figure 4.13 shows the resilience profiles of the network in the two cases.

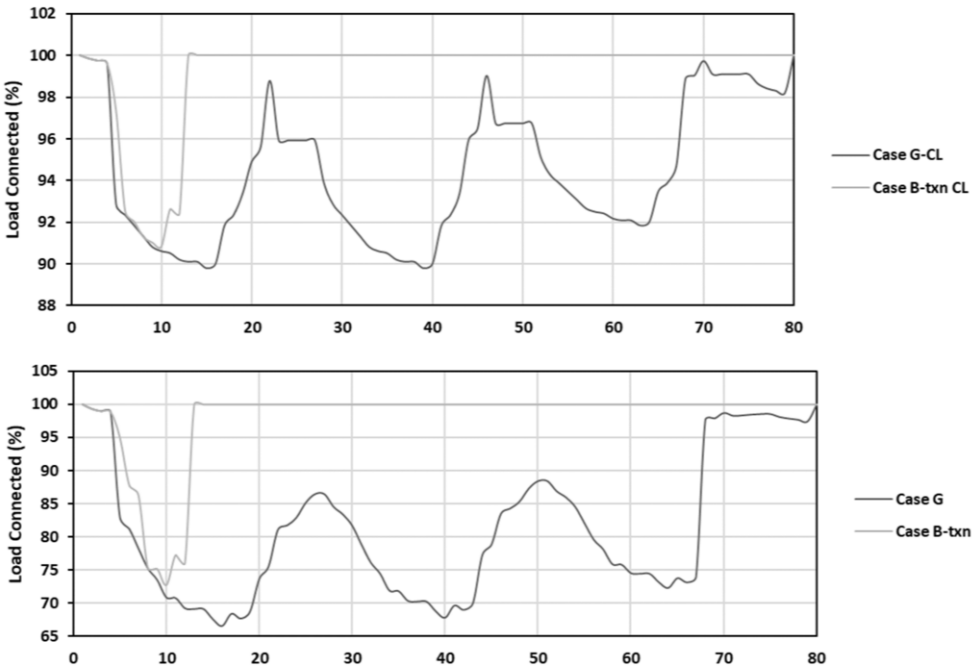

Figure 4.13 Resilience profile for Case I and B

Table 4.4 shows that large amount of energy is lost in a system with poor transmission line fragility.

Table 4.4 EENS (MWhr/int) for Case I and B-txn

Cases	EENS (MWhr/int)
G	66.67
B-txn	46.58

The drastic change in profiles in both the cases, is due to very poor fragility of poles in Case G. This shows that the improvement in resiliency of the distribution system is not guaranteed if the fragility of the transmission network supplying power to the distribution network is poor. In this case, a distribution system equipped with DERs can restore power to the distribution system loads until the transmssion lines are restored.

4.5. Conclusion

Extreme winds is one of the most frequently occurring extreme events threatening power distribution systems and is responsible for prolonged outages. This paper presents a

resiliency assessment framework against extreme winds and explores various resiliency enhancement strategies.

The paper illustrates the application of the proposed framework on the IEEE 69 Bus test system to assess the resiliency impacts of implementing a number of remedial strategies both at the planning and the operational phases. If sufficient investment for resiliency is made in the planning phase, the operating phase can avail the installed resources to mitigate the losses from the extreme wind event. If sufficient investment in pole hardening is made using pole of higher structural integrity such as steels, then it was found that the network could easily ride through windstorms of lower intensities, and bear minimal damages to the network on wind storms with higher intensities. Also, the paper recommends the implementation of 'rapid response unit' that consists of repair personnel ready to be deployed, after an extreme wind event has occurred as the result showed significant improvement in system down time when such units were deployed. The paper also shows that, if significant investment in DERs can be made in the planning phase, then considerable load loss can be minimized, and system down time can be reduced by deploying DERs in the operating phase. It was also found that the investment in DERs must also be accompanied with investment in selected pole hardening in order to deliver the distributed energy to the critical and non-critical loads in that priority order. The paper also explored the dependency of distribution network on the structural strength of transmission lines and found that the resiliency of distribution network cannot be guaranteed without a holistic approach, that uses policies and frameworks to incorporate strategies that strengthens both the transmission and distribution network. The distribution systems fed from fragile transmission network can benefit significantly from investment in DERs, as the decisions on transmission system investments are outside the reach of distribution system owners.

Preventive strategies such as pole hardening helps the network ride through extreme events with minimum damages, but do not provide any support when the structural integrity of the transmission network supplying the power to the grid is weak. Corrective strategies such as deployment of DERs, do not provide the ability to withstand the extreme events, but provide rapid restoration to the network. Moreover, deployment of DERs increases the independency of the network on the structural fragility of the transmission line supplying power to the network. Each strategy has a different response, and each strategy must be devised according to the need for the network, so the paper recommends for a balanced investment decisions to ensure a resilient distribution network. It is believed that the studies as presented in this paper

can be carried out on a distribution system of interest to determine the impacts of such investments and make a rational decision.

4.6. Reference

[1]. R. J. Campbell, “Weather-related power outages and electric system resiliency,” Congr. Res. Serv., Washington, DC, USA, Tech. Rep R42696, Aug. 2012. [Online]. Available:http://www.fas.org/sgp/crs/misc/R42696.pdf. Accessed on: Feb. 05, 2019

[2]. Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1289-1310, July 2017.

[3]. J.-P. Watson et al., “Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the united states,” Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2014-18019, 2014.

[4]. Min Ouyang, Leonardo Dueñas-Osorio, Multi-dimensional hurricane resilience assessment of electric power systems, Structural Safety, Volume 48, 2014, Pages 15-24.

[5]. H. Gao, Y. Chen, Y. Xu and C. Liu, "Resilience-Oriented Critical Load Restoration Using Microgrids in Distribution Systems," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2837-2848, Nov. 2016.

[6]. H. Farzin, M. Fotuhi-Firuzabad and M. Moeini-Aghtaie, "Enhancing Power System Resilience Through Hierarchical Outage Management in Multi-Microgrids," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2869-2879, Nov. 2016.

[7]. S. Ma, L. Su, Z. Wang, F. Qiu and G. Guo, "Resilience Enhancement of Distribution Grids Against Extreme Weather Events," in IEEE Transactions on Power Systems, vol. 33, no. 5, pp. 4842-4853, Sept. 2018

[8]. M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides and N. D. Hatziargyriou, "Metrics Quantification of Operational and Infrastructure Resilience in Power Systems," in IEEE Transactions on Power Systems, vol. 32, no. 6, pp. 4732-4742, Nov. 2017.

[9]. M. Panteli, D. N. Trakas, P. Mancarella and N. D. Hatziargyriou, "Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2913-2922, Nov. 2016.

[10]. M. Panteli, C. Pickering, S. Wilkinson, R. Dawson and P. Mancarella, "Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures," in IEEE Transactions on Power Systems, vol. 32, no. 5, pp. 3747-3757, Sept. 2017.

[11]. S. Yao, P. Wang and T. Zhao, "Transportable Energy Storage for More Resilient Distribution Systems With Multiple Microgrids," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3331-3341, May 2019.

[12]. A. Arif, S. Ma, Z. Wang, J. Wang, S. M. Ryan and C. Chen, "Optimizing Service Restoration in Distribution Systems With Uncertain Repair Time and Demand," in IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 6828-6838, Nov. 2018.

[13]. W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang and B. Zeng, "Robust Optimization-Based Resilient Distribution Network Planning Against Natural Disasters," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2817-2826, Nov. 2016.

[14]. Y. Xu, C. Liu, K. P. Schneider, F. K. Tuffner and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," in IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 426-437, Jan. 2018.

[15]. C. Yuan, M. S. Illindala and A. S. Khalsa, "Modified viterbi algorithm based distribution system restoration strategy for grid resiliency," in IEEE Transactions on Power Delivery, vol. 32, no. 1, pp. 310-319, Feb. 2017.

[16]. Z. Wang and J. Wang, "Self-healing resilient distribution systems based on sectionalization into microgrids," in IEEE Transactions on Power Systems, vol. 30, no. 6, pp. 3139-3149, Nov. 2015.

[17]. S. Poudel and A. Dubey, "Critical load restoration using distributed energy resources for resilient power distribution system," in IEEE Transactions on Power Systems, vol. 34, no. 1, pp. 52-63, Jan. 2019.

[18]. P. Bajpai, S. Chanda and A. K. Srivastava, "A novel metric to quantify and enable resilient distribution system using graph theory and choquet integral," in IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2918-2929, July 2018.

[19]. S. Mousavizadeh, M. Haghifam and M. Shariatkhah, “A linear two-stage method for resiliency analysis in distribution systems considering renewable energy and demand response resources,” Applied Energy, Vol. 211, pp. 443-460, 2018

[20]. Chanda, S., & Srivastava, A. K. (2016). Defining and enabling resiliency of electric distribution systems with multiple microgrids. IEEE Transactions on Smart Grid, 7(6), 2859-2868.

[21]. Gautam, P., Piya, P., & Karki, R. (2020). Resilience Assessment of Distribution Systems Integrated With Distributed Energy Resources. IEEE Transactions on Sustainable Energy, 12(1), 338-348.

[22]. Bie, Z., Lin, Y., Li, G., & Li, F. (2017). Battling the extreme: A study on the power system resilience. Proceedings of the IEEE, 105(7), 1253-1266.

[23]. Mukherjee, S., Nateghi, R., & Hastak, M. (2018). Data on major power outage events in the continental US. Data in brief, 19, 2079.

[24]. Wang, Z., & Wang, J. (2015). Self-healing resilient distribution systems based on sectionalization into microgrids. *IEEE Transactions on Power Systems*, *30*(6), 3139-3149.

[25]. Ouyang, M., & Duenas-Osorio, L. (2014). Multi-dimensional hurricane resilience assessment of electric power systems. Structural Safety, 48, 15-24

CHAPTER 5: SUMMARY AND CONCLUSIONS

It is very important to maintain the reliability of distribution systems within acceptable levels in order to minimize power outage costs to consumers, and to sustain economic developments. Reliability assessments are therefore routinely carried out to ensure distribution systems meet specified standards. These studies however do not incorporate natural or man-made extreme events that can result in catastrophic infrastructure failures, power outages and economic losses to the society. It has been evidenced that certain types of extreme events are occurring with increased frequency, and therefore, the resiliency of distribution systems against these events has become an important area of research and analysis.

The transition from traditional to a modern distribution system has benefited the DSOs providing them with a microscopic spectacle to ensure a reliable supply of electricity. This has been possible by the integration of physical and cyber layer of the distribution network. However, increased integration of cyber and physical layer has exposed many interdependencies in the network. These vulnerable points are often exploited in the form of cyber-attacks, which has caused financial and societal repercussions in the power system. Moreover, as the increase in global warming is being made apparent by scientists worldwide, it has aggravated earthquake, hurricane/tornadoes, floods, ice storms, etc. Extreme winds is one of the most frequently occurring extreme event that is known to threaten the distribution system and is responsible for wide scale outages. These man-made and natural events calls for a resilient grid that can withstand such extreme events to a considerable degree without any noticeable damage to the system. In regards to this, the thesis explored the resiliency of a distribution system to cyber-attacks, and extreme wind along with strategies to enhance the resiliency to the aforementioned extreme events, with the development of novel models, methodologies and frameworks. The thesis also explored reliability and resiliency, along with their assessment techniques with the aim of developing a unanimous understanding of the fundamentals of power system resiliency and creating a clear distinction between reliability and resiliency.

The increase in high impact, low probability events, and its effect on the grid have been observed and accepted by power system planners, operators, regulatory authorities, and policymakers. This has brought interest in the subject, and approaches on how to assess and quantify resiliency. This thesis provides a review of the definition and governing principles of resilience in the power system. The increasing interconnectedness and advent of the cyber-physical era and its effect on the grid are also discussed. In distinctions between reliability and resiliency, this thesis also addressed the previous works done in light of the evaluation of the reliability of the power system in extreme events that at the present have fallen under the scope of resiliency. Power system resiliency evaluation greatly depends on the type of event and as event are recognized as high impact, low probability events, it is difficult to obtain abundant data. Even if such data is available for a specific extreme event, it is likely unusable considering the nature of the events. The thesis also presented literatures on the available modelling techniques that do not rely on past data but provide efficient and reliable models. The thesis elaborated on the relationship between reliability and resiliency and discussed different measures to achieve a reliable and resilient distribution system.

The thesis then presented a detailed study of the impact of a cyber-attack on the reliability and resiliency of the power system. It presented a novel methodology to model cyber-attacks based on state estimation, and a novel reliability and resiliency assessment methodology to assess the impact of False Data Injection Attacks (FDIAs) on the distribution grid with the help of Expected EENS for cyber-attack. A cyber-attack such as FDIAs resulted in significant power outages. The probability of trouble of the developed attack is widespread throughout all of the load points. It was found that the frequency and the severity of the cyber-attacks rose as the distribution grids transitioned into cyber-physical systems. The thesis also suggested for a proper investigation of the cyber-physical interdependencies, and appropriate investment in system resiliency against cyber-attacks.

The resiliency indices framework- "Φ, E, EENS, Π" provided measures to assess the impact of extreme event in time sequence at the different stages of a system, and quantified the system's ability to absorb, adapt and recover from the event. Results showed that as the delay in identifying a cyber-attack increased, the system degradation increased simultaneously. The results concluded that importance must be given on immediate identification of the problem for minimum damage. Keeping this in mind, the thesis also developed an infrastructural resiliency enhancement strategy by implementing a bad-data detection algorithm to identify any sudden changes in the system. The bad-data detection strategy used the difference between the observed measurement, and the previous measurement, and compared it to a value from

chi-squared distribution table for identification of false data. The result showed significant improvement in the distribution system from investment in such strategies. It is known that investment for different type of HILP events are going to affect their impacts on the power system in different ways. The thesis suggested the concerned authorities and regulatory bodies to 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.

Also recognizing that extreme wind is one of the most occurring extreme event, the thesis then developed resiliency assessment framework for the distribution system against extreme wind. The results showed that a resilient grid could only be established if the resiliency is envisioned in both planning and operating phase of the network. The results found that if sufficient investment is made in the planning phase of the network, the operating phase can benefit from the resources made available to them. The thesis then presented infrastructural and operational enhancement strategies along with their application in the distribution system. The results showed that investment in pole hardening can help the distribution grid ride through extreme winds sustaining minimum damages. In addition, the thesis recommends the implementation of 'rapid response unit' that consists of repair personnel ready to be deployed after the extreme wind has occurred. The results showed that rapid response unit could significantly help reduce system down time, and restore loads to the load points quickly. The thesis also showed that the deployment of DERs could help reduce system down time and help in quick restoration after extreme wind has occurred. The thesis also incorporated transmission line into the study. The results showed that the resiliency of the distribution system could not be guaranteed if the structural fragility of the transmission line is poor. In cases like these, the results showed that a distribution network equipped with DERs had the best response.

The strategies that are employed in a distribution network are dependent on the need of the network. For example, if the system needs a systemic upgrade, then pole hardening shows the best results to achieve a resilient network against extreme wind. DERs also shows good responses against extreme wind. Unlike pole hardening which are preventive strategies, DERs are corrective in nature and do not help avoid extreme winds, but helps significantly in restoring the load points. In addition to that, deployment of DERs increase the independency of the network, and shows best response in network that are supplied with poor transmission lines. In cases where a systemic upgrade is not required or possible, the thesis recommends implementation of rapid response unit, which being a corrective strategy helps in quick restoration of the load points. Each strategy has a different response, and each strategy must be devised according to the need of the network so the paper recommends for a balanced

investment decisions to ensure a resilient distribution network. For future work, the thesis recommends exploring the study on justifiable investments to improve resiliency, and to assessing the cost and worth of implementing different types of remedial strategies against extreme wind events.

The study of impact of two different extreme events on the distribution system revealed important behaviors of resiliency. In cyber-attack, the success probability of the attack is in its discretion, so there is almost zero pre-notice of the event in this case. Therefore, the effect is also immediately apparent, and the response of the distribution system is completely dependent on the time taken to identify the occurrence of cyber-attack. On the other hand, in case of extreme wind, pre-notice can come several hours to days ahead. In this scenario, the distribution system can prepare accordingly, prioritizing load shed in less critical areas etc., but cannot start any restoration process before the event subsides. The response too depends on the resource available to the utility operators i.e. number of repair personnel, availability of DERs etc. It is also evident that the presence of DERs or a large number of repair personnel is not going to help mitigate distribution system facing cyber-attack. Likewise, implementation of bad-data detection strategies that can effectively mitigate FDIAs also cannot help in preventing the system in case of extreme winds. Resiliency enhancement is going to be dependent on the type of extreme event, and there is no general formula for achieving resiliency. Rather, resiliency of a system can be obtained observing the type of extreme events the system needs protecting from, and making balanced and well-informed investments to protect the system. It is believed that the methodologies presented in this thesis and the case studies illustrated will provide useful tools and indicators to distribution system planners, operators and policy makers to make decisions on enhancing the resilience of power distribution systems for extreme events that are known to endanger their jurisdictions.