2024

Modeling and Mitigating Power Grid Vulnerabilities: A Comprehensive Analysis of Renewable Energy Integration, Cascading Failures, and Microgrid Resilience

Saikat Das
Virginia Commonwealth University

Modeling and Mitigating Power Grid Vulnerabilities: A Comprehensive Analysis of Renewable Energy Integration, Cascading Failures, and Microgrid Resilience

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

By

Saikat Das

B.Sc. in Electrical and Electronic Engineering, Bangladesh University of Engineering and Technology, Bangladesh

Director: Zhifang Wang, Ph.D.

Associate Professor, Department of Electrical and Computer Engineering

Virginia Commonwealth University

Richmond, Virginia

May, 2024

Dedication

To my beloved wife and my best friend, ***Samprity***. I am incredibly lucky to have you by my side.

Acknowledgements

I would like to express my heartfelt gratitude to my advisor, Dr. Zhifang Wang, for her unwavering support, invaluable guidance, and constant encouragement throughout my Ph.D. journey. Her mentorship has been instrumental in shaping my academic and professional growth, and I am profoundly grateful for that.

I also wish to extend my sincere appreciation to my committee members, Dr. Yanxiao Zhao, Dr. Yuchi Motai, Dr. Hongsheng Zhou, and Dr. Yanjun Qian, for their insightful comments, constructive feedback, and invaluable suggestions.

I am deeply indebted to my parents and sister for their unconditional love and support. Their belief in me has been a source of strength and motivation throughout this journey.

I would also like to acknowledge the College of Engineering at VCU for providing me with access to resources and facilities that have facilitated my research endeavors.

TABLE OF CONTENTS

Abstract ... 12

1. Introduction ... 15

1.1. Motivation ... 15

1.2. Literature Review ... 20

1.2.1. Cascading Failure Simulation Model ... 20

1.2.2. Cascading Failure Risk Analysis ... 22

1.2.3. Microgrid Resilience ... 23

1.3. Contribution ... 25

1.3.1. Vulnerability Analysis of Electric Grid Networks ... 25

1.3.2. Statistical Analysis of Cascading Failure Risks ... 26

1.3.3. Impact of Data Loss and FDIAs on Microgrid Resilience ... 27

1.4. Structure of the Dissertation ... 27

2. Power Grid Vulnerability Analysis with Rising Renewables Infiltration ... 29

2.1. Introduction ... 29

2.2. System Model ... 29

2.2.1. Uncertainty modelling ... 30

2.2.2. Line flow based on AC power flow ... 30

2.2.3. Unscented transformation ... 31

2.2.4. Tripping mechanism and relay model ... 32

2.3. Modified OPF Algorithm ... 33

2.3.1. Objective function ... 33

2.3.2. Constraints ... 34

2.3.3. Algorithm ... 35

2.4. Simulation Results and Discussion ... 38

2.4.1. IEEE 118 Bus System ... 39

2.4.2. IEEE 300 Bus System ... 44

2.4.3. 500 bus case (ACTIVSg500) ... 47

2.5. Summary 51
3. Cascading Failure Risk Analysis of Electrical Power Grid 53
3.1. Introduction 53
3.2. Risk Analysis of Cascading Process from Historical Utility Data 53
3.3. Risk Analysis from Simulated Data 56
3.3.1. Simulation Model 56
3.3.2. Initial Line Tripping Mechanism 57
3.4. Result and Discussion 60
3.4.1. Test Case: ACTIVSg500 61
3.4.2. Test Case: AutoSyngrid case 66
3.5. Summary 73
4. Microgrid Resilience 74
4.1. Introduction 74
4.2. Microgrid Overview 75
4.2.1. Microgrid Components 76
4.3. Cyber Attack Types and Targets in Microgrid 77
4.3.1. Attack Types 77
4.3.2. Attack Targets 78
4.4. False Data Injection Attack Model 79
4.5. Microgrid Operation Strategy 82
4.5.1. Optimization-based Energy Management System 83
4.5.2. Adaptive Control Scheme 84
4.6. Simulation Model 85
4.6.1. Simulating Data Loss in Battery Command 86
4.6.2. Simulating FDIA in EMS 88
4.7. Result and Analysis 89
4.7.1. Impact of Data Loss 89
4.7.2. Impact of FDIA 100
4.8. Summary 106

5. Conclusion and Future Work 108

Reference 111

List of Publications 124

Vita 126

LIST OF TABLES

Table I. Structure of Dissertation 28

Table II. Vulnerability impacts evaluation (Scn 1)-IEEE118 39

Table III. Vulnerability impacts for a specific contingency-118 bus 43

Table IV. Vulnerability impacts evaluation (Scn 2)-300 bus 44

Table V. Vulnerability impacts evaluation (Scn 1)-500 bus 47

Table VI. Overall analysis in three test cases 49

Table VII. Non-uniform probability definition of initial line trips according to the loading level 58

Table VIII. Non-uniform probability definition of initial line trips according to the shortest path 59

Table IX. Non-uniform probability definition of initial line trips according to the connectivity . 60

Table X. Weights of different loading level 61

Table XI. Mean number of outages in a cascade for ACTIVSg500 system 63

Table XII. Mean duration of a cascade for ACTIVSg500 system 65

Table XIII. Mean load shedding percentage of a cascade for ACTIVSg500 system 65

Table XIV. Mean number of outages in a cascade for the ASGWECC_500_1 system 68

Table XV. Mean duration of a cascade for ASGWECC_500_1 system 69

Table XVI. Mean load shedding percentage of a cascade for ASGWECC_500_1 system 70

Table XVII. Overall comparison of cascading failure risk analysis for the BPA system and the synthetic test cases 71

Table XVIII. Comparison of mean load shedding percentage between two synthetic test cases . 72

Table XIX. Comparison of average grid electricity cost for varying PV penetration and data loss rate in microgrid 98

Table XX. Comparison of average BESS cost for varying PV penetration and data loss rate in microgrid 99

Table XXI. Summary of Microgrid Operation Under Various FDIA Scenarios 105

LIST OF FIGURES

Figure 1. Flowchart of the modified OPF 36

Figure 2. Overall overview of CF simulation 37

Figure 3. Average load shedding amount for increasing RE penetration (IEEE 118 bus system) 41

Figure 4. Number of tripped lines for increasing RE penetration (IEEE 118 bus system) 42

Figure 5. Cascading failure evolution for a specific contingency 43

Figure 6. Average load shedding amount for increasing RE penetration (IEEE 300 bus system) 45

Figure 7. Number of tripped lines for increasing RE penetration (IEEE 300 bus system) 46

Figure 8. Average load shedding amount for increasing RE penetration (500 bus system) 48

Figure 9. Number of tripped lines for increasing RE penetration (500 bus system)................... 49

Figure 10. Overall vulnerability analysis 50

Figure 11. Probability distribution with exponential fitting for BPA data 56

Figure 12. Probability distribution of the number of outages in a cascade for the ACTIVSg500 system 63

Figure 13. Probability distribution of the cascade duration for the ACTIVSg500 system 64

Figure 14. Probability distribution of the load shedding percentage of a cascade for the ACTIVSg500 system 65

Figure 15. Probability distribution of the number of outages in a cascade for the ASGWECC_500_1 system 67

Figure 16. Probability distribution of the cascade duration for the ASGWECC_500_1 system . 69

Figure 17. Probability distribution of the load shedding percentage of a cascade for the ASGWECC_500_1 system 70

Figure 18. Working flow for the optimization-based EMS 87

Figure 19. Working diagram for adaptive control schemes for microgrid operation 88

Figure 20. A specific case of 10% data loss scenario for a 10% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time 90

Figure 21. A specific case of 10% data loss scenario for a 50% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time 91

Figure 22. A specific case of 10% data loss scenario for a 100% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time 91

Figure 23. A specific case of 50% PV penetration scenario with no data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command 92

Figure 24. A specific case of 50% PV penetration scenario with 10% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command 93

Figure 25. A specific case of 50% PV penetration scenario with 30% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command 94

Figure 26. A specific case of 50% PV penetration scenario with 50% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command 95

Figure 27. A specific case of 50% PV penetration scenario with 100% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command 96

Figure 28. Comparison of grid electricity cost for the microgrid with 10% PV penetration with varied amounts of data loss 97

Figure 29. Comparison of BESS cost for the microgrid with 10% PV penetration with varied amounts of data loss 97

Figure 30. Comparison of average grid electricity cost for varying PV penetration and data loss rate in microgrid 98

Figure 31. Comparison of average BESS cost for varying PV penetration and data loss rate in microgrid 98

Figure 32. Microgrid Topology 101

Figure 33. (a) Actual load profile, (b)Grid electricity price, (c) PV power output during a day 101

Figure 34.(a) PV generation data under 20% FDIA, (b) Load profile data under 20% FDIA . 102

Figure 35. (a) SOC of BESS1, (b) SOC of BESS2, (c) Power profiles of PV generation, battery output, grid electricity, generator output and total load over time using hybrid EMS method under FDIA type 1 103

Figure 36. Total electricity cost and final SOC with increasing intensity of FDIA type 1(a) & type 2(b) in 24-hour microgrid operation for optimization-based EMS 104

Figure 37. Total electricity cost and final SOC with increasing intensity of FDIA type 1(a) & type 2(b) in 24-hour microgrid operation for hybrid EMS 105

ABSTRACT

MODELING AND MITIGATING POWER GRID VULNERABILITIES: A COMPREHENSIVE ANALYSIS OF RENEWABLE ENERGY INTEGRATION, CASCADING FAILURES, AND MICROGRID RESILIENCE

By Saikat Das, Ph.D.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

Virginia Commonwealth University, 2024

Director: Zhifang Wang, Ph.D., Associate Professor, Department of Electrical and Computer Engineering

In today's modern power systems, rapid integration of renewable energy and the emergence of microgrid technology emphasize the necessity for a comprehensive understanding of vulnerabilities and robust defense mechanisms. This thesis sets out on a journey to uncover the intricacies of power grid dynamics, cascading failures, and microgrid operations. It proposes practical mitigation strategies to fortify power systems against potential disruptions and cyber threats, thereby paving the way for a more sustainable and secure energy future.

The research begins with an exploration of power grid vulnerabilities amidst the increasing integration of renewable energy sources, laying the foundation for a comprehensive analysis. Power grids' vulnerability to cascading failures with respect to the penetration level of renewable energy into the grid has been analyzed. A novel power balance technique is employed for cascading failure analysis and power grid vulnerability measurement. Simulation results indicate

that the growing penetration of renewable energy has a proportionally higher impact on grid vulnerability to cascading failures due to increased uncertainties injected into the grid. After a certain level of renewable energy penetration, some systems may deteriorate rapidly, necessitating preventive measures when the penetration level exceeds this threshold. This initial investigation sets the stage for a deeper exploration into cascading failure risk analysis. The subsequent segment digs into cascading failure risk analysis by statistically analyzing key metrics such as line outages per cascade, cascade duration, and load shedding amounts. The analysis is based on historical utility data and simulation data of synthetic test cases, building upon the simulation model developed in the initial exploration of power grid vulnerabilities. Both uniform and non-uniform probability distribution functions have been considered for the initial line trips in the cascading failure simulation to determine which function better approximates the cascading failure risks of the real-world power grid. The combination of empirical and simulated analyses provides a comprehensive understanding of cascading processes, illuminating key risk factors and offering avenues for effective preventive measures.

Shifting focus to microgrid resilience, the research meticulously explores data integrity attacks. Through a comprehensive simulation model, vulnerabilities are explored, and mitigation strategies are devised to safeguard microgrid operations against data integrity attacks like data loss and false data injection. A multi-layered microgrid simulation model with an optimization-based energy management system is developed to investigate the impact of renewable energy penetration and data loss in battery command. The analysis of false data injection attacks' impact on microgrid operation introduces a hybrid approach to ensure stability and reliability across diverse scenarios. Realistic attack models targeting load profiles and renewable generation data reveal potential load balance discrepancies during islanded microgrid operation under these attacks. By integrating optimization-based energy management with adaptive control schemes, the proposed hybrid approach ensures stable microgrid operation in various conditions. This research lays the groundwork for strengthening microgrid resilience against cyber threats by integrating additional techniques for real-time FDIA detection and resolution, thereby contributing to the ongoing advancement of microgrid cybersecurity frameworks and benefiting the broader research community.

Overall, this thesis represents a comprehensive exploration of power grid vulnerabilities, cascading failures, renewable energy integration, and microgrid resilience. By combining theoretical analysis with practical application, it seeks to strengthen the resilience and security of energy systems, ensuring their sustainability amid evolving challenges.

1. INTRODUCTION

The ongoing evolution of modern power systems is marked by significant changes driven by increasing electricity demand and the imperative to curb carbon emissions for sustainable development. This dual pressure has led to a rapid integration of renewable energy sources into existing power grids and the rise of microgrid technology, reshaping their dynamics. In the midst of modern power systems undergoing rapid changes, a pressing need arises: the need to comprehend vulnerabilities and establish resilient defense mechanisms. Our research sets out on a path to dig into the complexities of power grid dynamics, cascading failures, and microgrid operations, while also introducing viable mitigation strategies.

1.1. Motivation

The motivation for this dissertation stems from the dynamic landscape of modern power systems undergoing significant transitions. With the escalating demand for electricity and the imperative to limit carbon emissions to achieve sustainable development goals, there is a rapid integration of renewable energy (RE) sources into the existing power grid [1]. However, while RE sources offer promising avenues for clean energy generation, this integration introduces new challenges and complexities due to their variable and intermittent nature. Unlike traditional fossil fuel-based power generation, which can be controlled and dispatched according to demand, RE generation is highly dependent on weather conditions and other environmental factors. As a result, the integration of RE introduces significant uncertainty into the power grid. For example, sudden changes in weather patterns can lead to fluctuations in RE generation, causing rapid changes in power supply that the electric grid must accommodate. This variability can strain the stability and reliability of the grid, particularly during periods of high RE penetration. Furthermore, the dynamic nature of RE generation increases the likelihood of cascading failures (CF) in interconnected power systems. A cascading failure occurs when the failure of one part or element of the system triggers a chain reaction, causing other parts or elements to fail in succession. In the context of RE integration, sudden fluctuations in RE can overload transmission lines or destabilize grid operations, leading to cascading failures that can result in line outages and, in severe cases, blackouts.

Therefore, understanding the impact of RE penetration on the vulnerability of the grid to CF is crucial to grid modernization for ensuring the reliability and stability of the power system. By analyzing the dynamics of RE integration and its effects on grid operation, researchers and practitioners can develop strategies to mitigate the risks associated with CF and enhance the resilience of the power grid in the face of increasing RE penetration.

Cascading failure is a well-documented phenomenon in interconnected power grids, where the failure of one part or element of the system can propagate to other parts, leading to widespread disruptions [2]. Although CFs are not frequent occurrences, they have catastrophic effects when they occur, often resulting in large-scale blackouts [3]. Therefore, it is essential to research and analyze these events to understand their underlying mechanisms and mitigate their risks.

Utility companies store extensive daily outage data, which serve as valuable resources for researchers studying CFs. By analyzing historical outage data, researchers can quantify the risks associated with cascading processes and identify potential mitigation strategies. Furthermore, existing simulation models can be validated using statistical parameters derived from past events, providing a benchmark for assessing the accuracy and effectiveness of these models. Studying real-world outage data and validating simulation models are essential steps in assessing and mitigating the risks posed by CFs in the power grid. By understanding the dynamics and risks of cascading processes and developing effective simulation model and mitigation strategies, we can enhance the reliability and resilience of the modern electrical power system.

The emergence of microgrids as integral components of the smart grid adds another layer of complexity to the power system, reflecting the ongoing transitions in the modern power landscape. The transition towards a more decentralized power grid is driven by the introduction of distributed energy resources (DER), such as solar panels, wind turbines, and energy storage systems. This shift marks a departure from the traditional centralized power grid model towards a more distributed and resilient infrastructure.

Microgrids have emerged as a versatile solution to address the evolving needs of the power system. These small-scale power grids can operate independently or in parallel with the main grid, offering a range of benefits across various applications. From providing reliable power to remote communities to ensuring backup power for critical facilities like hospitals and data centers, microgrids play a crucial role in enhancing energy reliability and resilience.

Defined by the Department of Energy (DOE) as interconnected loads and distributed energy resources within clearly defined electrical boundaries, microgrids act as a single controllable entity with respect to the grid [4]. They operate in various modes, including grid-connected and island mode, and can even function off-grid in certain applications.

Microgrids are characterized as cyber-physical systems (CPS), enabling bidirectional communication of both information and electric power between utility providers and users [5]. By integrating smart grid technologies, microgrids optimize energy management, reduce peak load, and ensure a stable energy supply for critical loads. Additionally, they promote grid modernization and community participation in electricity supply while effectively managing renewable energy variability and providing ancillary services to the bulk power system.

However, the intermittent and uncertain nature of renewable energy sources presents significant challenges to the efficient operation of microgrids. To overcome these challenges and maximize the potential of renewable energy integration, energy management systems (EMS) play a crucial role in optimizing microgrid operations. Initially developed for large-scale grids, EMS technology has evolved to address the specific needs of smaller systems like microgrids [6], [7]. In the context of microgrids, EMS functions as control software, orchestrating the allocation of power among distributed generation (DG) units, energy storage systems, and loads. At its core, a microgrid EMS ensures economical load service and facilitates seamless transitions between grid-tied and islanded modes based on real-time conditions. By dynamically adjusting energy allocation in response to changing demand and generation patterns, EMS maximizes the utilization of available resources while maintaining grid stability and reliability. A sophisticated microgrid EMS must effectively coordinate the operation of DGs, energy storage systems, and loads to deliver high-quality, reliable, sustainable, and cost-effective energy services [8]. This involves optimizing energy dispatch, managing battery charging and discharging cycles, and implementing demand response strategies to balance supply and demand in real-time.

Data integrity attacks represent a growing concern for microgrid operation, posing additional threats to system reliability and security. These attacks involve the insertion or alteration of data within network traffic or data servers, aiming to deceive the EMS and trigger incorrect decisions [9]. As a cyber-physical system, the microgrid relies heavily on advanced information and communication technology to control electrical units and optimize operations. However, any failure or degradation of the cyber system can have significant repercussions, impacting voltage and frequency stability, power balance, and dispatch reliability. Among the various types of data integrity attacks, False Data Injection Attacks (FDIAs) stand out as particularly prominent in microgrid systems. These attacks can severely disrupt microgrid operation by compromising the integrity of data used for decision-making and control, potentially leading to widespread system failures and compromised grid reliability.

Another significant challenge that microgrids encounter is the potential loss of data within communication channels. This loss can stem from various factors, including network failures, cyber-attacks, or transmission errors. When critical information, such as battery control commands or load forecasting data, is compromised due to data loss, it can lead to adverse effects on microgrid operation, resulting in increased costs and decreased system reliability. Therefore, gaining a comprehensive understanding of the impact of data loss on microgrid operation is essential for designing robust and resilient energy management systems.

The critical importance of microgrids in ensuring uninterrupted power supply to critical loads and bolstering power system reliability emphasizes the need to evaluate and mitigate risks stemming from data integrity attacks. By comprehensively assessing the economic ramifications of data loss, both system operators and researchers can devise effective strategies to mitigate its adverse effects and improve the overall performance of microgrids. A thorough understanding of the vulnerabilities introduced by FDIA empowers stakeholders to proactively implement measures that fortify microgrid operation against potential disruptions. By integrating hybrid operation strategies capable of dynamically adjusting objectives to ensure reliable microgrid operation across various attack scenarios, operators can enhance system resilience and fortify defenses against potential cyber threats. Such proactive measures not only ensure the uninterrupted operation of critical infrastructure but also lay the groundwork for the seamless integration of new technologies into existing microgrid systems. By prioritizing resilience and adaptability, stakeholders can strengthen overall grid reliability and readiness for future technological advancements in the microgrid landscape.

1.2. Literature Review

1.2.1. Cascading Failure Simulation Model

The literature on CF mainly focuses on the modelling and analytical tools for a given network. In [10], the authors have provided a brief overview to cascading failure analysis in power systems, outlining various analytical models. Different aspects of cascading failures and current advancements in analysis tools and models have been discussed by examining their features. A great diversity of methodologies has been proposed aiming at modeling the cascading failures. Topological models in cascading failure analysis focus on network structure, analyzing node degrees, betweenness centrality, and path length to assess vulnerability. Initially, they emphasized topological properties [11–14], but modified models now incorporate electrical features like Kirchhoff's law and line impedance [15,16]. Maximum flow models, adapted from traffic analysis [17], identify vulnerabilities by considering maximum flow from source to sink nodes, with recent enhancements including node weights and multi-attribute evaluations [18–20]. High-level statistical models offer a simplified approach to analyzing cascading failure in power systems, prioritizing speed over detailed mechanisms. The CASCADE model, for instance, assumes random initial loads and redistributes load upon failure, accurately predicting total failures and blackout sizes [21,22]. Branching process models simulate failure propagation through interdependent components, providing fast computation speeds and approximate results similar to

CASCADE [23–25]. While these models lack detailed mechanisms, they offer general estimates of failure propagation and blackout size distribution.

The CF models found in the literature can be classified based on their method of simulating power system response during cascades of tripping events [26]. Two main approaches are commonly identified: dynamic transient models and quasi-steady state (QSS) models. In [27], a dynamic model is presented which can simulate various cascading outage mechanisms. Steady state models are more common in literature to study and evaluate CF process. In [28], [29], the mixed OPF-stochastic models are the examples of steady state CF model where DC power flow (DCPF) was used to reduce computational burden. As DC models resulted in large errors in flow estimation [30] for large networks, [31], [32], are among the models incorporates AC power flow in the simulation of CF. In the stochastic CF model in [32], conventional optimal power flow (OPF) is used in the power balance algorithm which failed to accurately evaluate the negative impacts introduced by RE on the grid vulnerability.

The highly variable nature of renewable generation is expected to significantly influence voltage profile dynamics, potentially altering grid behavior during cascading failures. In [33], the authors integrate frequency control dynamics into modeling cascading failures and evaluating power system robustness under high levels of renewable energy penetration. In [34], the authors propose a hybrid probabilistic modeling approach to address cascading overload failures in renewable integrated power grids, incorporating load flow balancing and transient stability assessment under the occurrence of multiple interval faults. The authors in [35], analyze power system vulnerability to cascading failures considering higher security criteria and renewable energy integration using a graph-based model, proposing evaluation indices to assess system vulnerability under varying operation states and generation uncertainty levels. Although modeling the cascading failure process in power grids is well-documented in the literature, there is a notable gap in research concerning the effects of stochastic renewable generation on grid vulnerability to cascading failures.

1.2.2. Cascading Failure Risk Analysis

To assess the risk of cascading failures, it is essential to not only rely on simulation models but also study past events documented by utility and power distribution companies. By using statistical parameters from historical data as a benchmark, existing simulation models can be effectively validated. In [36], the authors took a complex system approach to analyze the blackout risk of power transmission systems using the North American Electrical Reliability Council (NERC) data. In [37], the authors evaluated the statistics of cascading line outages spreading using utility data. In [38], the authors studied different algorithms for cascading failure analysis in the power grid. In [32], [39], the authors incorporated a cascading failure simulation model with ac power flow to show power systems' vulnerability to cascading failure with rising renewables integration. In [40], the authors investigated the distribution of cascaded outages by leveraging both historical data and a simulation model. They emphasized the importance of defining an appropriate mechanism for the initial line trip, which triggers the cascading failure process. Notably, the study adopted a uniform probability distribution function for the cascading failure analysis, emphasizing the significance of selecting suitable parameters for accurate simulation outcomes. However, the existing literature lacks comprehensive studies on cascading failure risk analysis that compare historical data with simulated data. Moreover, there is a notable gap in research concerning the mechanisms for the initial line trip during cascades, particularly comparing the effects of uniform and non-uniform distribution. Additionally, there is limited exploration into validating simulation models with real-world data, which is essential for ensuring the accuracy and reliability of the models used in assessing cascading failure risks.

1.2.3. Microgrid Resilience

The literature on microgrid EMS offers insights into strategies for optimizing microgrid operation and system reliability. In [41], the authors have presented an in-depth review of microgrid energy management strategies and solution approaches, emphasizing the multi-objective nature of microgrid energy management and its role in sustainable development. In [42], the study has introduced a real-time energy management system for renewable-based microgrids, aiming to minimize costs while considering resource forecasts. In [43], the authors have demonstrated the economic benefits of a rolling horizon unit commitment approach compared to standard methods, enhancing system adaptability. In [44], the authors have outlined a microgrid control system managing distributed energy resources connected to a single bus. It employs a centralized heuristic approach, considering variables like photovoltaic power generation, fuel cell utilization, battery state of charge, load profile, and electricity tariff. The system aims to ensure reliable and economical energy resource utilization while maintaining power quality.

Data integrity attacks, a growing concern for microgrid operation, involve inserting or altering data in network traffic or data servers to mislead the EMS and prompt incorrect decisions [9]. Several studies have investigated the impacts of cyber-attacks on microgrid reliability, including analytical methods and comprehensive analyses of threats such as false data injection attack (FDIA), denial of service (DoS), and man in the middle (MITM) attacks, along with their mathematical modeling and impact assessments on distributed microgrids [45–48]. FDIA stands out as one of the most prominent types of data integrity attacks in microgrid systems. It can significantly impact the operation of microgrids by compromising the integrity of data used for decision-making and control. In [49], the authors have explored FDIA consequences, examining attacker strategies to exploit legitimate participants while maintaining supply-demand balance. In [50], the authors have proposed a resilient controller for DC microgrids, countering FDIA and DoS attacks with an adaptive control scheme. In [51], a false data injection attack model for the smart grid has been proposed, along with detection methods based on deep reinforcement learning. In [52], the authors have examined FDIA impact on distributed load sharing in autonomous microgrids, studying information corruption and utilization under various injection strategies. In [53,54], cyber-attack minimization techniques and resilient control frameworks have been proposed for smart grid security. In [55], the study has investigated renewable energy penetration and data loss effects on microgrids, while in [56], the authors have proposed a cyber-resilient control approach for islanded microgrids, addressing hybrid FDIA and denial-of-service attacks. The existing literature on microgrid EMS and FDIA offers valuable insights into optimizing microgrid operations and addressing cybersecurity challenges. However, there is a notable gap in exploring hybrid operational strategies adaptable to diverse microgrid conditions, and real-time attack mitigation techniques are lacking.

However, another significant challenge that microgrids face is the potential loss of data in the communication channels. In [57], the authors delivered a comprehensive overview of diverse tools and their specific characteristics applicable in smart grid research which encompasses both the communication aspects and the associated information and communication technology infrastructure that complement the power grid. In [58], the authors presented a framework for conducting power and communication system co-simulation, specifically focusing on the impact of communication systems on microgrid stability. The framework was utilized to investigate an operational use case where a battery energy storage system is employed to compensate for generation loss in an islanded microgrid. In [59], the authors introduced a comprehensive microgrid simulation model that integrates both the power subsystem and the communication subsystem using MATLAB Simulink. In [60], the authors analyzed the impact of packet loss on demand estimation in smart grids and observed that packet loss increases the cost of power supply. In [45], an analytical method has been proposed to measure the impacts of cyber system failures and transmission interference on reliable microgrid operation. However, there is a lack of research focusing on quantifying the impact of data loss in battery command on microgrid energy management systems. Moreover, the conventional method for simulating microgrid energy management systems with communication data loss typically involves multiple simulators connected through interfaces, which can be complicated. However, there is a need for a more streamlined and compact model that integrates all the relevant components of simulation into a single simulator.

1.3. Contribution

1.3.1. Vulnerability Analysis of Electric Grid Networks

We have significantly enhanced the accuracy and reliability of our cascading failure simulation model by incorporating an improved power balance algorithm. Our enhanced model now includes a modified optimal power flow (OPF) algorithm which utilizes a least square adjustment method to restore network balance during cascading failures, thereby providing more precise and actionable insights into the vulnerability of electric grid networks. We have quantified the vulnerabilities associated with the increasing penetration of RE in the existing power grid concerning CF. Specifically, we assessed the impact of RE penetration on the grid's vulnerability by analyzing metrics such as the amount of load shedding and the number of tripped lines during a cascade process. Our analysis has also identified critical thresholds beyond which system deterioration escalates rapidly, highlighting the urgent need for preemptive measures to mitigate the adverse impacts of renewable energy integration during cascading failure processes. By addressing the shortcomings of existing models and introducing innovative improvements, our research significantly advances the state-of-the-art in cascading failure analysis and enhances our understanding of the challenges posed by rising renewable energy penetration in modern power systems.

1.3.2. Statistical Analysis of Cascading Failure Risks

Through a statistical analysis, we have investigated the risk associated with cascading failure processes by leveraging historical utility data and our developed CF simulation model. We have processed and categorized real-world outage data into cascades, enabling us to conduct statistical analyses and quantify the risk parameters associated with past CF events. We have explored the mechanisms of initial line trips of a cascade and assessed the impact of different probabilities for initial line tripping. By comparing uniform and non-uniform probabilities in initial line trips in a cascade in simulated test cases and historical utility data, we provided valuable insights into the complexities of CF risk assessment and approximations for the best initial line tripping mechanism. Additionally, by validating our findings in the simulation scenarios with real-world cascade events, we have gained valuable insights into the distribution of the risk factors, such as the duration and number of outage lines, load shedding amount associated with cascading failure events. This validation process strengthened the credibility and practical relevance of our simulation model.

1.3.3. Impact of Data Loss and FDIAs on Microgrid Resilience

We have developed a multi-layered microgrid simulation model with an optimization-based EMS and investigated the impact of data loss and FDIA on microgrid operation. We have developed two FDIA model to simulate different FDIA scenarios. Utilizing MATLAB-based simulation model, we have quantified the impacts of data loss in battery command and proposed a hybrid approach integrating optimization-based EMS with adaptive control methods during FDIA in islanded mode. This hybrid approach dynamically switches its objective according to operation scenarios to ensure reliable microgrid operation. Through simulation analyses, we have demonstrated the effectiveness of our hybrid strategy in safeguarding microgrid operation, while also highlighting the potential for further enhancement through the integration of artificial intelligence techniques for real-time detection and resolution of FDIAs.

1.4. Structure of the Dissertation

In Chapter 2, we have conducted a vulnerability analysis of the power grid in light of the increasing integration of renewables. We outlined the system model and introduced a modified OPF algorithm. Through extensive simulations on uncertain renewables within IEEE standard test cases, we thoroughly examined the outcomes and implications. In chapter 3, our focus shifted to the risk analysis of cascading failure processes within the power grid. We detailed the sourcing and grouping process of historical outage data and explored the risk assessment using both real-world and simulated data. By comparing uniform and non-uniform initial line tripping probabilities with historical utility data and simulated data, we aimed to determine the function providing better approximations of grid cascading failure risks. Transitioning to chapter 4, we have investigated the impact of data loss and false data injection attacks on microgrid operation. After providing an overview of microgrid structure and various cyber threats and targets, we have presented our FDIA model and proposed microgrid operation strategy. Subsequently, we have described our simulation model and comprehensively analyzed the obtained results and findings.

Table I. Structure of Dissertation

Chapter	**Title**	**Description**
2	*Grid Vulnerability Analysis with Renewables Integration*	Conducted vulnerability analysis of the power grid considering increasing integration of renewable energy. Introduced a modified OPF algorithm for analysis.
3	*Cascading Failure Risk Analysis and Validation*	Investigated the risk of cascading failure processes within the power grid. Sourced and grouped historical outage data for risk assessment. Validated findings using real-world and simulated data.
4	*Microgrid Resilience and Cyber Threat Analysis*	Focused on microgrid resilience and cyber threat analysis. Introduced an FDIA model and proposed microgrid operation strategy. Analyzed simulation results and findings.

2. POWER GRID VULNERABILITY ANALYSIS WITH RISING RENEWABLES INFILTRATION

2.1. Introduction

The increasing penetration of renewable energy has a significant impact on the performance and reliability of the power grid. This is largely because of the uncertainty of the renewable resources and the complex nature of the power system infrastructure. In this chapter, we have analyzed power grids' vulnerability to cascading failures with respect to the penetration level of renewable energy into the grid. A novel power balance technique is used for cascading failure analysis and power grid vulnerability measurement. The proposed approach incorporates a modified optimal power flow algorithm to enhance the existing CF simulation model [32] in the grid vulnerability analysis study which accurately reflects the most probable path of cascading failure evolution process with uncertain renewable generation. The simulation results on IEEE 118 bus system, IEEE 300 bus system and a synthetic 500 bus system showed that increasing penetration of renewable energy have proportionally higher impact on grid vulnerability to cascading failures due to injection of higher uncertainties into the grid. It was also evident that after a certain level of RE penetration, some system might deteriorate rapidly and preventive measures should be taken if and when RE penetration level exceeds that limit [61].

2.2. System Model

The modern power system is an ever-evolving complex infrastructure. Their complex interconnected nature along with characteristics of different parameters introduce uncertainties into the network. Demand growth, availability of renewable energy sources, contingencies, climatic conditions, interconnections, power markets, are some examples of uncertain data. The goal of this study is to assess the grid vulnerability to cascading process from uncertainty perspective. Our proposed model considers uncertainty from load and renewable generation which propagates linearly in the line flow process.

2.2.1. Uncertainty modelling

In the proposed uncertainty model [62], the load demand power and renewable generator output power are represented with two terms as follows:

$$P(t) = \mu_p(t) + \epsilon_p(t) \tag{1.1}$$

where $\mu_P(t)$ is the mean of load demand power or renewable generator output power at time *t*. In other words, it is the expected power signal ahead of time. It is actually the forecasted power we achieve through some forecasting techniques using historical data. And $\epsilon_P(t)$ represents the uncertainty which is a zero-mean signal. It is the difference between forecasted data and actual data. In this study, we assume load forecasting errors and wind output power mismatches as uncertainties. As the historical data and future data follow same pattern for load demand and renewable resources, a widely popular forecasting model, autoregressive moving average (ARMA) technique [63] is used to model uncertainties in this study.

2.2.2. Line flow based on AC power flow

The power flow study is the numerical computation of voltage magnitude and phase angle at each bus in an interconnected network under steady state condition. The DC power flow approximation is a common approach for calculating load flow and detecting overloaded branches. This approximation considers some assumption to achieve the linearization of power flow equations which results in reduction of computational burden. In DCPF, we assume flat voltage profile which means the voltage amplitude is equal for all nodes and voltage angle differences between neighboring nodes are small. We also assume line resistance are negligible compared to line reactance. The accuracy of DCPF depends on these assumptions' validity in real network situation. These assumptions do not hold true for AC power flow which may result in huge computational burden and convergence problem for large complex network. On the other hand, the accuracy of AC power flow solutions is much higher and we can access the voltage profile of the busses in the network. Due to these approximations, DCPF underestimate the severity of cascading failure in large complex networks [30]. In our proposed cascading failure model, we have used ACPF to detect overloaded branches. However, to determine the mean flow in the branches, unscented transformation (UT) method is used to avoid the disadvantages of ACPF [64], [65].

2.2.3. Unscented transformation

The unscented transformation (UT) method can overcome the limitations of linearization by providing a direct and definitive approach for transforming statistical information. UT method can provide higher accuracy with the same computational burden as linearization. The basic idea of UT method is that it is easier to estimate a probability distribution function than it is to estimate an arbitrary nonlinear function [64]. In UT method, the input points are selected in a way that they can maintain enough information to represent their probability distribution function. The UT method is applicable to different uncertain problems with satisfactory result. This method calculates the statistics of output random variables undergoing a set of nonlinear transformations. In our model, the inputs of the UT methods are the load demand and renewable generation. We have chosen the input points in a way so that we can determine the mean and covariance of the input variables. Then UT method can estimate the mean and covariance of the output random variables, in our case, line flow in the network [32]. Special focus should be given on the idea that, in the UT method, the sample points are not selected randomly. They are chosen in a specific way so that they have a predefined mean and covariance. This statistical information propagates through some nonlinear function and ultimately results in an accurate estimation of statistics of the output variable.

2.2.4. Tripping mechanism and relay model

In the proposed relay model, we have used the mean and covariance of the branch flow derived by the UT method [32]. This statistical information is the main component of the CF simulation relay model. Here, power flow of each branch is assumed to be Gaussian to determine the normalized overload distance and in result, the overloading probability of each branch [28]. Then, we can calculate the mean overload time ($\overline{\tau_l}$) of branch l using the normalized overload distance (z_l) and overloading probability (ρ_l).

$$\overline{\tau_l} = \frac{2\pi\rho_l e^{\frac{z_l^2}{2}}}{BW_l} \tag{1.2}$$

Where, BW_l is the equivalent bandwidth of the flow process for the lth line [66].

This relay model introduces the uncertainties injected from RE sources and loads to the line flows. The time-inverse relay algorithm is in motion when the line becomes overloaded and the time to trip (t_{tr}) is inversely proportional to the line overloading value. This value is determined based on the thermal stability of the transmission lines [67]. This t_{tr} value is compared to the mean overload time, $\overline{\tau_l^u}$, if it is larger the trip timer is set to zero, otherwise, the trip timer is set to the relay time to trip. This tripping mechanism enables us to model the stochastic process of CF and identify the most probable path for its propagation.

2.3. Modified OPF Algorithm

During cascading failure process, branches of the power grid may trip and become disconnected. The grid network changes after every line trip. To restore the balance in the system some modification may be required. In [32], author proposed a power balance algorithm to restore the balance. In this algorithm, conventional OPF is used which could not accurately evaluate the impacts of RE penetration into the grid during CF. As CF is a very fast evolving process, conventional OPF would not properly reflect the transition path of CF process after every line tripped. Here, we proposed a modified OPF algorithm which can restore the balance of the grid within its capacity limit. In this algorithm, we have proposed least square adjustment of the parameters of power grid within their valid capacity limit. The main goal of this algorithm is to mimic the most likely evaluation path of CF process in each step of the simulation process. The solution of this optimization problem restores the balance of the grid network within the least possible adjustment of generation and load controls in the grid and in result, accurately evaluates the impacts of RE penetration during CF process by representing the most likely transition path of CF process after every line trip.

2.3.1. Objective function

The objective function of this modified OPF is the least square adjustment of generation and load controls after every line tripping occurs. In this optimization problem, we try to minimize the differences of generation and load control parameters from their initial value. As oppose to the conventional OPF, it only focusses on real and reactive generation, real and reactive load demand and bus voltage magnitude. In CF process, every line tripping result in change of the existing network and the adjustment of generation and load is necessary. The modified OPF serve this purpose keeping the system as close to the initial condition.

$$\min_{P_G, P_D, Q_G, Q_D, V} \boldsymbol{W}[\ \|\Delta P_G\|_2^2\ \ \|\Delta P_D\|_2^2\ \ \|\Delta Q_G\|_2^2\ \ \|\Delta Q_D\|_2^2\ \ \|\Delta V\|_2^2\ ]^{\boldsymbol{T}} \tag{1.3}$$

Here, $\Delta P_G, \Delta Q_G, \Delta P_D, \Delta Q_D$ and ΔV represent the real power generation adjustment, reactive power generation adjustment, real load adjustment, reactive load adjustment and the voltage magnitude adjustment respectively for each bus before and after line tripping. And, $\boldsymbol{W}$ represents coefficients or the penalty factors for the respective terms in optimization problem. Here, $\boldsymbol{W} = [\ w_1\ w_2\ w_3\ w_4\ w_5]$. The values of these coefficients determine the gravity of their respective terms in the overall minimization problem. For example, in a specific case when minimizing load shedding is of top importance, one can put extra effort in minimize it by setting higher value of w_2 from other coefficients, which may result into other parameters shift away from initial value. In other cases, it could be of more importance to keep the differences of generation dispatch as less as possible. In that case, coefficient w_1 will be set to a higher value to minimize the difference of generation dispatch which may lead to higher amount of load shedding. Thus, the values of the coefficients can be chosen in a way to serve specific purpose in specific cases. Here, in our simulation, all the coefficient values are set to 1 to give equal importance to every term in the modified OPF algorithm.

2.3.2. Constraints

The modified OPF is a constrained optimization problem which has two types of constraints.

Equality Constraint: The active and reactive power balance in each bus, namely the AC power flow equation is the equality constraint set for this modified OPF.

$$f(V_m, \theta, S_{G,} S_D, Y) = 0 \tag{1.4}$$

Here V_m represents bus voltage magnitudes, θ represents bus voltage angles, S_G is the complex generation power, S_D is the complex load and Y is the admittance matrix for the grid after line tripping occurs.

Inequality constraint: The operating limits of the components of power grid control the steady state operation of the network. These operating limits are the inequality constraints set for this modified OPF.

$$X_{min} \leq X \leq X_{max} \tag{1.5}$$

Here X represents real and reactive generation, real and reactive load, bus voltage magnitude and bus voltage angle, X_{max} is the upper boundary and X_{min} is the lower boundary of the parameters. These are the inequality constrains of the modified OPF.

2.3.3. Algorithm

In CF simulation process, after every line tripping this modified OPF restores the balance of the network using least square adjustment of the generation and load controls

Figure 1 shows the flowchart of the modified OPF. This modified OPF model represents a nonlinear constrained optimization problem. We have used an optimization toolbox of MATLAB, ‘fmincon’, to solve this problem. This modified OPF takes the transformed admittance matrix after line tripping and power flow solution of the network before line tripping as inputs. The parameters are initialized as the power flow solution of the network before line tripping. The inequality constraints are set as the operating limits of the generation and load controls and the equality constraints are the real and reactive power balance equations for each bus.

In Figure 2, the overall working diagram of the proposed model has been shown. For a specific network we have chosen a few different scenarios where several generators were selected to replace them with wind generators. For every scenario, we have chosen different conventional generators for replacement. According to the load data, wind data and scenarios, we performed an initial optimal power flow to determine the generation dispatch for different RE penetration. Then we introduced n-2 contingency into the system to initiate cascading failure.

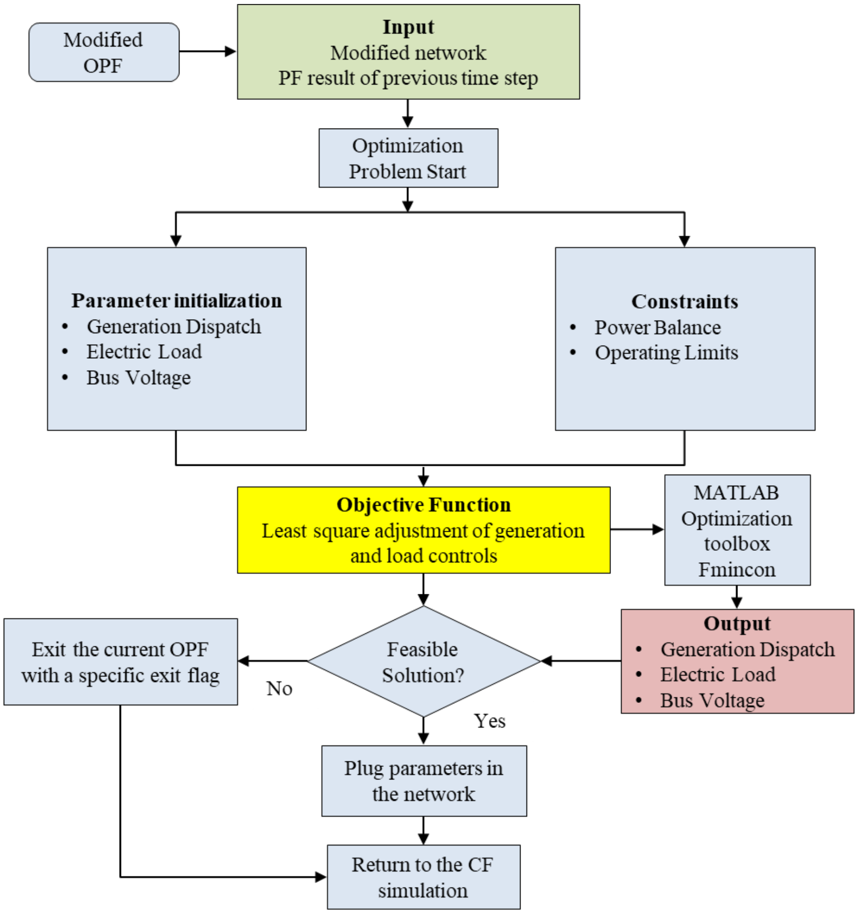

Modified OPF
Input
Modified network
PF result of previous time step
Optimization Problem Start
Parameter initialization
Generation Dispatch
Electric Load
Bus Voltage
Constraints
Power Balance
Operating Limits
Objective Function
Least square adjustment of generation and load controls
MATLAB Optimization toolbox Fmincon
Output
Generation Dispatch
Electric Load
Bus Voltage
Feasible Solution?
No
Yes
Exit the current OPF with a specific exit flag
Plug parameters in the network
Return to the CF simulation

Figure 1. Flowchart of the modified OPF

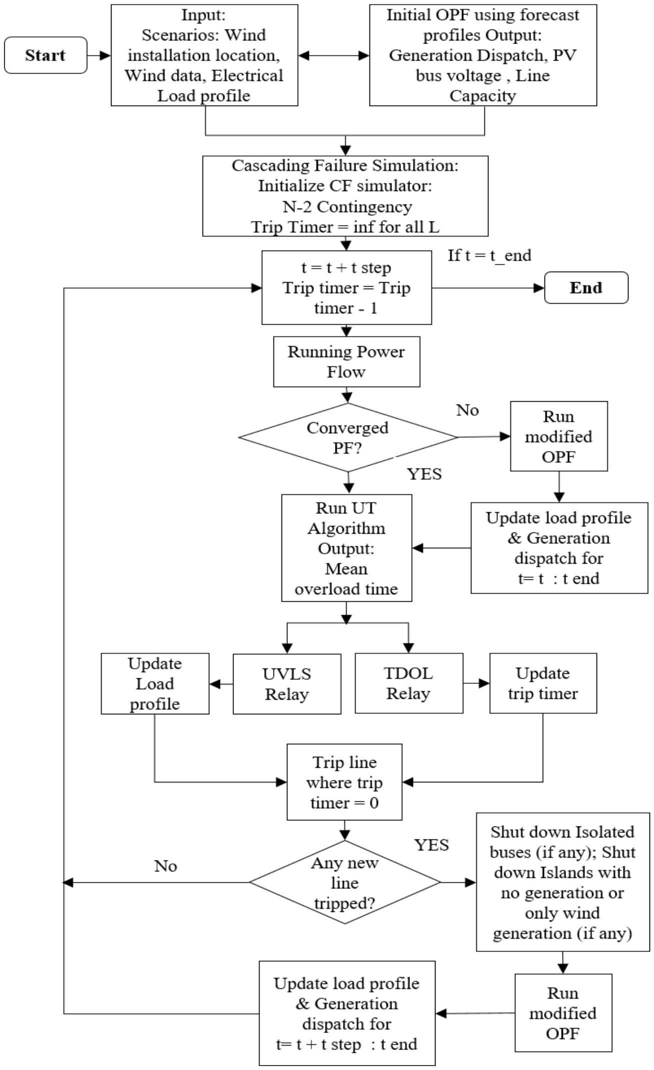

Start
Input: Scenarios: Wind installation location, Wind data, Electrical Load profile
Initial OPF using forecast profiles Output: Generation Dispatch, PV bus voltage , Line Capacity
Cascading Failure Simulation: Initialize CF simulator: N-2 Contingency Trip Timer = inf for all L
t = t + t step Trip timer = Trip timer - 1
If t = t_end
End
Running Power Flow
Converged PF?
No
YES
Run modified OPF
Update load profile & Generation dispatch for t= t : t end
Run UT Algorithm Output: Mean overload time
Update Load profile
UVLS Relay
TDOL Relay
Update trip timer
Trip line where trip timer = 0
Any new line tripped?
No
YES
Shut down Isolated buses (if any); Shut down Islands with no generation or only wind generation (if any)
Run modified OPF
Update load profile & Generation dispatch for t= t + t step : t end

Figure 2. Overall overview of CF simulation

After every line tripping, the modified OPF restored the power balance of the network with least square adjustments of the parameters within their boundary. In every time step, we performed power flow analysis to determine the overloaded lines. For every overloaded line, we have used UT method to find out mean overloading time and specific lines have been tripped when the trip timer hit zero. During cascading process, we have shut down all isolated buses and islands without generation. After the simulation, load shedding amount and number of tripped lines have been stored. For every scenario, we have used several different n-2 contingencies to initiate cascading process and took the average of load shedding and trip count to measure the severity of the cascading process. For every scenario, we have repeated the process for different level of RE penetration to see the impact of RE penetration level on the severity of cascading process.

2.4. Simulation Results and Discussion

We have simulated the impacts of increasing renewable generation integration on grid vulnerability to cascading overload failures in two IEEE standard cases (IEEE 118 and IEEE 300 bus system) and one synthetic 500 bus system (ACTIVSg500). In all the cases, we have selected a few different scenarios and several different initial n-2 contingencies to initiate cascading process. We have used four hours of load data and wind generation data with 4 second resolution.

Scenarios: In a specific scenario, we have selected six different conventional generators to replace those with wind generators. The six conventional generators have been selected in a way so that they could contribute at least 30% of the total generation of the system which in result, represents up to 30% RE penetration in the system. Then these conventional generators are gradually replaced by wind generators to see the effect of increasing RE penetration in the grid. In our simulation, we have chosen a limited number of scenarios in order to reduce the computational burden. The scenarios have been chosen in a way so that most of the conventional generators by turn could have been replaced by wind generators.

Contingency: To initiate the CF simulation, we have manually tripped two branches (n-2 contingency) at the initial stage of the simulation. We have selected several different n-2 contingencies to initiate the CF simulation to see different cascading failure evaluation path for every scenario. In order to reduce the computational work load, we have selected limited number of initial n-2 contingencies. The contingencies have been selected from a batch of contingencies which mostly represents the critical lines of the system which leads to CF process.

2.4.1. IEEE 118 Bus System

The IEEE 118 bus test case represents a portion of the American Electric Power with 54 committed generators, 99 loads and 186 branches [68]. We have considered fifteen different scenarios where we replaced conventional energy with wind energy to see the impact of RE penetration in case of cascading failure.

To initiate cascading failure, we introduced 50 different N-2 contingencies in the simulation for every scenario to see its evolution process. To measure the severity of the cascading process we considered the load shedding amount and trip count for every case. For every scenario, we have tested our model for 0% to 30% renewable penetration. We have taken the mean of the total load shedding amount for 50 different initial n-2 contingencies.

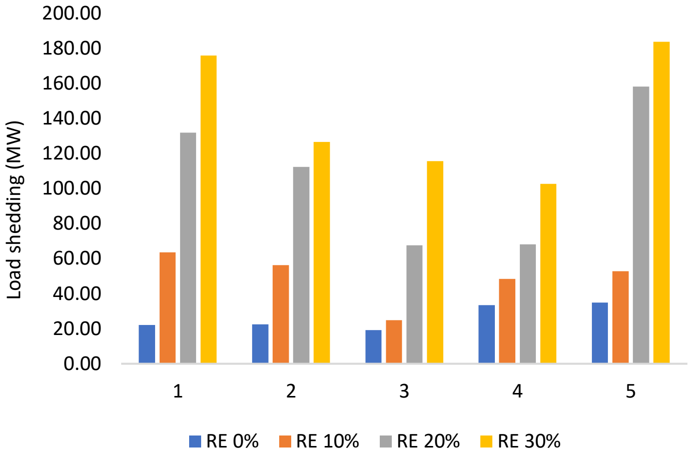
In scenario 1, generator 5, 10, 17, 21, 30 and 40 have been replaced by wind generator. We have simulated this scenario for 50 different n-2 contingencies. The average load shedding amount and average count of line tripping are the measuring tool to assess vulnerability to cascading failures.

Table II. Vulnerability impacts evaluation (Scn 1)-IEEE118

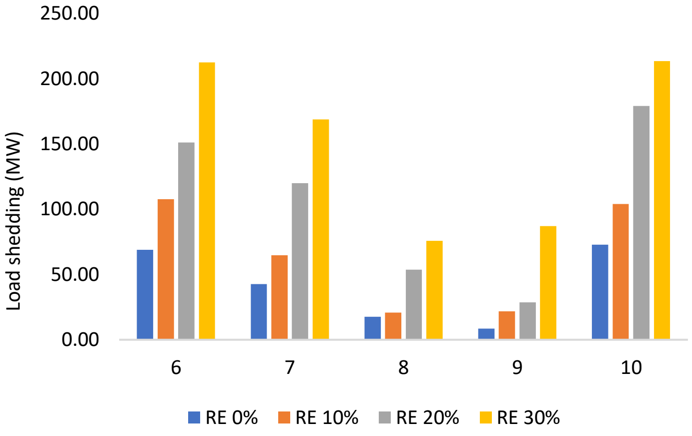
Avg Load Shedding (MW)				**Avg number of lines tripped**			
RE 0%	*RE 10%*	*RE 20%*	*RE 30%*	*RE 0%*	*RE 10%*	*RE 20%*	*RE 30%*
22.19	63.49	131.95	175.84	2.54	4.02	4.98	5.90

From Table II, we can see that for scenario 1, with increasing renewable penetration, the average load shedding amount increased from 22.19 MW to 175.84 MW. And the average trip count also increased from 2.54 to 5.90. The increasing renewable penetration increased uncertainty into the system which results in larger amount of load shedding which makes the network more vulnerable to cascading failure.

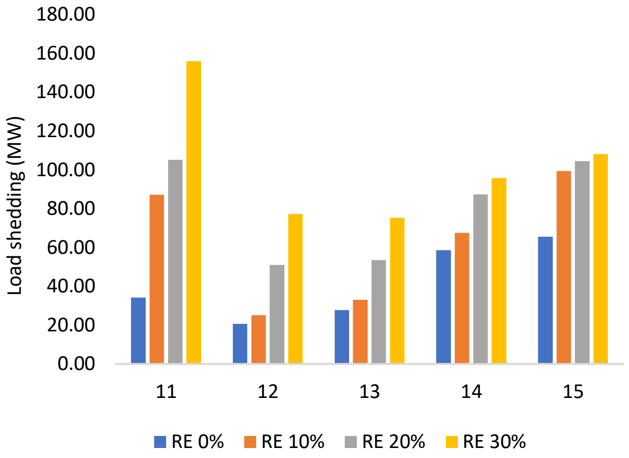
From Figure 3, we can see the same trend for every scenario, which is the increasing trend of load shedding amount with increasing RE penetration. If we take a closer look on Figure 3, we can see that for 50% of cases there is a sudden increase in load shedding when RE penetration level reached 20%.



Scenario (1-5)



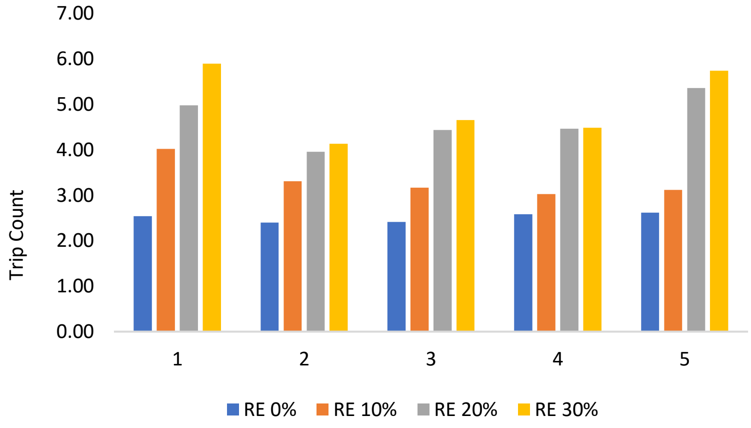
Scenario (6-10)



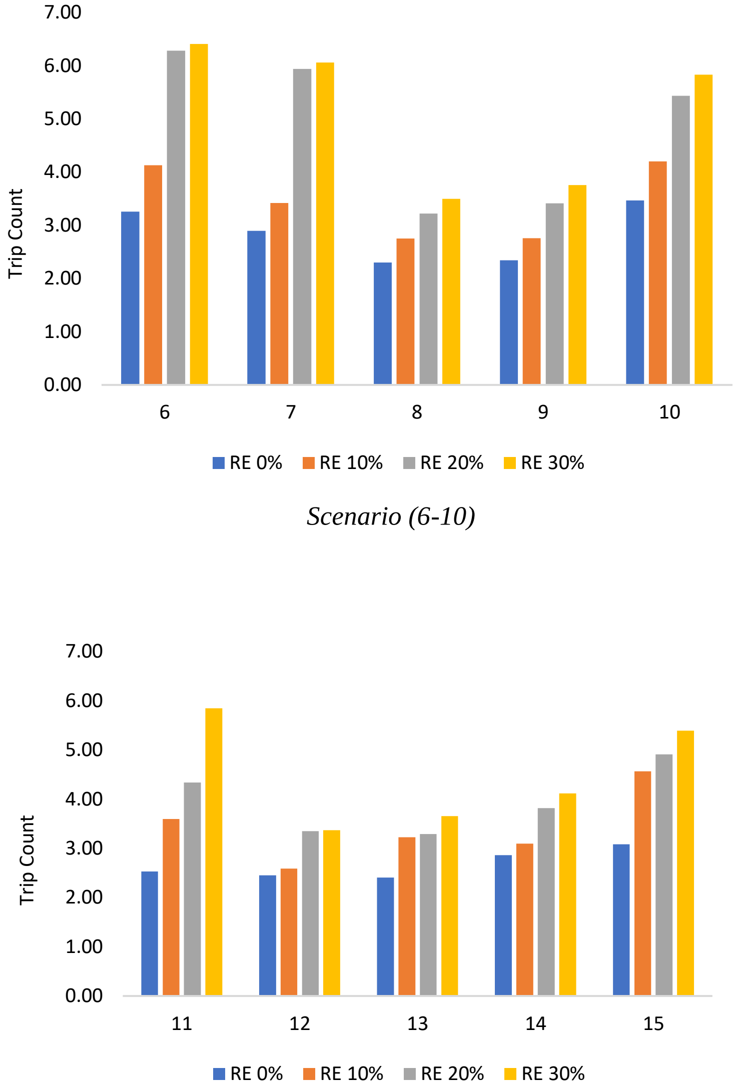
Scenario (11-15)

Figure 3. Average load shedding amount for increasing RE penetration (IEEE 118 bus system)

In Figure 4, we have shown the average number of line trips for every scenario with 50 different n-2 contingencies. The line trip count also increased with the increasing RE penetration.



Scenario (1-5)



Scenario (6-10)

Scenario (11-15)

Figure 4. Number of tripped lines for increasing RE penetration (IEEE 118 bus system)

For a specific scenario and for a specific contingency we can see the most probable cascading process evaluation path. In Table III, we can see that for scenario 1, when we initially tripped line 51 and 168 to initiate CF process, the trip count and the load shedding percentage increased with increasing RE penetration.

Table III. Vulnerability impacts for a specific contingency-118 bus

Scenario	N-2 Contingency	RE Penetration	Trip Count	LNS (%)
1	51, 168	0%	4	0.60
		10%	13	8.77
		20%	17	12.71
		30%	26	24.10

In Figure 5, we can see the cascading failure evolution process for scenario 1 where branch 51 and 168 was initially tripped. We can see the initial escalation in the initial stage of the CF process and then after some time the system becomes stable. For RE penetration of 0% the system has stabilized very quickly compared to higher RE penetration level. With increasing RE penetration, the system took more time to stabilize which also indicates the vulnerability to CF with uncertain generation.

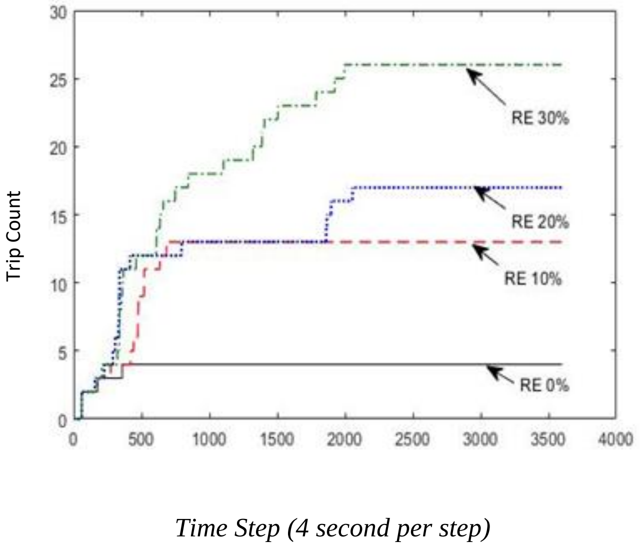


Figure 5. Cascading failure evolution for a specific contingency

2.4.2. IEEE 300 Bus System

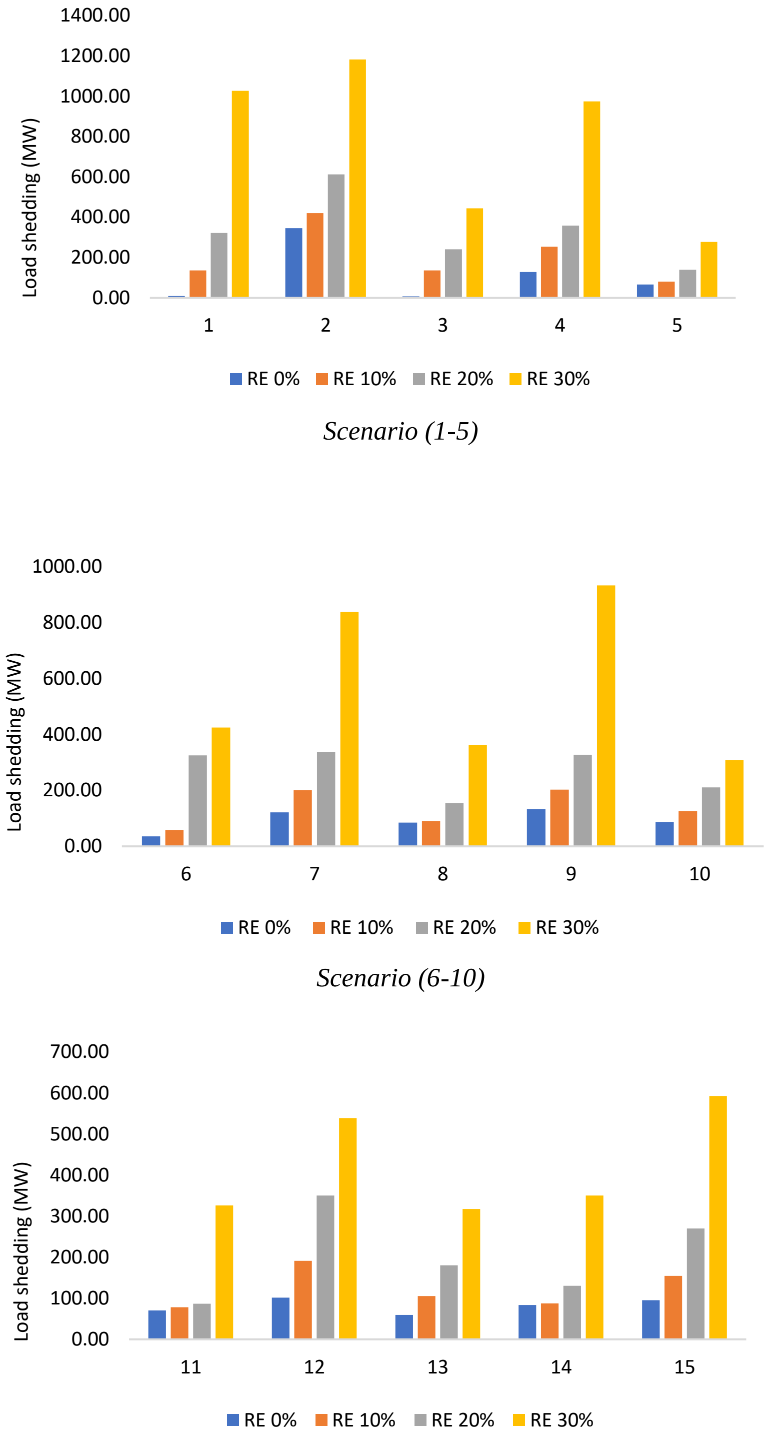
We have tested our algorithm on another IEEE test case, IEEE 300 bus system. This test case was developed by the IEEE test systems task force under the direction of Mike Adibi in 1993. This system contains 69 generators, 304 transmission lines and 195 loads, and its loading level is higher than 118 bus system [69]. We have considered ten different scenarios for this test case where we replaced conventional energy with wind energy to see the impact in case of cascading failure. To initiate cascading failure, we introduced N-2 contingencies in the simulation. For every scenario, we have considered 10 different n-2 contingencies to initiate cascading failure and see its most probable evolution process. To measure the severity of the cascading process we have considered the load shedding amount and trip count for every case as measuring tool.

For example, in scenario 2, generator 11, 14, 31, 48, 62 and 64 have been replaced by wind generator. We have simulated this scenario for 10 different n-2 contingencies. The average load shedding amount and average number of tripped lines are the measuring tool to assess vulnerability to cascading failures.

Table IV. Vulnerability impacts evaluation (Scn 2)-300 bus

Avg Load Shedding (MW)				**Avg number of lines tripped**			
RE 0%	*RE 10%*	*RE 20%*	*RE 30%*	*RE 0%*	*RE 10%*	*RE 20%*	*RE 30%*
346.4	420.1	613.2	1181.9	4	4.67	6.22	8.11

From Table IV, we can see that for scenario 2, with increasing renewable penetration, the average load shedding amount increased from 346.4 MW to 1181.9 MW. And the average trip count also increased from 4 to 8.11.



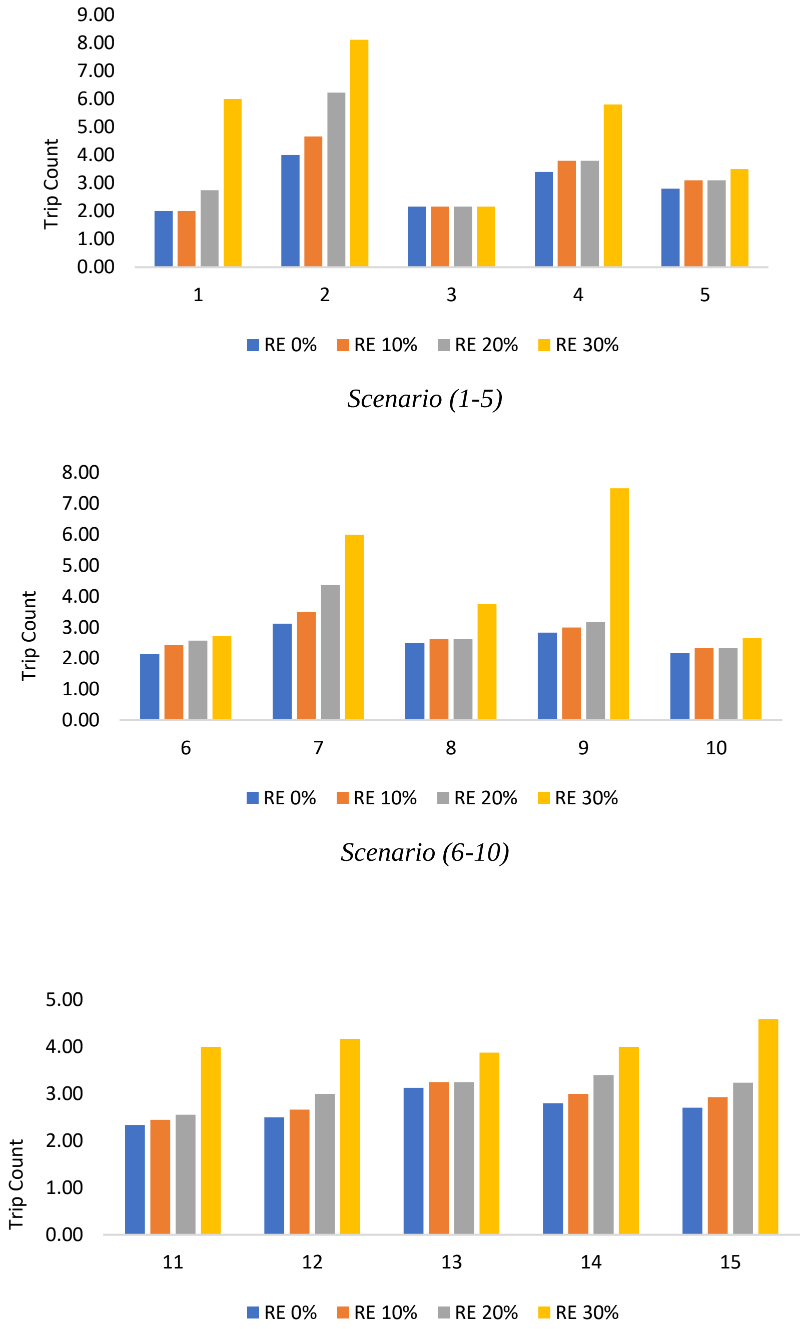
Scenario (1-5)

Scenario (6-10)

Scenario (11-15)

Figure 6. Average load shedding amount for increasing RE penetration (IEEE 300 bus system)

The increasing renewable penetration increased uncertainty into the system which resulted into larger amount of load shedding and made the network more vulnerable to cascading failure.



Scenario (1-5)

Scenario (6-10)

Scenario (11-15)

Figure 7. Number of tripped lines for increasing RE penetration (IEEE 300 bus system)

From Figure 6, we can see the same trend for every scenario, which is the increasing trend of load shedding amount with increasing RE penetration. If we take a closer look on Figure 6, we can see that for almost 80% of the cases, when RE penetration level reached 30%, there is a rapid increase in load shedding amount which indicates that the system becomes more vulnerable at this level of RE penetration.

In Figure 7, we have shown the average number of line trips for every scenario with 10 different n-2 contingencies. The line trip count also increased with the increasing RE penetration.

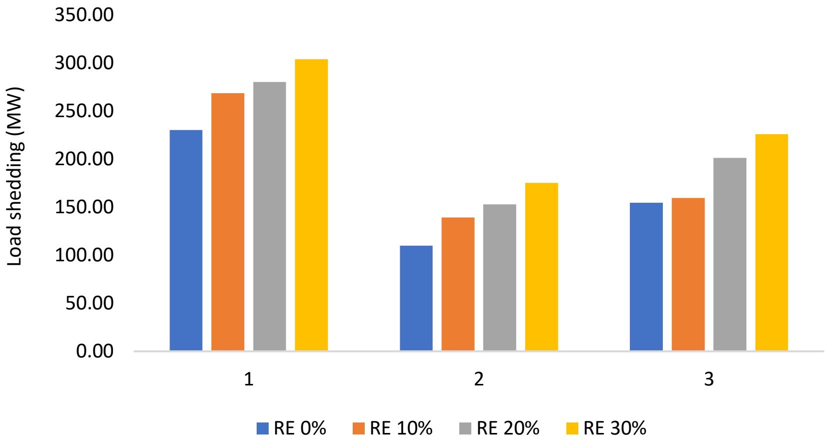
2.4.3. 500 bus case (ACTIVSg500)

The ACTIVSg500 case is a 500-bus power system test case that is entirely synthetic, built from public information and a statistical analysis of real power systems. It bears no relation to the actual grid in this location, except that generation and load profiles are similar [70]. This system contains 56 committed generators, 597 transmission lines and 200 loads, total generation capacity 12188.9 MW and load 7750.7 MW. We have considered only three different scenarios for this test case due to high computational burden. To initiate cascading failure, we introduced N-2 contingencies in the simulation. For every scenario, we have considered 25 different n-2 contingencies to initiate cascading failure and see its most probable evolution process.

Table V. Vulnerability impacts evaluation (Scn 1)-500 bus

Avg Load Shedding (MW)				**Avg number of lines tripped**			
RE 0%	*RE 10%*	*RE 20%*	*RE 30%*	*RE 0%*	*RE 10%*	*RE 20%*	*RE 30%*
230.2	268.6	280.6	303.9	6.05	6.53	6.68	6.79

From Table V, we can see that for scenario 1, with increasing renewable penetration, the average load shedding amount increased from 230.2 MW to 303.9 MW. And the average trip count also increased from 6.05 to 6.79.

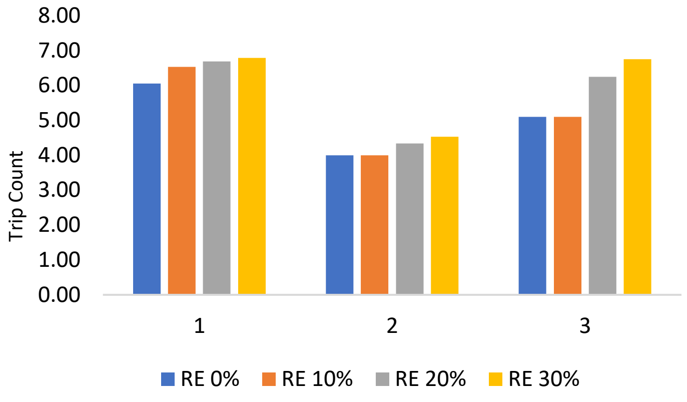


Scenario (1-3)

Figure 8. Average load shedding amount for increasing RE penetration (500 bus system)

From Figure 8, we can see the same trend for every scenario, which is the increasing trend of load shedding amount with increasing RE penetration. If we take a closer look on Figure 8, we can see that there is a steady increase in load shedding amount.

In Figure 9, we have shown the average number of line trips for every scenario with 25 different n-2 contingencies. The line trip count also increased with the increasing RE penetration.



Scenario (1-3)

Figure 9. Number of tripped lines for increasing RE penetration (500 bus system)

Comparing the results of the three cases we can say that, in all the cases with increasing penetration of RE, the amount of load shedding and the number of tripped lines increased. As measuring tool of vulnerability to cascading failure, the system becomes more vulnerable to cascading failure. Moreover, from Figure 6, we can notice sudden rapid increase of load shedding amount for most of the scenarios in 300 bus system when RE penetration increases from 20% to 30%. As a matter of fact, on an average there is around 120% increase of load shedding when RE penetration increased from 20% to 30%.

Table VI. Overall analysis in three test cases

Test Case	**Load shedding (%)**				**Trip count**			
	RE 0%	***RE 10%***	***RE 20%***	***RE 30%***	***RE 0%***	***RE 10%***	***RE 20%***	***RE 30%***
IEEE 118	39.18	61.32	101.78	131.98	2.7	3.4	4.5	4.9
IEEE 300	95.00	155.00	270.00	593.00	2.7	2.9	3.2	4.6
ACTIVSG500	165.00	189.00	211.00	235.00	5.05	5.21	5.76	6.02

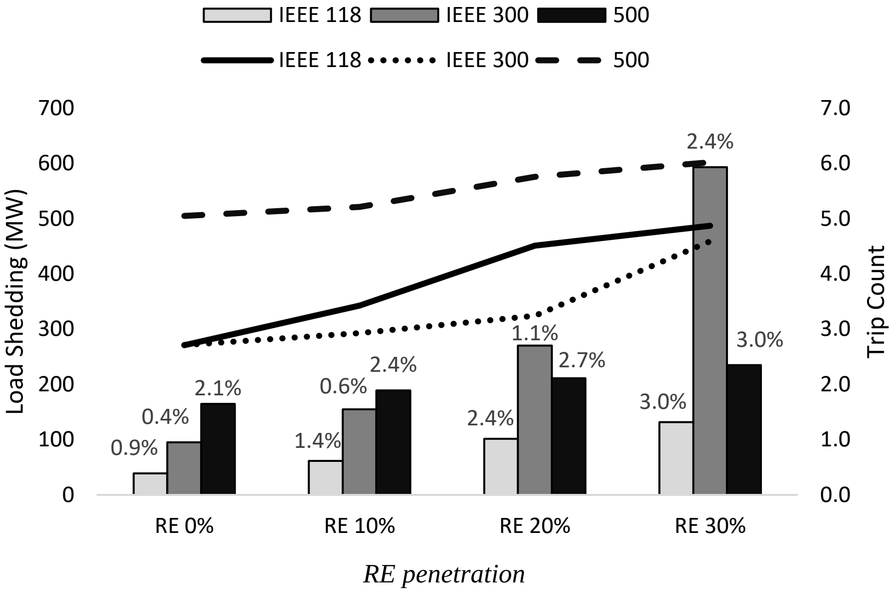


Figure 10. Overall vulnerability analysis

From Figure 10 and Table VI, we can see the overall vulnerability analysis for IEEE 118 bus system, IEEE 300 bus system and 500 bus system averaging all the scenarios. We can see that for IEEE 118 bus system, load shedding reached 2.35% for 20% RE penetration. For IEEE 300 bus system, there is a sudden increase in load shedding (2.4%) when RE penetration reached 30%. And for synthetic 500 bus system we can see a steady increase of load shedding amount with increasing RE penetration. It is evident for some cases that when RE penetration reached a certain point, the system may enter a critical stage where it can deteriorate rapidly and preventive measures should be taken to mitigate the negative impacts of RE penetration. Hence, by incorporating the modified OPF power balance algorithm in simulation process, the negative impacts introduced by RE on the grid vulnerability have been accurately reflected.

2.5. Summary

In this research, we have analyzed the impacts of renewable generation on grid vulnerability to cascading overload failures in terms of its penetration level. The existing CF simulation model, which utilizes the ACPF method along with the UT method, has undergone significant enhancement. By integrating a modified OPF algorithm for power balance, the model now better reflects the probable evolution path of the CF process, leading to increased accuracy in our study. This modification allows for a more precise representation of system dynamics and enables more reliable predictions of cascading failure scenarios. Blackout size and the number of tripped lines has been used as measuring tools to assess vulnerability to CF. It is found that higher penetration from renewable energy leads to a higher number of trips counts and a larger amount of load shedding. The proposed model has also been able to identify that after a certain level of RE penetration, some systems may deteriorate rapidly, and preventive measures should be taken if and when RE penetration levels exceed that limit.

The improved simulation model incorporating the novel power balance algorithm with modified OPF offers several advantages over conventional OPF methods. By incorporating the least square adjustment method, it better captures the fast-evolving CF process, thus providing more accurate predictions of system vulnerabilities. This enhanced accuracy is crucial for decision-makers to implement preemptive measures and avoid the potential danger of cascading failure due to higher renewable penetration. Take-aways from the simulation results of IEEE 118 and 300 bus systems reveal the necessity to upgrade infrastructure to mitigate the fast-increasing potential of danger from cascading failures. These findings emphasize the importance of proactive infrastructure upgrades to ensure grid reliability and resilience in the face of rising renewable energy penetration. Looking forward, future work could entail conducting additional simulations on a broader range of test cases to gain a deeper understanding of threshold levels and system vulnerabilities. It is important to recognize that every power system has unique characteristics, including varying loading levels, bus-to-branch ratios, and network topologies. As a result, the threshold level of RE penetration for cascading failure vulnerabilities may differ across different systems. By simulating more test cases with a higher number of scenarios and initial contingencies, we can acquire deeper insights into the vulnerabilities associated with increased renewable energy penetration. However, it is crucial to acknowledge the computational burden and time constraints associated with extensive simulations. Despite these challenges, expanding the scope of simulations to encompass various scenarios and contingencies will be pivotal in advancing our understanding of grid vulnerabilities and informing effective mitigation strategies.

3. CASCADING FAILURE RISK ANALYSIS OF ELECTRICAL POWER GRID

3.1. Introduction

In this chapter, we have studied the severity of cascading failure processes of electrical power grids by statistically analyzing the number of line outages per cascade, the cascade duration, and the load shedding amount of a cascade, based on the historical utility data of the BPA system and the simulation data of two synthetic test cases using our developed CF simulation model. Both uniform and non-uniform probability distribution functions have been considered for the initial line trips in the cascading failure simulation in order to determine which function better approximates the cascading failure risks of the real-world grid. The obtained simulation data and statistical analysis results from the two 500-bus synthetic test cases are then compared with those from the historical utility data [71].

3.2. Risk Analysis of Cascading Process from Historical Utility Data

Transmission line outages are a useful measuring tool to assess the severity of cascading failure in the system. In this study, the historical transmission line outage data from the Bonneville Power Administration (BPA) website [72] have been collected and statistically analyzed. The BPA system is an American federal agency operating in the Pacific Northwest. Bonneville is one of four regional Federal power marketing agencies within the U.S. Department of Energy (DOE). We examined 21 years of transmission line outage data (1999-2020) publicly available on the BPA website. Every outage has information on the outage date and time, outage duration, voltage level, outage type, cause of the outage etc. All the outages can be categorized into automatic outages and planned outages. Only automatic outages are considered for our study as these outages normally initiate CF processes in the system. From 1999 to 2020, there are 43,240 automatic outages documented on the BPA data. These outages are then grouped into different cascades according to their start times: if two-line outages separated by more than an hour, they will be grouped into two different cascades. Otherwise, if the start time difference of two consecutive outages is less than or equal to one hour, they will be grouped into the same cascade. This grouping process is adopted from [37]. Here, we have processed 20,211 automatic outages excluding outages having duration less than one minute as these outages did not spread any further and according to this grouping method, there are 5,724 cascades in the observed outage data. Among these cascades, 4,968 (86.79%) cascades have only one generation and do not spread further. After grouping all the outages into separate cascades, we analyzed the risk associated with each cascade.

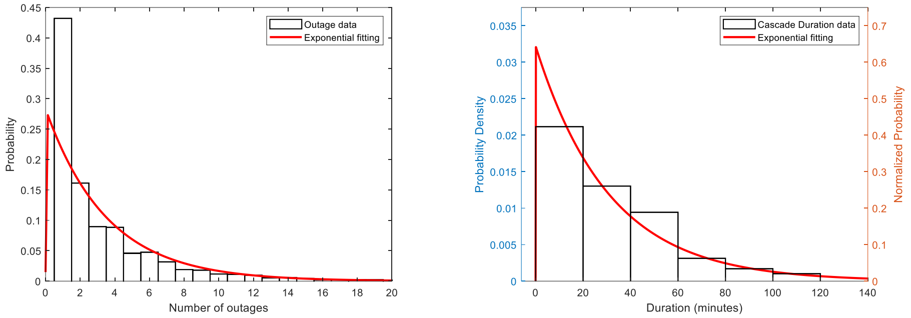
Outage number, cascade duration, and load shedding amount are crucial parameters used to assess the severity and risk of CF events in power systems. The outage number represents the total count of disabled lines or components during a CF event, indicating the extent of the disruption within the grid. A higher outage number implies a larger-scale impact on system reliability and resilience. Cascade duration refers to the duration of a CF event, reflecting the length of time it takes for the cascade to unfold and propagate through the system. Longer cascade durations signify prolonged system instability and disruption, highlighting the challenges faced by operators in restoring normal operation. Load shedding amount quantifies the quantity of load that must be curtailed to maintain grid stability during a CF event. Higher load shedding amounts indicate increased strain on the system and the potential for widespread service interruptions. Analyzing these parameters provides valuable insights into CF dynamics, helping stakeholders identify vulnerabilities and develop effective mitigation strategies to enhance system resilience. In order to measure the severity of CF processes, the number of tripped lines (outage number) and the duration of each cascade have been studied for the BPA system. The higher the outage number and the longer the duration of a cascade, the higher risk it will pose to the system. As the BPA data does not include records of load shedding, we are unable to analyze this metric for it.

In Figure 11(a), we can see the probability distribution of the outage numbers in a cascade for the BPA data. Here, the probability of a cascade with only one outage is the highest. After that, with the increasing number of outages, the probability decreases rapidly. We tried several statistical distributions to model the probability of outages in a cascade. Considering the simplicity of the model and measuring the goodness of fit, we propose an exponential distribution function to fit the data. The probability distribution function of an exponential distribution is as follows:

$$f(x,\lambda) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases} \tag{3.1}$$

Here, λ is the parameter of the distribution often called the rate of the distribution, and (1/λ) represents the mean of this distribution.

The exponential distribution function is adopted to fit the BPA outage data. According to this distribution, the mean number of outages in a cascade is 3.53. In Figure 11(b), the probability distribution of the cascade duration has been shown. The probability of a cascade lasting less than 20 minutes is the highest. After that, with the increasing amount of duration of a cascade, the probability decreases rapidly. We have also fitted this duration data with the exponential distribution function considering the simplicity of the model and also measuring the goodness of the fit. The mean duration according to this distribution function is 30.9 minutes [40,73].



(a) Probability distribution of outage number in a cascade

(b) Probability distribution of cascade duration

Figure 11. Probability distribution with exponential fitting for BPA data

3.3. Risk Analysis from Simulated Data

3.3.1. Simulation Model

The CF simulation model described in chapter 2 is used for the simulations on two synthetic power system test cases in order to analyze the risk of CF processes [61]. At first, the optimal power flow (OPF) algorithm is used on the forecasted load profiles to determine the initial generation dispatches in normal condition. Then a single branch of the system has been tripped manually to initiate the CF process. After every branch gets tripped, AC power flow has been used to determine the overloaded branches of the system. The unscented transformation (UT) method has been used to determine the mean overload time of the overloaded branches [64]. These values are then used in the relay mechanism to determine whether any other branches are getting tripped or not. After every new line trip, a modified version of the OPF algorithm is used to restore the power balance of the system. Here, the least-square adjusted OPF algorithm is used to mimic the most viable path of the CF process. The CF process will eventually stabilize and there will be no more overloaded lines in the system. After every CF simulation, we have determined the total number of line trips during the cascade, the duration of the cascade, and also the load shedding amount (if any).

3.3.2. Initial Line Tripping Mechanism

We have initiated our cascading failure simulation by tripping a single branch of the system. If a system has *n* number of branches, *n* different cascades can be initiated by tripping each different branch. We have considered both uniform and non-uniform distribution for these initial line trips.

Uniform Initial-Line-trip Distribution: In this case, it is assumed that every line getting tripped to initiate a CF process is with the same probability in the system. For that scenario, a system with n lines has n different cascades and the probability of these cascades happening are same.

Non-uniform Initial-Line-trip Distribution: We have also considered the non-uniform probability of initial line trips. Three different parameters have been considered to assign the non-uniform probability of initial line trips so that every cascade in the system may have a different probability.

Branch Flow: First we consider the branch flow as a defining parameter to assign the probability of initial line trips. The loading level of each branch of the system is determined as the ratio of the branch power flow under normal operation condition and its maximum branch capacity. After that, we divided all the branches into ten categories and assigned them different weights for the CF estimation, as shown in Table VII.

Table VII. Non-uniform probability definition of initial line trips according to the loading level

Loading level (*l*)	**Weight**
$0 \leq l \leq 0.1$	1
$0.1 < l \leq 0.2$	2
$0.2 < l \leq 0.3$	3
$0.3 < l \leq 0.4$	4
$0.4 < l \leq 0.5$	5
$0.5 < l \leq 0.6$	6
$0.6 < l \leq 0.7$	7
$0.7 < l \leq 0.8$	8
$0.8 < l \leq 0.9$	9
$0.9 < l \leq 1.0$	10

The higher the loading levels, the higher the probability of a branch initially getting tripped to start a cascading process.

Shortest Path: In this case, we use the network topology of a power grid to assign the non-uniform probability of initial line trips. We first define all the generation buses as the boundary nodes of a system and calculate the shortest path from every bus to the boundary. The distances are measured in terms of the hops on the shortest path. As every branch is connected with two buses, we have taken the minimum of the shortest paths associated with the two buses connected to the branch. Hence, for every branch, we have a corresponding shortest path to the boundary. We have considered this distance to assign a specific weight for every initial line trip. The longer the distance, the higher the probability of a line initially getting tripped, as shown in Table VIII.

Connectivity: In this case, we have considered the connectivity of every bus as a defining parameter. In the power grid, every bus is connected to several other buses. For every bus, we have determined this connectivity number. As every branch is connected by two buses, for every branch, we have considered the average connectivity number of the corresponding buses. This connectivity number is considered to assign the non-uniform probability of initial line trips. The higher the connectivity, the higher the probability of a line getting tripped initially and starting a CF process, as shown in

Table *IX*.

Table VIII. Non-uniform probability definition of initial line trips according to the shortest path

Shortest path to boundary (d)	**Weight**
d=1	1
d=2	2
d=3	3
d=4	4
d=5	5
d=6	6
d=7	7

Table IX. Non-uniform probability definition of initial line trips according to the connectivity

Connectivity number of every line (n)	**Weight**
n = 1	1
n = 1.5	2
n = 2	3
n = 2.5	4
n = 3	5
n = 3.5	6
n = 4	7
n = 4.5	8

3.4. Result and Discussion

Due to security and confidentiality reasons, detailed topology information regarding the BPA control area load and renewable penetration scenario is not publicly accessible. Additionally, the outage data spanning 21 years utilized in this study encompasses periods of significant system changes, including the retirement of old lines and the addition of new ones. Despite these limitations, we have inferred the system's loading level and utilized available information to conduct comprehensive analysis. Specifically, our study incorporates two synthetic 500-bus test cases for cascading failure simulation and statistical risk assessment, enabling comparison with real-world data and enhancing the robustness of our findings.

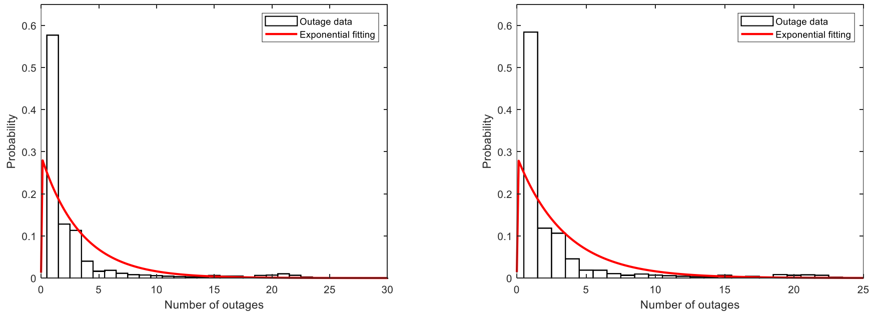
3.4.1. Test Case: ACTIVSg500

The ACTIVSg500 case is a 500-bus power system test case that is entirely synthetic, built from public information and statistical analysis of real power systems. It bears no relation to the actual grid in this location, except that generation and load profiles are similar [74]. This synthetic 500-bus test case contains 56 committed generators, 597 transmission lines, and 200 loads, a total online generation capacity of 8863.6 MW, and a load of 7750.7 MW. As the system has 597 transmission lines, we will have 597 different CF processes by initially tripping these 597 lines. For each CF simulation process, we have calculated the number of total lines tripped during the cascade, the duration of the cascade, and the amount of load shedding in percentage. We have considered both uniform and non-uniform probability of initial line trips. For the uniform probability of initial line trips, all the cascades initiated by a single line trip have the same probability. On the contrary, for the non-uniform probability of initial line trips, all the cascades have a different probability of occurrence. We have considered three different loading levels for our CF simulation and every loading level have a different weight according to the load duration curve of the BPA control area load. These three different loading levels have been combined according to their weight to mimic the real-world scenario where loading levels are different during different times of the day.

Table X. Weights of different loading level

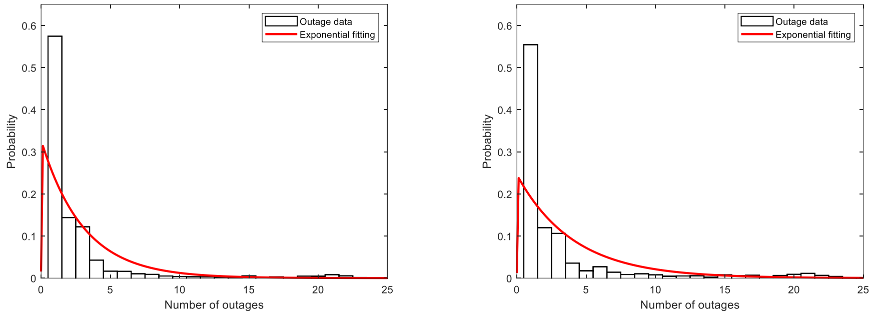
Loading Level	**Weight**
85%	0.1
70%	0.7
50%	0.2

In Figure 12, the probability distributions of the total number of outages in a cascade are shown. Figure 12(a) considers the uniform probability of any initial line trips and Figure 12(b), (c), and (d) consider the non-uniform probability of initial line trips. In Figure 12(b), the power flow in a branch is used as a defining parameter to assign different weights on initial line trips. Similarly, in Figure 12(c) and Figure 12(d), the shortest path to the boundary and connectivity of the systems are used as defining parameters to assign different weights on the initial line trips respectively. It is obvious from the figure that most of the cascades have only one outage and did not spread any more. The probability of a cascade having a large number of outages is very low and this probability decreases with the increasing number of outages. We have fitted our simulated outage number data with exponential distribution. In Table XI, the mean number of outages per cascade has been shown. Initial line trip probability according to branch flow has given us the best estimation compared with the BPA data while probability according to shortest path underestimated the mean outage number and probability according to connectivity overestimated the number the most.



(a) Uniform initial line trip probability

(b) Initial line trip probability according to branch flow



(c) Initial line trip probability according to the shortest path to the boundary

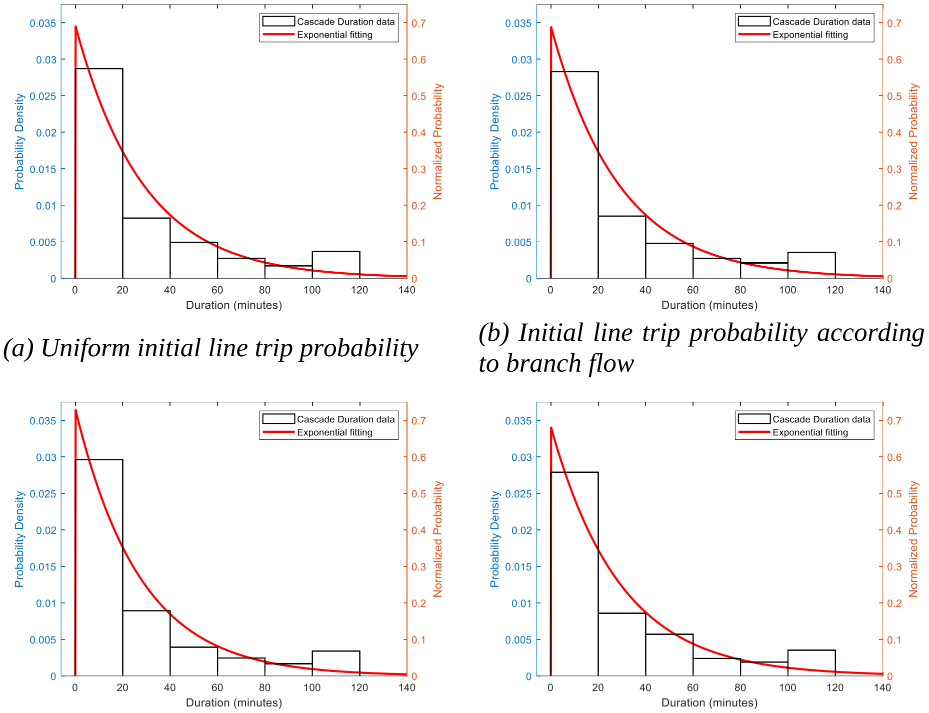
(d) Initial line trip probability according to the connectivity

Figure 12. Probability distribution of the number of outages in a cascade for the ACTIVSg500 system

Table XI. Mean number of outages in a cascade for ACTIVSg500 system

Probability of initial line trip	**Uniform**	**Non-uniform**		
		Branch flow	**Shortest Path**	**Connectivity**
Mean number of outages	3.44	3.46	3.05	4.07

In Figure 13, the probability distributions of the duration of a cascade are shown. Figure 13(a) considers the uniform probability of any initial line trips and Figure 13(b), (c), and (d) consider the non-uniform probability of initial line trips. The probability of a cascade having a long duration is very low and this probability decreases with the increasing duration. We have fitted our simulated cascade duration data with exponential distribution. In Table XII, the mean duration of a cascade has been shown which is pretty close to the number we got from the BPA data. Initial line trip probability according to the connectivity of the system has given us a more accurate mean duration value compared with the BPA data while probability according to the shortest path underestimated the mean duration of a cascade the most.



(a) Uniform initial line trip probability

(b) Initial line trip probability according to branch flow

(c) Initial line trip probability according to the shortest path to boundary

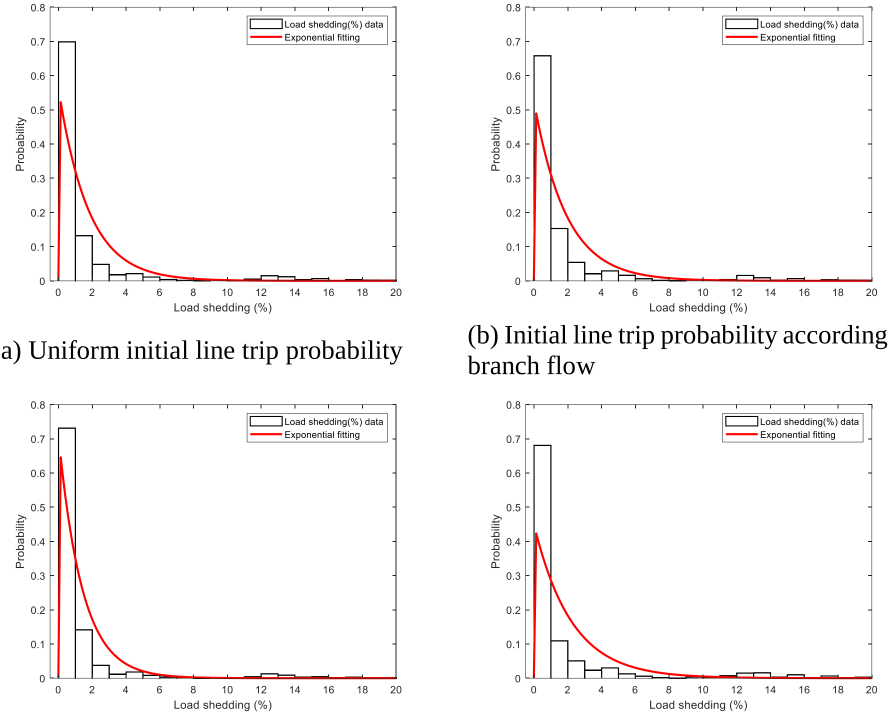
(d) Initial line trip probability according to the connectivity

Figure 13. Probability distribution of the cascade duration for the ACTIVSg500 system

In Figure 14, the probability distributions of the load shedding percentage during a cascade are shown. Figure 14(a) considers the uniform probability of any initial line trips and Figure 14(b), (c), and (d) consider the non-uniform probability of initial line trips. The probability of a cascade having a large load shedding amount is very low and this probability decreases with the increasing load shedding amount. We have fitted our simulated load shedding percentage data with exponential distribution. In Table XIII, the mean load shedding percentage of a cascade has been shown where probability according to the shortest path resulted in the lowest amount of load shedding and the probability according to connectivity resulted in the largest amount of load shedding.

Table XII. Mean duration of a cascade for ACTIVSg500 system

Probability of initial line trip	**Uniform**	**Non-uniform**		
		Branch flow	**Shortest Path**	**Connectivity**
Mean duration (minutes)	28.86	28.94	27.32	29.26



(a) Uniform initial line trip probability

(b) Initial line trip probability according to branch flow

(c) Initial line trip probability according to the shortest path to boundary

(d) Initial line trip probability according to the connectivity

Figure 14. Probability distribution of the load shedding percentage of a cascade for the ACTIVSg500 system

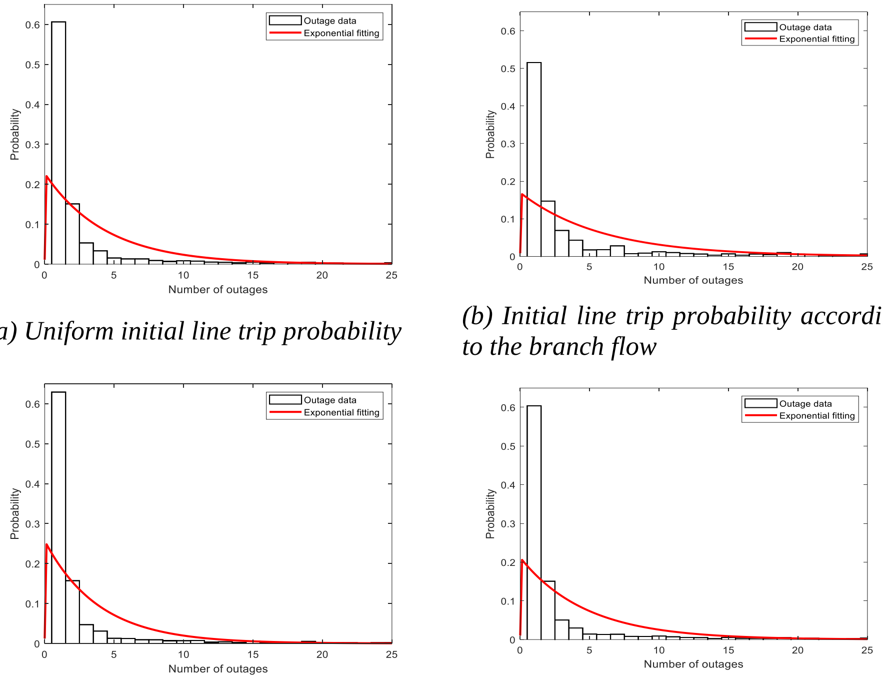
Table XIII. Mean load shedding percentage of a cascade for ACTIVSg500 system

Probability of initial line trip	**Uniform**	**Non-uniform**		
		Branch flow	**Shortest Path**	**Connectivity**
Mean load shedding (%)	1.78	1.91	1.41	2.23

3.4.2. Test Case: AutoSyngrid case

We have used another 500-bus test case for our CF simulation model. This test case has been developed using AutoSyngrid, a MATLAB-based toolkit for the automatic generation of synthetic power grids [75]. For our generated test case, WECC (Western Electricity Coordinating Council) system has been utilized as a reference system for generation and load settings as this system is closely related to the BPA control area load. We have named this test case ASGWECC_500_1. This test case contains 103 committed generators, 875 transmission lines, 109 loads, a total online generation capacity of 34,277.8 MW, and a load of 29,313.8 MW. Like the previous test case, as the system has 875 transmission lines, we will have 875 different CF processes by initially tripping these 875 lines. For each CF simulation process, we have calculated the number of total lines tripped during the cascade, the duration of the cascade, and the amount of load shedding in percentage. In this test case also, we have considered both uniform and non-uniform probability of initial line trips. Just like the previous test case, we have considered three different loading levels for our CF simulation, and every loading level has a different weight according to the load duration curve of the BPA control area load. These three different loading levels have been combined according to their weight to mimic the real-world scenario where loading levels are different during different times of the day.

In Figure 15, the probability distributions of the total number of outages in a cascade are shown. Figure 15(a) considers the uniform probability of any initial line trips and Figure 15 (b), (c), and (d) consider the non-uniform probability of initial line trips. In Figure 15(b), the power flow in a branch is used as a defining parameter to assign different weights on initial line trips. Similarly, in Figure 15(c) and Figure 15(d), the shortest path to the boundary and connectivity of the systems are used as defining parameters to assign different weights on the initial line trips respectively. It is evident from the figures that most of the cascades have only one outage and did not spread any further. The probability of a cascade having a large number of outages is very low and this probability decreases with the increasing number of outages. We have fitted our simulated outage number data with exponential distribution. In Table XIV, the mean number of outages per cascade has been shown which is higher than the number we got from the BPA data and the previous test cases. Initial line trip probability according to the shortest path to boundary has given us the best estimation with the BPA data while probability according to the branch flow overestimated the number the most.



(a) Uniform initial line trip probability

(b) Initial line trip probability according to the branch flow

(c) Initial line trip probability according to the shortest path to the boundary

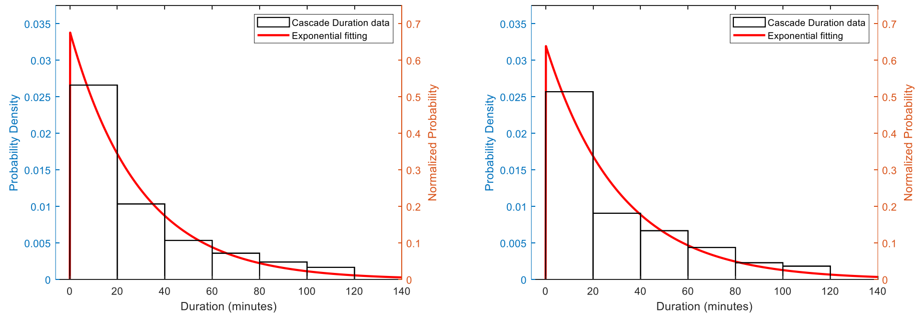
(d) Initial line trip probability according to the connectivity

Figure 15. Probability distribution of the number of outages in a cascade for the ASGWECC_500_1 system

Table XIV. Mean number of outages in a cascade for the ASGWECC_500_1 system

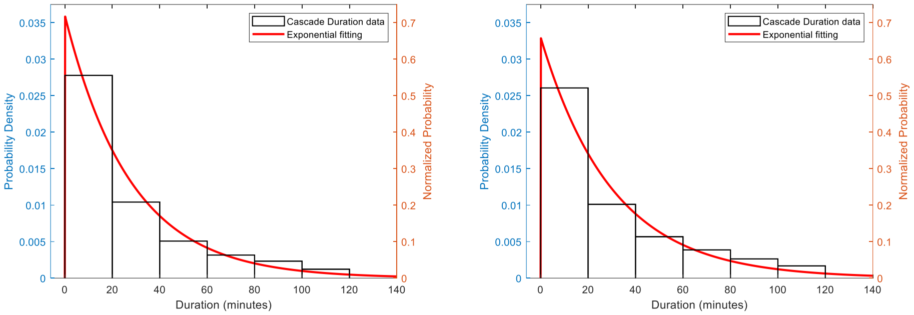
Probability of initial line trip	Uniform	Non-uniform		
		Branch flow	Shortest Path	Connectivity
Mean number of outages	4.40	5.91	3.39	4.72

In Figure 16, the probability distributions of the duration of a cascade are shown. Figure 16(a) considers the uniform probability of any initial line trips and Figure 16(b), (c), and (d) consider the non-uniform probability of initial line trips. The probability of a cascade having a long duration is very low and this probability decreases with the increasing duration. We have fitted our simulated cascade duration data with exponential distribution. In Table XV, the mean duration of a cascade has been shown which is very close to the number we got from the BPA data. Initial line trip probability according to the branch flow of the system has given us the best estimation of the mean duration value compared with the BPA data while probability according to the shortest path underestimated the mean duration the most.



(a) Uniform initial line trip probability

(b) Initial line trip probability according to branch flow



(c) Initial line trip probability according to the shortest path to the boundary

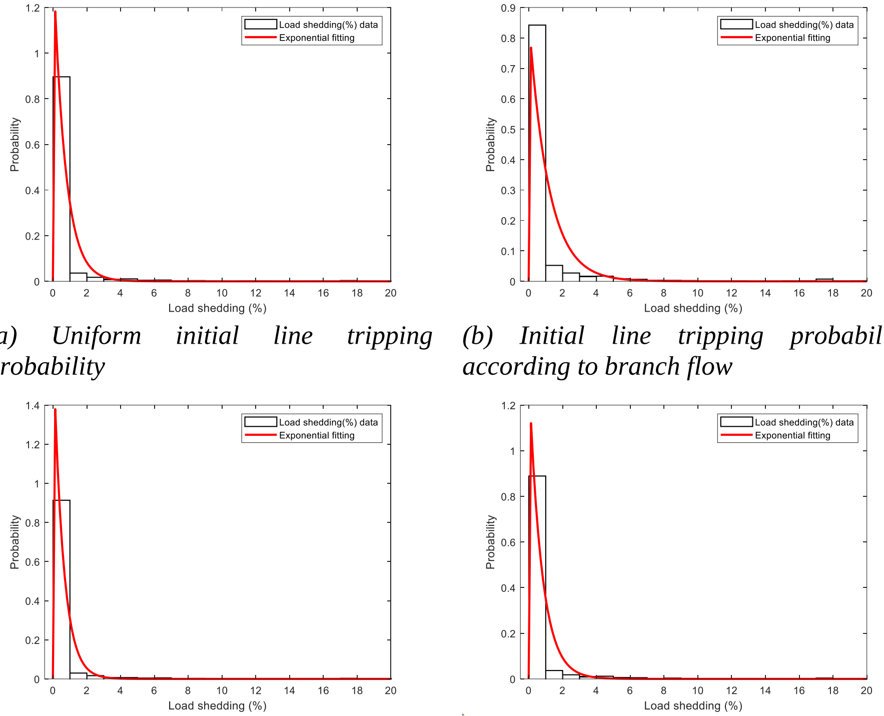
(d) Initial line trip probability according to connectivity

Figure 16. Probability distribution of the cascade duration for the ASGWECC_500_1 system

Table XV. Mean duration of a cascade for ASGWECC_500_1 system

Probability of initial line trip	**Uniform**	**Non-uniform**		
		Branch flow	**Shortest Path**	**Connectivity**
Mean duration (minutes)	29.50	31.17	27.78	30.29

In Figure 17, the probability distributions of the load shedding percentage during a cascade are shown. Figure 17(a) considers the uniform probability of any initial line trips and Figure 17(b), (c), and (d) considers the non-uniform probability of initial line trips. The probability of a cascade having a large load shedding amount is very low and this probability decreases with the increasing load shedding amount. We have fitted our simulated load shedding percentage data with exponential distribution. In Table XVI, the mean load shedding percentage of a cascade has been shown which is lower than in the previous test case. Initial line tripping probability according to the shortest path resulted in the lowest amount of load shedding and the probability according to branch flow resulted in the largest amount of load shedding.



(a) Uniform initial line tripping probability

(b) Initial line tripping probability according to branch flow

(c) Initial line tripping probability according to the shortest path to boundary

(d) Initial line tripping probability according to connectivity

Figure 17. Probability distribution of the load shedding percentage of a cascade for the ASGWECC_500_1 system

Table XVI. Mean load shedding percentage of a cascade for ASGWECC_500_1 system

Probability of initial line trip	**Uniform**	**Non-uniform**		
		Branch flow	**Shortest Path**	**Connectivity**
Mean load shedding (%)	0.70	1.16	0.58	0.75

In Table XVII, the overall summary of the CF processes in terms of the total number of tripped lines and cascade duration has been presented. For test case ACTIVSg500, the mean number of tripped lines in cascade is similar to BPA data for the uniform probability of initial line trips. However, we get the best result while assuming a non-uniform probability of initial line trips according to branch flow. For test case ASGWECC_500, all the simulated results overestimated the mean number of tripped lines during a cascade and we get the best result in comparison with BPA data for a non-uniform probability assumption for initial line trips according to the shortest path to boundary parameter. For cascade duration, the results from both the test cases are similar to BPA data. Here, the non-uniform probability assumption for initial line trips according to the branch flow gives the best results for ASGWECC_500, and the non-uniform probability assumption for initial line trips according to the connectivity of the system gives the best results for the ACTIVSg500 test case.

Table XVII. Overall comparison of cascading failure risk analysis for the BPA system and the synthetic test cases

System	**Number of tripped lines**				**Cascade duration (minutes)**			
BPA	*3.53*				*30.9*			
Probability distribution of initial line trips	**Uniform**	**Non-uniform**			**Uniform**	**Non-uniform**		
		Branch flow	*Shortest path*	*Connectivity*		*Branch flow*	*Shortest path*	*Connectivity*
ACTIVSg500	3.44	**3.46**	3.05	4.07	28.86	28.94	27.32	**29.26**
ASGWECC_500	4.40	5.91	**3.89**	4.72	29.5	**31.17**	27.78	30.29

For the load shedding, the BPA system lacks historical data and we do not have a benchmark for performance comparison. We can only say that from Table XVIII, the load shedding percentage is higher for the ACTIVSg500 test case for both uniform and non-uniform probability distribution of initial line trips.

Table XVIII. Comparison of mean load shedding percentage between two synthetic test cases

System	**Load shedding (%)**			
Probability distribution of initial line trips	Uniform	Non-uniform		
		Branch Flow	Shortest Path	Connectivity
ACTIVSg500	1.78	**1.91**	1.41	2.23
ASGWECC_500	0.70	**1.16**	0.58	0.75

From Table XVII, we can say that the non-uniform probability distribution of initial line trips appears to yield the most consistent results across both test cases. However, to establish a definitive conclusion, further simulations using additional test cases are warranted. These simulations will enable a self-comparison among various test cases, allowing us to determine which probability distribution function is superior in terms of accuracy and reliability. It is also important to note that we currently lack detailed information about the BPA control area load, which limits our ability to precisely replicate real-world conditions in our test cases. Obtaining this information would enhance the accuracy of our comparisons and enable us to make more definitive assessments regarding the effectiveness of different parameters of non-uniform initial line trip distribution. Additionally, the absence of data on RE penetration levels presents another limitation in our study. Integrating RE penetration levels into our simulations would allow us to analyze their impact on cascading failure risk analysis. This presents a promising avenue for future research, as understanding the influence of RE penetration levels on CF risk analysis is essential for enhancing grid resilience and reliability. In summary, while our current findings suggest the superiority of non-uniform distribution of initial line trips, further research efforts are needed to validate and refine our conclusions. Obtaining detailed information about BPA control area load and exploring the effects of RE penetration levels in future simulations will contribute to a more comprehensive understanding of cascading failure dynamics and inform more effective risk mitigation strategies.

3.5. Summary

In conclusion, our analysis highlights the significance of considering various parameters to measure the severity of cascading failure processes in power grids. By examining the number of tripped lines, duration of the CF process, and load shedding requirements, we gain valuable insights into the impact and magnitude of these events. Our study incorporates both uniform and non-uniform probability distributions of initial line trips, revealing that non-uniform distributions offer more accurate estimations for mean outage number and cascade duration. Specifically, the probability distributions based on branch flow and connectivity show promising results for different test cases, indicating their effectiveness in estimating outage number and cascade duration, respectively. However, the lack of load shedding information in the BPA system poses challenges for performance comparison, highlighting the need for comprehensive data sources. Moving forward, further simulations are essential to refine our understanding and validate our findings across different real-world data sources. Obtaining detailed information on the BPA control area load would enhance comparability with simulation data, facilitating more accurate assessments. Additionally, conducting additional simulations on various real-world data sources will provide a clearer perspective on the accuracy of non-uniform distribution models for initial line trips. Overall, our work lays the foundation for improved risk assessment and mitigation strategies in power grid resilience planning, contributing to the robustness and reliability of future grid operations.

4. MICROGRID RESILIENCE

4.1. Introduction

In this study we have developed a multi-layered microgrid simulation model with an optimization-based energy management system. We have explored two critical aspects impacting the optimization and security of microgrid operations: data loss and false data injection attacks.

We have investigated the impact of renewable energy penetration and data loss in battery command in a simulation framework. Data loss in battery command can cause voltage instability, energy supply loss, and increased operational costs in microgrid systems, especially in electricity markets. In contrast to the conventional co-simulation approach, the presented simulation model exclusively utilizes MATLAB to simulate the energy management system in a microgrid and quantify the impacts of data loss of battery command. The simulation results show that on average, more data loss results in higher operational costs, but there are situations where less data loss can be more detrimental to microgrid operation than higher levels of data loss. This research provides valuable insights into the effects of data loss in battery command and its potential economic impact on microgrid operation [55].

Furthermore, this chapter presents a comprehensive analysis of false data injection attacks' impact on microgrid operation introducing a hybrid approach to ensure stability and reliability across diverse scenarios. Two realistic FDI attack models are developed, targeting load profiles and renewable generation data. Simulation results reveal potential load balance discrepancies during islanded microgrid operation under these attacks using optimization-based EMS. To mitigate these challenges, the proposed hybrid approach integrates optimization-based energy management with adaptive control schemes, ensuring stable microgrid operation in various conditions. Our present work lays the foundation for further advancement incorporating artificial intelligence techniques which represents a promising avenue to enhance the accuracy and effectiveness of our initial model.

Together, our contributions provide valuable insights into enhancing the optimization and security of microgrid operations, addressing pertinent challenges in the field and paving the way for further advancements in microgrid research.

4.2. Microgrid Overview

A microgrid can be seen as a modern small-scale electrical power grid infrastructure for better efficiency, reliability, and integration of renewable energy sources. It can be defined as an interconnection of energy storage devices, distributed energy resources, and loads with defined boundaries that act as a single controllable entity [76]. Microgrid can be defined as a system that enables a two-way flow of both powers for the electrical network and information for the communication network. This bidirectional communication of power and information offers various advantages such as efficient monitoring of the network conditions, predicting failures, and reducing maintenance costs [77]. By leveraging advanced control techniques and real-time monitoring, microgrids can operate in islanded mode, disconnected from the main grid, and seamlessly switch to grid-connected mode whenever required. The integration of renewable energy sources and energy storage systems in a microgrid can also help in reducing carbon emissions and providing a reliable and sustainable source of power.

4.2.1. Microgrid Components

A microgrid comprises various components that work together to provide a reliable and sustainable power supply. These components include [78]:

Distributed Energy Resources (DERs): DERs are decentralized power generation sources located within the microgrid. They can include renewable energy technologies like solar panels, wind turbines, biomass generators, and small-scale hydroelectric systems. DERs generate electricity locally and contribute to the power supply of the microgrid.

Energy Storage Systems (ESS): ESSs store excess energy generated by DERs during periods of low demand and supply it during periods of high demand. Common types of ESSs include batteries, flywheels, and pumped hydro storage. Energy storage enhances the stability and reliability of the microgrid by balancing supply and demand fluctuations and improving the integration of intermittent renewable energy sources.

Loads: Loads in a microgrid refer to the electrical consumption from various sources, including residential buildings, commercial entities, and industrial parks. These loads can vary in terms of power demand, duration, and characteristics, and they form the basis for energy consumption within the microgrid.

Control and Monitoring Systems: These systems ensure the efficient and reliable operation of the microgrid by monitoring and controlling the power flow, voltage, frequency, and other parameters. They use advanced algorithms and communication technologies to coordinate the operation of DERs, ESSs, and other components, optimizing their performance and responding to changes in demand or grid conditions.

Point of Common Coupling (PCC): The PCC is the electrical connection point between the microgrid and the utility system. It is typically located at the low-voltage bus of the substation transformer. The PCC serves as the interface between the microgrid and the main utility grid, allowing for bi-directional power flow and the exchange of electricity when needed.

By integrating and coordinating these components, microgrids offer greater control, resilience, and efficiency in meeting electricity needs, supporting renewable energy integration, and enhancing the overall sustainability of the power system.

4.3. Cyber Attack Types and Targets in Microgrid

There are several types of cyber-attacks that can target microgrid operations. These attacks aim to exploit the vulnerabilities in the microgrid's communication, control, and information infrastructure.

4.3.1. Attack Types

Some common types of cyber-attacks in microgrids include the following:

False Data Injection/ Data Manipulation*:* This attack involves intentionally injecting inaccurate or manipulated data into the microgrid's monitoring, control, or communication systems. By tampering with the data, malicious actors can deceive the EMS and compromise the integrity and reliability of microgrid operations. Such attacks can lead to incorrect decision-making, suboptimal control actions, and potential disruptions in energy supply.

Denial-of-Service Attacks: In this type of attack, the attacker overwhelms the microgrid's communication or control systems with a flood of requests or data, causing them to become unresponsive or unavailable.

Malware and Ransomware: Malicious software can be injected into the microgrid's systems, compromising their integrity and functionality. Ransomware attacks encrypt critical system data and demand ransom in exchange for restoring access.

Man-in-the-Middle Attacks: In this type of attack, the attacker intercepts and modifies communication between components in the microgrid. This allows them to eavesdrop on sensitive information, inject malicious commands, or alter data exchanged between devices.

Physical Attack: Physical attacks involve the deliberate physical manipulation or destruction of microgrid components, such as tampering with equipment or cutting power lines. While not strictly cyber-attacks, they can have severe consequences on the microgrid's operation.

4.3.2. Attack Targets

In a microgrid, various types of data can be targeted in a cyber-attack. Here are some examples of data that can be under attack:

Control Data: Control data includes commands and instructions sent to the microgrid components for operation and coordination. Attackers can manipulate or disrupt control data to manipulate the behavior of the microgrid, leading to incorrect operation or instability.

Sensor Data: Sensor data is collected from various sensors deployed in the microgrid to monitor its performance, including voltage, current, temperature, and renewable energy generation. Manipulating sensor data can mislead the control algorithms and decision-making processes, causing incorrect system operation.

Market Data: If the microgrid operates in an electricity market, market data such as real-time prices, demand forecasts can be under attack. Manipulating market data can impact the microgrid's economic performance and decision-making processes, leading to financial losses.

Operational Data: Operational data includes historical data, performance logs, maintenance records, and system configurations. Attackers can target operational data to gain unauthorized access, extract sensitive information, or disrupt the normal functioning of the microgrid.

Customer Data: In cases where the microgrid serves customers, their data, including personal information, consumption patterns, and billing details, can be targeted. Breaching customer data can result in privacy violations, financial losses, or identity theft.

Data-related attacks in microgrid systems encompass a variety of types and can target different types of data within the system. These attacks pose significant risks and can occur at any time, whether randomly or during critical periods, resulting in severe consequences for microgrid operation.

4.4. False Data Injection Attack Model

There are various types of cyber-attacks targeted towards cyber physical system like microgrid; among these, FDIAs stand out as the most prominent, frequent, and effective tactics favored by attackers, burdening controllers and leading to revenue losses, device mismanagement, and load dysfunction [47]. Attackers can manipulate data through various FDI techniques, including reading, modifying, or deleting it. These attacks come in different types, such as continuous, interim, stealthy, constrained, unconstrained, and time-varying FDI attacks. They also vary in duration and intensity, with transient attacks causing strong perturbations over a short period and continuous attacks remaining undetected for longer periods. Intensity-wise, attacks can be constant or variable, with constant attacks having similar magnitudes and variable attacks being stochastic or asymptotic.

The choice of FDIAs as the primary focus for modeling cyber-attacks on cyber-physical systems like microgrids stems from several factors. Firstly, FDIAs are among the most prominent, frequent, and effective tactics employed by attackers targeting such systems. Their prevalence and effectiveness make them a critical threat that requires thorough analysis and mitigation strategies. Moreover, FDIAs can manifest in various forms, including reading, modifying, or deleting data, providing attackers with a versatile toolkit for manipulating system behavior. This diversity of attack techniques necessitates a comprehensive understanding of FDIA dynamics to develop effective defense mechanisms. Furthermore, FDIAs exhibit different characteristics, such as continuous, interim, stealthy, constrained, unconstrained, and time-varying variations, each posing unique challenges for detection and mitigation. Their varying durations and intensities, ranging from transient perturbations to continuous, undetected attacks, underscore the need for a nuanced approach to modeling and analyzing FDIA scenarios. While other attack models exist, such as denial-of-service attacks, ransomware or man-in-the-middle attacks, FDIA's unique characteristics, prevalence, and effectiveness make them particularly worthy of study in the context of microgrid security. By focusing on FDIA modeling, researchers can gain valuable insights into the vulnerabilities and potential mitigation strategies specific to these sophisticated cyber-attacks, ultimately enhancing the resilience and security of microgrid systems against evolving threats.

We constructed two types of FDIA model to simulate FDI attack in the microgrid EMS. One is continuous intensity FDIA model (type 1), in which, the false data injection occurs continuously over a defined period. The intensity of the attack remains within a constant range throughout the attack duration. The attacker injects false data into the system at a consistent intensity, which can mimic normal system behavior to a certain extent. This model is characterized by a steady flow of false data into the system. Another is probabilistic intermittent FDIA model (type 2). In this type of attack model, the false data injection occurs intermittently with a certain probability. Instead of a continuous flow, the attack happens sporadically, with periods of normal system behavior interspersed between the attack intervals. The attacker injects false data into the system, with a predefined probability dictating the likelihood of successful execution of this attack. This model is characterized by unpredictable and sporadic bursts of false data, making it more challenging to detect compared to continuous attacks.

In the continuous intensity FDI attack model (type 1), the attacker defines the start and end times of the attack (t_{start} and t_{end}) and sets the maximum and minimum intensity of the attack (I_{max} and I_{min}). With complete knowledge of the system, the attacker can strategically inject data within the stability limits, making detection and mitigation challenging. At each time step during the attack, a random intensity value (I) is generated from a uniform distribution within the interval (I_{max}, I_{min}).

$$if\ t_{start} \leq t \leq t_{end}$$

$$I(t) = random(I_{max}, I_{min})$$

$$D_{att}(t) = D_{act}(t) + \frac{I(t)}{100} \times D_{act}(t) \tag{4.1}$$

Here, $D_{act}(t)$ represents the actual data and $D_{att}(t)$ represents the attacked data at time t.

For probabilistic intermittent FDI attack model (type 2), during the specified time interval $t_{start} \leq t \leq t_{end}$, at each step, there is a probability ε_{attack} of constructing and injecting the attack. If the probability is not met, no attack is conducted. This type of attack can also test the response speed of detection methods.

$$if\ t_{start} \leq t \leq t_{end}$$

$$I(t) = random(I_{max}, I_{min})$$

$$D_{att}(t) = \begin{cases} D_{act}(t) + \frac{I(t)}{100} \times D_{act}(t),\ if\ random(0,1) < \varepsilon_{attack} \\ D_{act}(t), otherwise \end{cases} \tag{4.2}$$

4.5. Microgrid Operation Strategy

Microgrids offer the flexibility to operate in both grid-connected and island mode, adapting to varying energy supply and demand conditions. Grid-connected microgrids may shift to island mode for scheduled maintenance, peak demand management, grid instability, or emergencies, guaranteeing continuous power supply and enhancing system resilience [79–82]. During grid-tied operation, a microgrid leverages the buffering effect of the main electric grid, partly mitigating the impact of false data injection attacks and managing resulting power imbalances. If FDIA persists undetected or unresolved, the microgrid will continue to operate, though sub-optimally, while adhering to operational constraints. However, in islanded mode, FDIA presents a more significant threat, requiring careful management to uphold network power balance, integrity, and stability.

In our proposed methodology, we have proposed a hybrid approach combining optimization-based EMS with tailored adaptive control schemes, specifically crafted for islanded microgrid operations during FDIA scenarios. This hybrid strategy ensures adaptability and resilience, leveraging optimization-based EMS for normal grid-tied operations, even in the face of FDIA challenges, while employing adaptive control methods to safeguard microgrid functionality during islanded operation under FDIA conditions.

4.5.1. Optimization-based Energy Management System

In microgrid systems, EMSs play a crucial role in maximizing renewable energy integration, economic efficiency and ensuring reliability. They address dispatch optimization problems by considering production and storage capacities, market data, and operational constraints, relying on accurate forecasts. Communication networks coordinate the operation of diverse energy resources, including renewables, generators, and storage systems. Our study employs an optimization-based EMS to manage microgrid operation in normal condition, addressing these challenges effectively.

Objective Function: In our study, the microgrid EMS optimizes to minimize operational costs while ensuring power balance and meeting system constraints. These costs include grid electricity, diesel generator, and battery storage expenses, with optimization targeting a 24-hour horizon.

$$\min(\sum_{t=0}^{N}(C_{grid}(t) \times P_{grid}(t)) \times \Delta t + \sum_{t=0}^{N}\left(P_{gen}(t)\right) \times C_{gen} \times \Delta t + \sum_{t=0}^{N}\left(P_{batt}(t)\right) \times C_{batt} \times \Delta t) \qquad (4.3)$$

Here, $C_{grid}(t)$ represents the cost of grid electricity at time t, $P_{grid}(t)$ represents the power flow from the grid to the microgrid at time t, C_{gen} represents the diesel generator fuel cost per unit of electric power, $P_{gen}(t)$ represents the output power of the generator to the microgrid at time t, $P_{batt}(t)$ represents the power flowing into or out of the battery energy storage system (BESS) within the microgrid at time t, C_{batt} represents the operational and maintenance cost of the BESS per unit of electric power, and Δt represents the specific time slot. In our study, we have data for every time slot (Δt) and we are optimizing the operational cost of the microgrid for the next 24-hour horizon in every time slot.

Constraints: The EMS optimization in this study involves a constrained optimization problem with two distinct types of constraints. These constraints encompass power balance and input/output power to the battery, serving as equality constraints within the optimization process.

$$P_{pv}(t) + P_{grid}(t) + P_{batt}(t) + P_{gen}(t) = P_{load}(t) \tag{4.4}$$

$$E_{batt}(t) = E_{batt}(t-1) + P_{batt}(t) \times \Delta t \tag{4.5}$$

Here $P_{pv}(t)$ represents the PV output power at time t, $P_{load}(t)$ represents the total load that needs to be served at time t, $E_{batt}(t)$ represents the stored energy of the BESS at time t. In (4.4), the power balance equation ensures the load is served by the available generation. In (4.5), the equation relates the battery energy with the charging/discharging rate at every time slot.

The operating limits of the components of the microgrid are the inequality constraints of the optimization.

$$X_{min} \leq X \leq X_{max} \tag{4.6}$$

Here, X represents P_{grid}, P_{batt}, P_{gen} and E_{batt}, X_{min} is the lower boundary and X_{max} is the upper boundary of the parameters.

4.5.2. Adaptive Control Scheme

Adaptive control schemes for microgrid operation refer to strategies that dynamically adjust control parameters or algorithms based on changing operating conditions or system dynamics. These schemes aim to optimize microgrid performance and enhance its resilience in response to variations in renewable energy generation, load demand, grid disturbances, or other factors. Adaptive control schemes may include techniques such as heuristic approaches, which enable microgrids to adapt their control actions in real-time to maintain stability, improve efficiency, and ensure reliable operation. Heuristic approaches involve using practical rules or strategies that prioritize speed and simplicity over finding the optimal solution. Examples of heuristic approaches in microgrid operation include priority-based dispatch, droop control, and load shedding strategies.

In our proposed adaptive control method, we utilize real-time sensor data for load, PV generation, and BESS status, omitting the use of 24-hour horizon forecast data to enhance resilience against FDIA. Droop control settings are implemented for diesel generators to adjust power output based on requirements, leading to frequency deviations. The parameters are configured so that half of the rated output power is maintained for the rated frequency. Our primary focus lies in prioritizing renewable energy sources for meeting load demand, followed by BESS utilization based on SOC. The diesel generator covers any unmet load, affecting system frequency deviation. If load demand exceeds the generator's capacity, a predetermined portion is shed to maintain power balance. Conversely, in surplus scenarios, excess PV generation may be curtailed to ensure balance.

4.6. Simulation Model

In our simulation setup, the microgrid operates in grid-tied mode under normal conditions and can seamlessly transition to islanded mode when required. We have assumed access to historical data on weather information, customer load, and electricity market prices specific to the microgrid location. These datasets served as the basis for forecasting a 24-hour horizon in our EMS optimization. We utilized an open-source dataset [83] providing 24-hour ahead forecasted data for every fifteen minutes using a recurrent neural network (RNN) with the Keras Python library. This forecasted data served as direct input for our EMS, which incorporated additional inputs such as microgrid parameters, BESS parameters, and other constraints.

Figure 18 illustrates the working diagram of the proposed optimization-based EMS simulation model, comprising three main components. The first part involves datasets of weather information, customer load, and electricity market data, processed using forecasting techniques to generate 24-hour horizon data for renewable energy (RE) generation, load profile, and variable electricity prices. These serve as inputs for the second part, EMS, which employs an optimization approach to evaluate optimal battery control, load control, and diesel generator dispatch commands. These commands are then sent to the physical microgrid, which constitutes the third part of our simulation framework. Real-time measurements of load, RE generation, and BESS state of charge are used to update the database and system parameters, facilitating the updating of forecasted data. The EMS conducts optimization every thirty minutes using the updated forecasted data and transmits optimized commands for battery, load, and diesel generator dispatch. For constrained optimization, we utilize MATLAB's 'fmincon' solver. The EMS optimizes operational costs every thirty minutes based on forthcoming 24-hour data and dispatches control instructions to microgrid controllers accordingly, ensuring optimal operation based on the latest information. The physical microgrid is modeled using the power flow function in our simulation setup.

4.6.1. Simulating Data Loss in Battery Command

Data loss in communication systems can have vital impacts on the operation of any system that relies on data transfer for control or decision-making. In a microgrid, where energy generation and consumption need to be carefully managed and coordinated, data loss can result in suboptimal control decisions or even system instability. For example, if battery control commands are lost, the microgrid may not be able to properly utilize its energy storage resources, leading to reduced efficiency and increased operating costs. In addition, if data loss occurs during critical events such as sudden load changes or system failures, the microgrid may not be able to respond appropriately, potentially resulting in blackouts or other disruptions. Therefore, it is important to consider the impact of data loss in communication channels when designing and operating microgrids. In our simulation model, we have simulated probabilistic data loss in battery command data to assess the economic impact of microgrid operation. Probabilistic data loss refers to the random loss of data that can occur in communication channels or storage devices. One way to model this type of loss is through probability distributions, such as the uniform distribution. The uniform distribution assumes that the probability of losing data is equal across all possible values. In other words, each possible data value has the same likelihood of being lost. This distribution can be used to simulate the effects of data loss in a system and to quantify the potential impact on the system's performance. By incorporating probabilistic data loss models into simulation tools, researchers and engineers can better understand the behavior of complex systems under uncertain conditions, and design more robust and reliable systems.

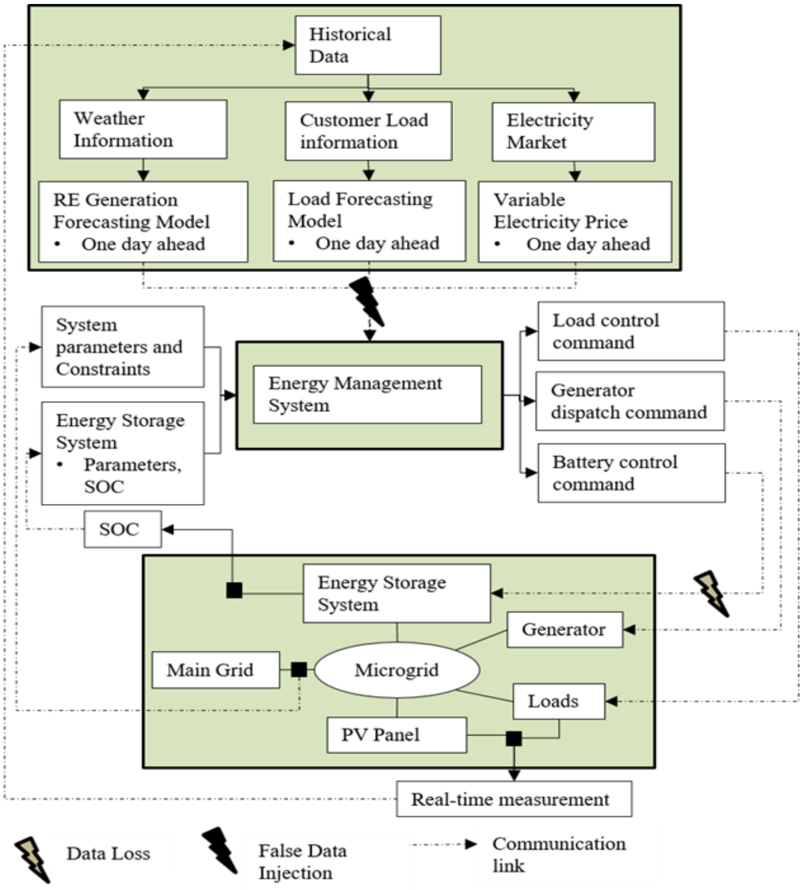


Figure 18. Working flow for the optimization-based EMS

4.6.2. Simulating FDIA in EMS

Our simulation model is primarily configured to operate the microgrid in grid-tied mode with the capability to transition to island mode for several hours, a common scenario in microgrid operation. During islanded operation, if FDIA is detected, the microgrid switches to adaptive control modes, relying solely on real-time sensor data due to potential manipulation of forecasted data. Figure 19 illustrates the working flow of the adaptive control methods of microgrid operation. The generator operates in droop control mode, dispatching half of its rated power at the rated frequency and adjusting generation as needed to maintain power balance. It is advisable to have backup redundancy for real-time sensor data in critical systems like microgrids, especially in the face of potential cyber threats like FDIAs. Redundancy options may include redundant sensors or communication systems. Following a 24-hour microgrid simulation, we calculate the total electricity cost, generation-load mismatch, and final SOC of the BESS. In cases of load shedding, a penalty cost is added to the total electricity cost, typically assumed as 240c/kWh according to the literature [84–86].

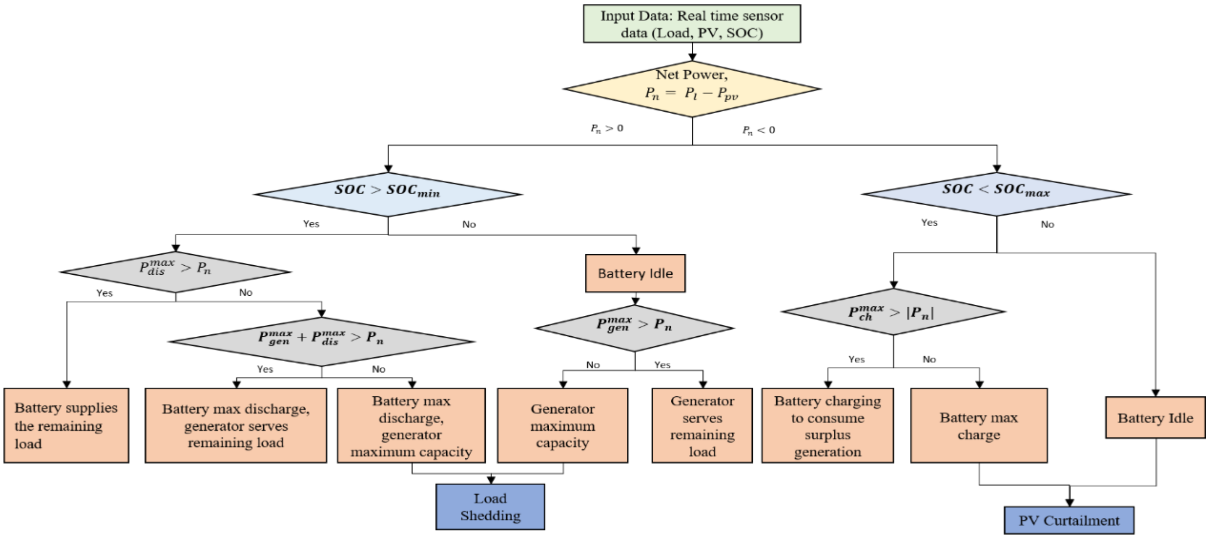

Input Data: Real time sensor data (Load, PV, SOC)
Net Power, $P_n = P_l - P_{pv}$
$P_n > 0$
$P_n < 0$
$SOC > SOC_{min}$
Yes
No
$SOC < SOC_{max}$
Yes
No
$P_{dis}^{max} > P_n$
Yes
No
Battery Idle
$P_{ch}^{max} > |P_n|$
$P_{gen}^{max} + P_{dis}^{max} > P_n$
Yes
No
$P_{gen}^{max} > P_n$
No
Yes
Yes
No
Battery supplies the remaining load
Battery max discharge, generator serves remaining load
Battery max discharge, generator maximum capacity
Generator maximum capacity
Generator serves remaining load
Battery charging to consume surplus generation
Battery max charge
Battery Idle
Load Shedding
PV Curtailment

Figure 19. Working diagram for adaptive control schemes for microgrid operation

To implement the hybrid approach of microgrid operation effectively, certain infrastructure requirements must be met. Firstly, the installation of an advanced FDIA detection model is essential. This model will enable the accurate detection of cyber-attacks on the system, facilitating the seamless transition from optimization-based EMS to adaptive control mode when necessary. By promptly identifying and mitigating FDIAs, the microgrid can maintain reliable operation and mitigate potential risks. Furthermore, the adaptive control schemes utilized in the hybrid approach rely heavily on real-time sensor data. Therefore, it is crucial to ensure the integrity and reliability of this data. Redundancy measures can be implemented to enhance data reliability and resilience against corruption. For instance, redundant sensors can be deployed throughout the microgrid to provide backup data in case of sensor failure or data manipulation. Additionally, redundant communication systems can be employed to ensure uninterrupted data transmission and communication between system components. By implementing these infrastructure requirements, such as advanced FDIA detection models and redundant sensor and communication systems, the hybrid approach can operate effectively and ensure reliable microgrid operation. These measures enhance the resilience of the microgrid against cyber threats and contribute to maintaining stable and secure energy distribution within the system.

4.7. Result and Analysis

4.7.1. Impact of Data Loss

In this study, we have simulated the impacts of increasing data loss in battery command for various renewable energy penetration on a small microgrid. In our simulation, the microgrid has a peak load of 10.2 kW. It is also composed of a PV system as a distributed energy resource and a battery energy storage system. We have integrated different PV penetration (10%, 50%, 100%) to see the economic impact on microgrid operation. For 10% PV penetration, we have used a 15kWh battery energy storage system with a maximum charging/discharging rate of 1kW and for 50% and 100% PV penetration, we have used a 75kWh battery energy storage system with a maximum charging/discharging rate of 5kW. For each scenario, we have simulated different amounts of data loss (0%, 10%, 30%, 50%, 100%) in battery command to see the impact on microgrid operation. We have simulated every case several times and compared the results.

In Figure 20, we can see a specific case of a 10% data loss scenario for 10% PV penetration in the microgrid where Figure 20(a) represents the state of charge of the battery system during the day. And in Figure 20(b), we can see how the total load is served by the PV generation, grid electricity, and battery output power during the whole day. In Figure 21 and Figure 22, we can see two cases of a 10% data loss scenario for 50% and 100% PV penetration in the microgrid.

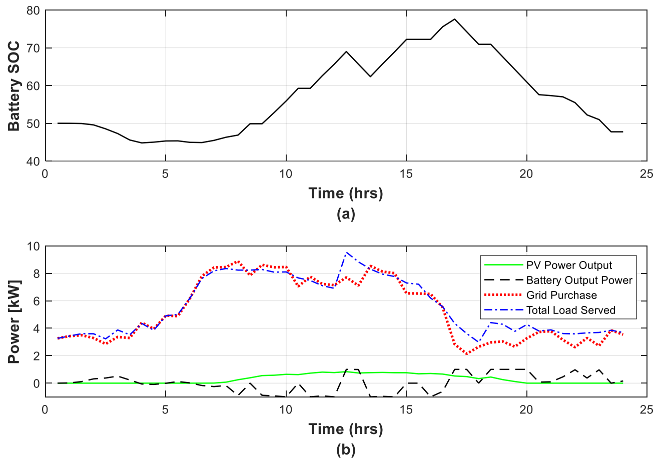
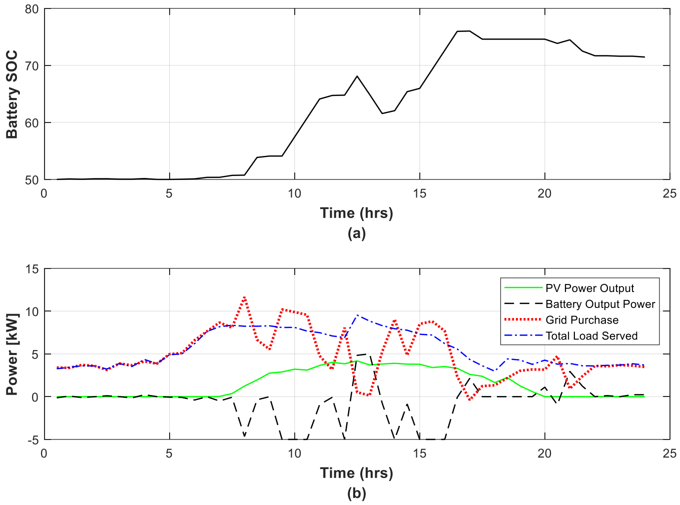


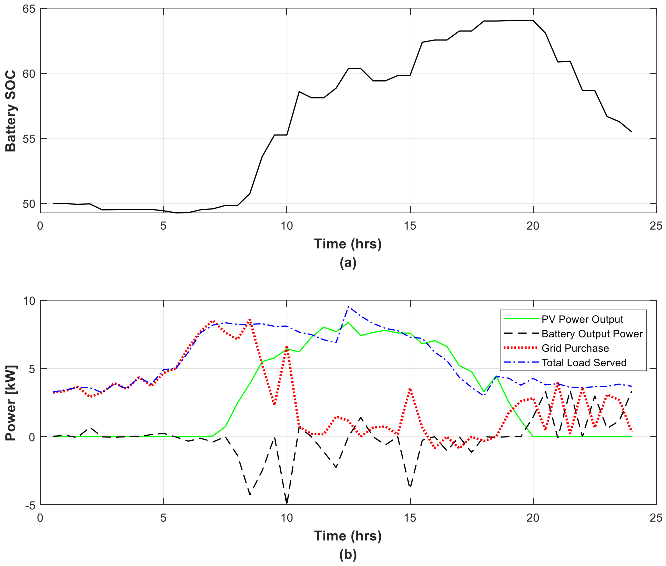
Figure 20. A specific case of 10% data loss scenario for a 10% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time



(a)

(b)

Figure 21. A specific case of 10% data loss scenario for a 50% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time



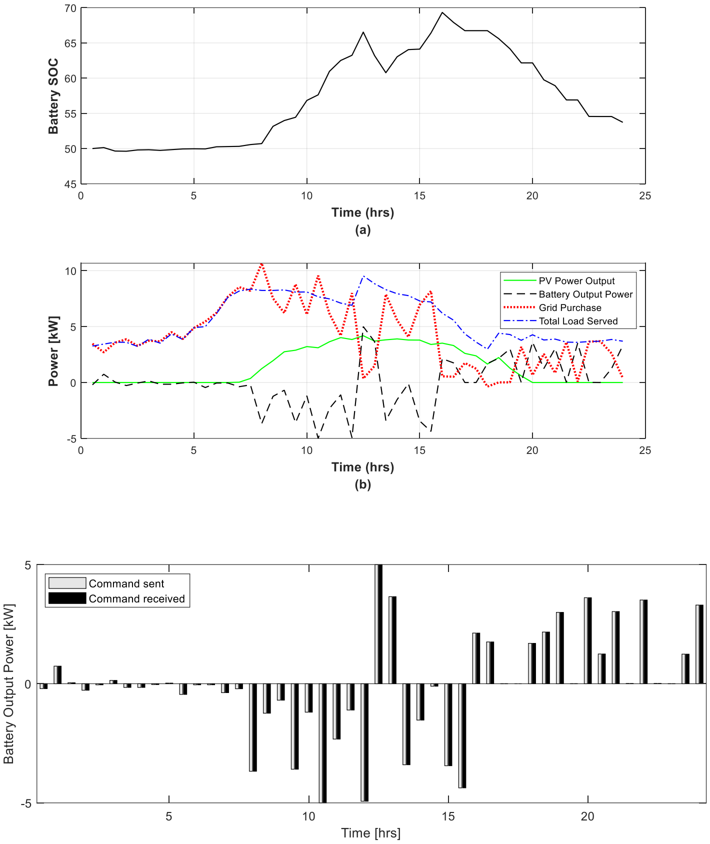
(a)

(b)

Figure 22. A specific case of 10% data loss scenario for a 100% PV penetration in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time

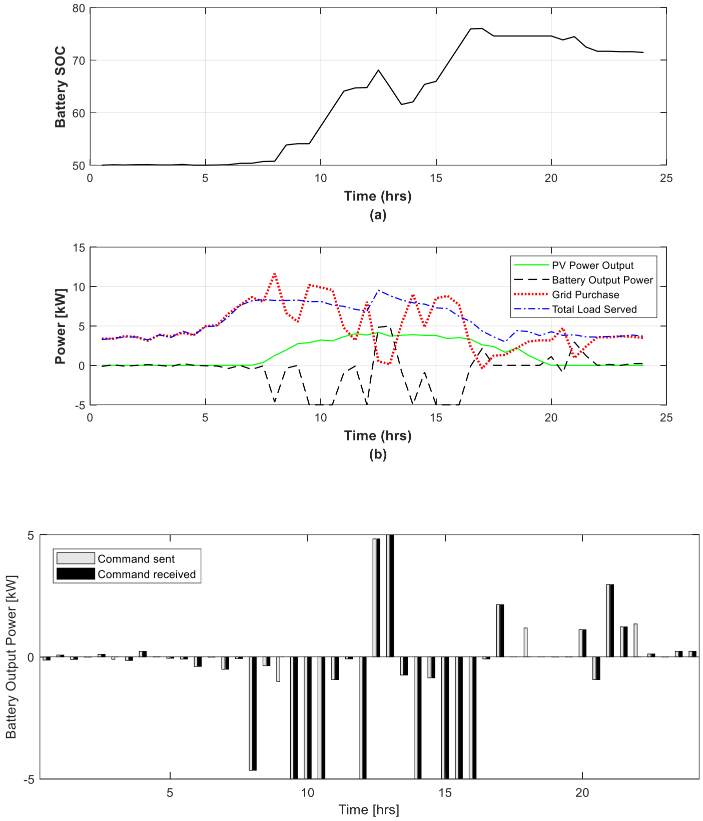
In Figure 23, we can see specific cases of 0% data loss scenario for 50% PV penetration in the microgrid where Figure 23(a) represents the state of charge of the battery system during the day.

And in Figure 23(b), we can see how the total load is served by the PV generation, grid electricity, and battery output power during the whole day. In Figure 24-27, we can see other cases of 10%, 30%, 50%, and 100% data loss scenarios for 50% PV penetration in the microgrid.



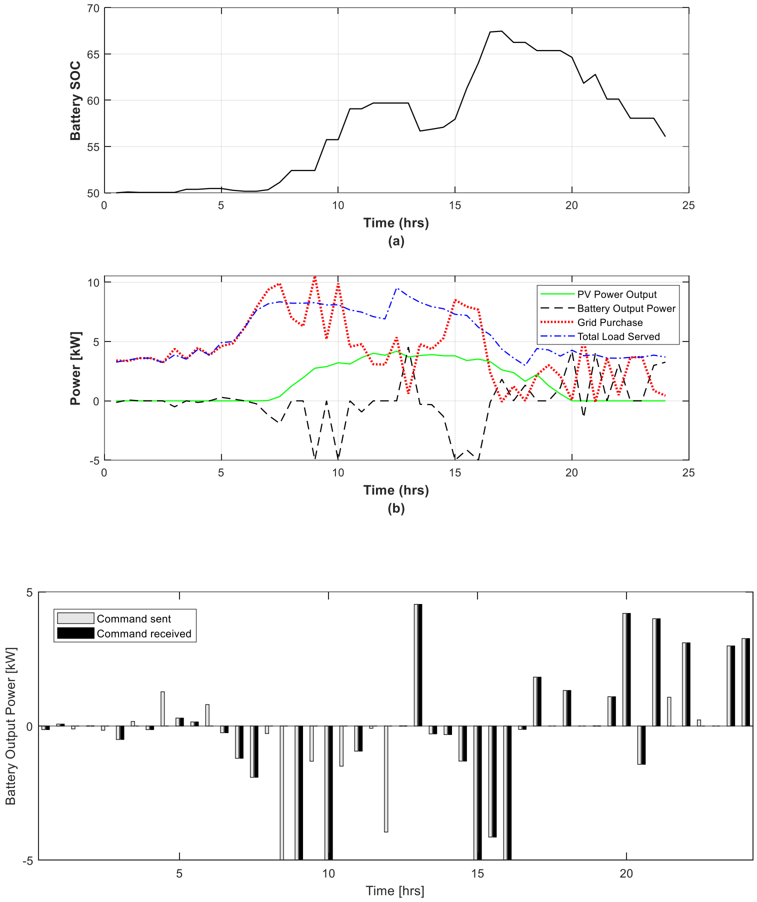
(c)

Figure 23. A specific case of 50% PV penetration scenario with no data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command



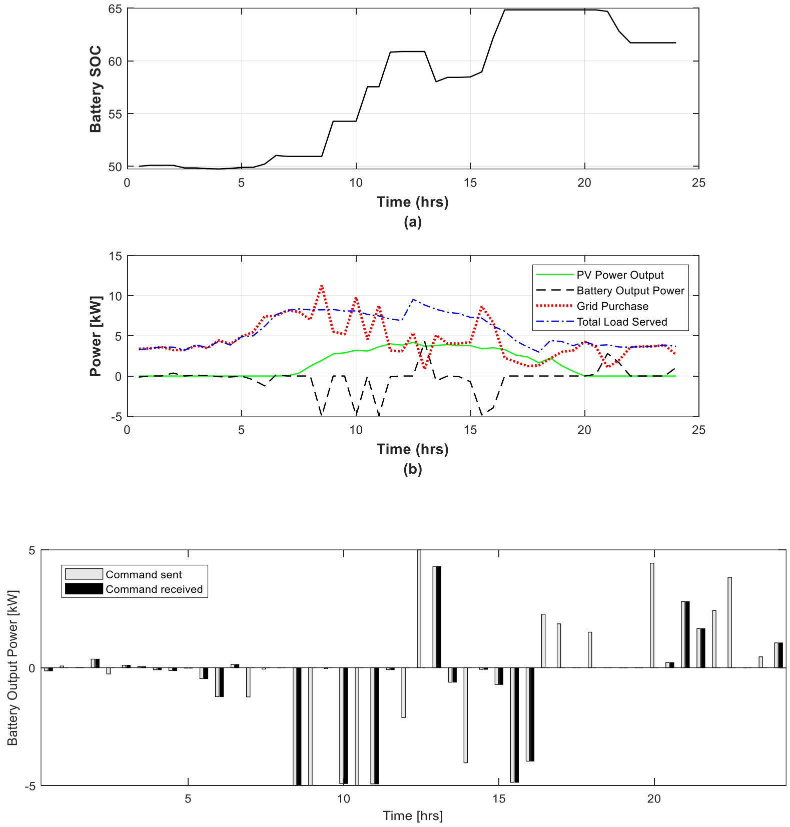
(c)

Figure 24. A specific case of 50% PV penetration scenario with 10% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command



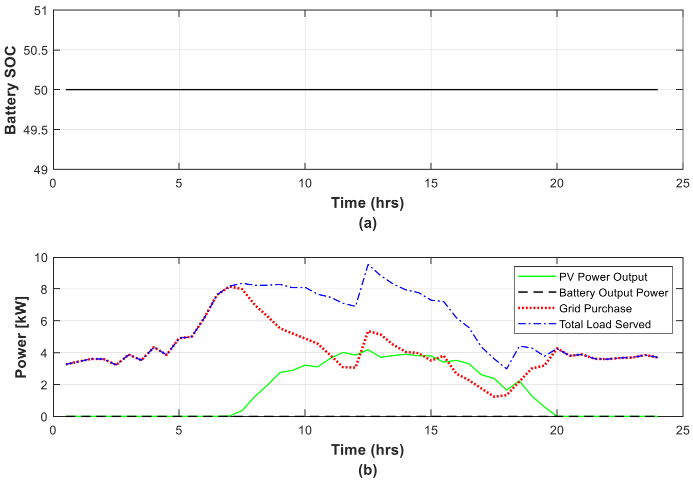
(c)

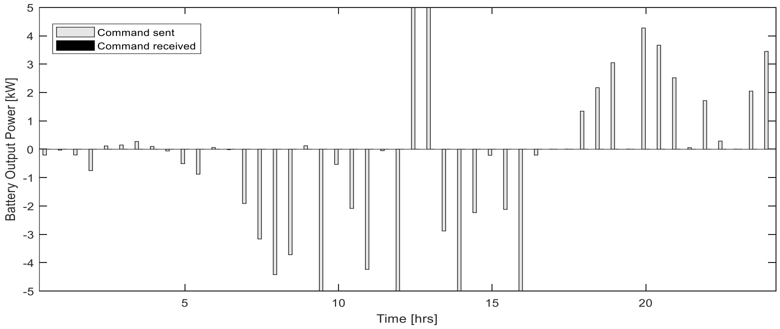
Figure 25. A specific case of 50% PV penetration scenario with 30% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command



(C)

Figure 26. A specific case of 50% PV penetration scenario with 50% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command





(c)

Figure 27. A specific case of 50% PV penetration scenario with 100% data loss in the microgrid (a) State of charge of the BESS, (b) Optimized power profiles of PV generation, battery output, grid electricity, and total load over time, (c) Battery charging/discharging command

In Figure 23-27(c), we can see how different levels of data loss impact the charging-discharging schedule command of the battery system in the microgrid. Whenever the data is lost, the battery will neither be charged nor be discharged for this specific time slot and the system will wait for the next command to receive.

Figure 28 illustrates the varying grid electricity costs of the microgrid under the same level of data loss. In each setup, with a 10% photovoltaic (PV) penetration and data loss amounts of 10%, 30%, and 50%, fifteen different simulations were conducted. There are instances where a 10% data loss leads to higher operational costs compared to a 50% data loss. This outcome is primarily influenced by the timing of data loss. If the battery command is lost during a period of high-priced grid electricity, when the battery should be discharged to meet the load demand, it significantly raises the operational cost of the microgrid. Consequently, even with a lower data loss percentage, the loss occurring during critical time slots can result in elevated operational costs. This highlights the importance of considering the timing and context of data loss in assessing its impact on microgrid operation. In Figure 29, we can see the varying BESS cost for the same amount of data loss in different cases.

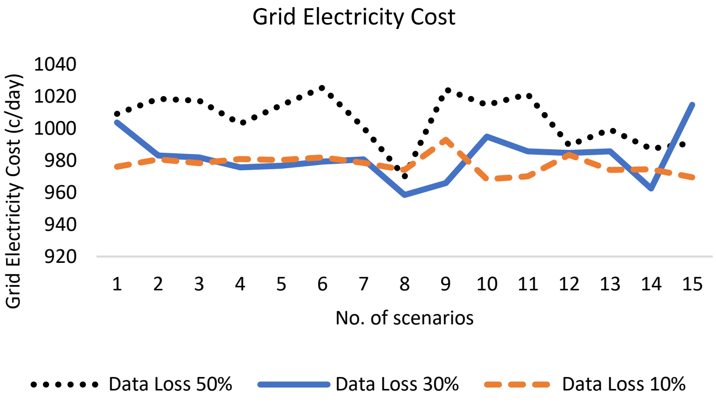


Figure 28. Comparison of grid electricity cost for the microgrid with 10% PV penetration with varied amounts of data loss

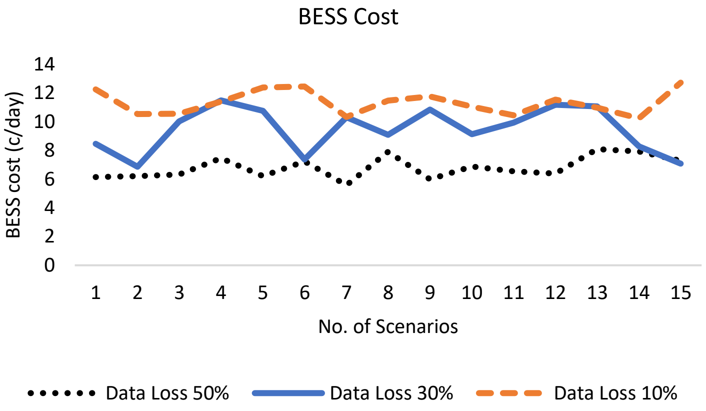


Figure 29. Comparison of BESS cost for the microgrid with 10% PV penetration with varied amounts of data loss

In Figure 30 and Table XIX, we can see the average grid electricity cost for different PV penetration with varied amounts of data loss. We can notice that high PV penetration results in less grid electricity cost in microgrid operation as it should. Also, with increasing data loss amount, the average grid electricity cost increased in most cases.

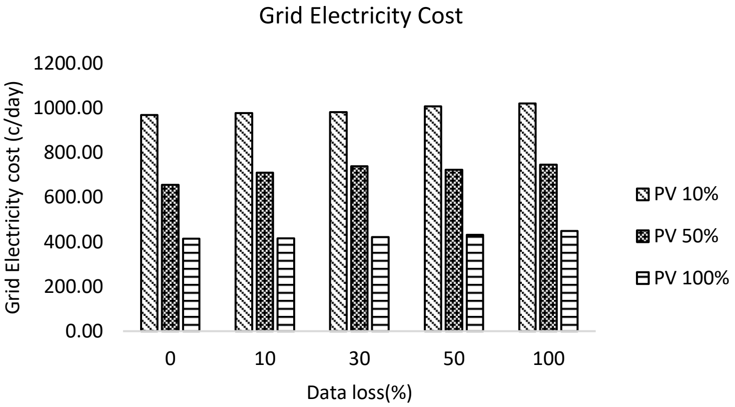


Figure 30. Comparison of average grid electricity cost for varying PV penetration and data loss rate in microgrid

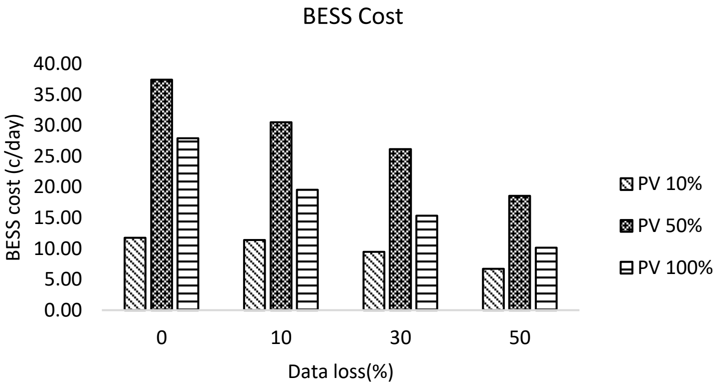


Figure 31. Comparison of average BESS cost for varying PV penetration and data loss rate in microgrid

Table XIX. Comparison of average grid electricity cost for varying PV penetration and data loss rate in microgrid

Data Loss / PV %	Grid Electricity Cost (c/day)				
	0	**10**	**30**	**50**	**100**
10	969.64	977.63	982.33	1007.86	1021.10
50	656.12	710.55	739.41	723.31	746.65
100	414.53	417.04	421.50	432.63	448.88

For 10% PV penetration in the microgrid, 10%, 30%, 50%, and 100% data loss result in on average 0.8%, 1.3%, 3.9%, and 5.3% increase in grid electricity cost respectively. For 50% PV penetration in the microgrid, 10%, 30%, 50%, and 100% data loss result in on average 8.3%, 12.7%, 10.2%, and 13.8% increase in grid electricity cost respectively. For 100% PV penetration in the microgrid, 10%, 30%, 50%, and 100% data loss result in on average 0.6%, 1.7%, 4.4%, and 8.3% increase in grid electricity cost respectively.

In Figure 31 and Table XX, we can see the average BESS cost for different PV penetration with varied amounts of data loss. We can notice that, with increasing data loss amount, the average BESS cost decreased.

Table XX. Comparison of average BESS cost for varying PV penetration and data loss rate in microgrid

Data Loss **PV %**	**BESS Cost (c/day)**				
	0	**10**	**30**	**50**	**100**
10	11.77	11.38	9.46	6.70	0
50	37.45	30.52	26.18	18.59	0
100	27.93	19.55	15.37	10.15	0

Despite the intuitive expectation that less data loss would always result in lower operational costs in a microgrid, this is not always the case. The timing of the data loss plays a crucial role in cost minimization. Additionally, the microgrid operates on a 24-hour ahead optimization basis, where control commands are generated using forecasted data for the next 24 hours. For instance, at noon, the optimization considers forecasted data 24 hours ahead to determine the optimal control commands. Consequently, when calculating the operational cost for a single day, it may not reflect the entire picture, as higher costs on a particular day may be part of an optimized set of actions within the 24-hour horizon.

4.7.2. Impact of FDIA

Our microgrid simulation model comprises three buses interconnected in a radial configuration. There is a point of connection between bus 1 and the utility grid and bus 1 also accommodates a diesel generator and load. Bus 2 and bus 3 each integrate PV system, battery storage system, and load components (Figure 32). The total peak load of the microgrid amounts to 25 kW, while the combined PV capacity is 16.75 kW. The microgrid incorporates a diesel generator with a capacity of 25 kW and each battery storage system has a capacity of 75 kWh, with a maximum charging and discharging rate of 5 kW. The microgrid can operate both in grid-tied and islanded mode. In Figure 33, we can see the actual load profile, PV power output and utility grid electricity price during a day for the microgrid.

In our simulation model, we conducted a thorough analysis of microgrid operation over a 24-hour period, exploring various scenarios by adjusting parameters such as microgrid operation methods, FDIA characteristics, and islanded mode operation time. We compared two microgrid operation methods: traditional optimization-based EMS and a hybrid EMS combining optimization-based strategies with adaptive control during FDIA attacks in islanded mode. Using two types of FDIA attack models, we manipulated load and PV generation data to assess economic impacts and system parameters like state of charge and load mismatch percentages. Each intensity level of FDIA underwent a minimum of 40 simulation runs to ensure accuracy, with average results calculated across these runs for reliability. Figure 34 illustrates the impact of a 20% intensity FDIA on the actual load profile and PV power output. Figure 35 illustrates the resultant SOCs of the BESSs and how the total load is served by the PV, utility grid, generator, and battery using the hybrid EMS approach of 24-hour microgrid operation under 20% FDIA type 1.

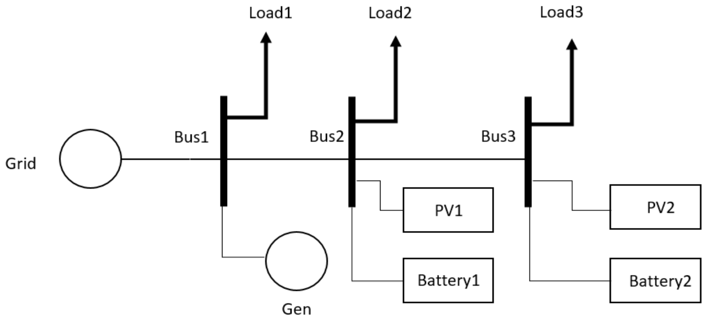


Figure 32. Microgrid Topology

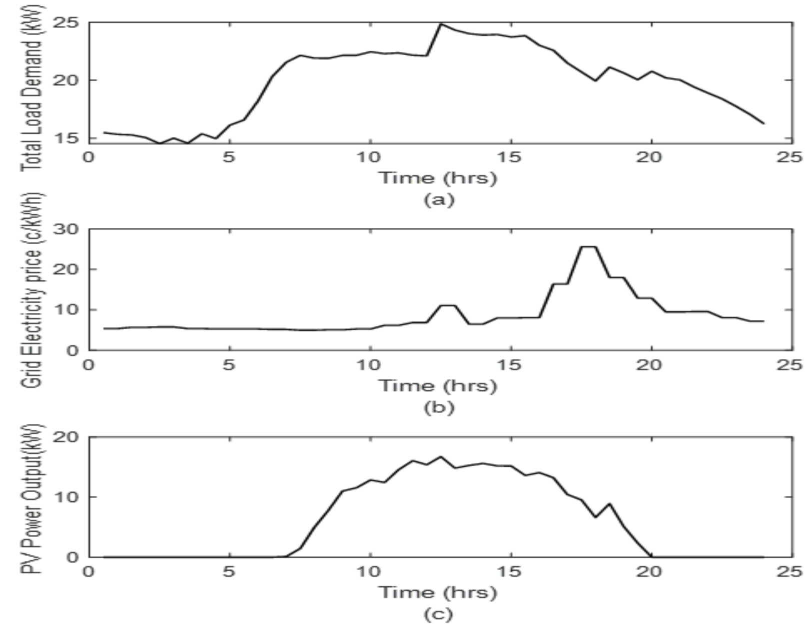


Figure 33. (a) Actual load profile, (b)Grid electricity price, (c) PV power output during a day

In our simulation setup, the FDIA begins at 5:00 am and ends at 8:00 pm. Additionally, the microgrid operates in islanded mode from 2:00 pm to 6:00 pm. The convergence of these events heightens the microgrid's vulnerability to FDIA. The microgrid primarily operates using the optimization-based EMS, except for 2:00 pm to 6:00 pm when it switches to the adaptive control mode for the hybrid EMS method. In each scenario, we have compared the results obtained using both methods. For the optimization-based EMS, as the FDIA intensity increases from 0% to 30%, the total cost for electricity per day generally increases. In Figure 36 and Table XXI, we can observe that at 0% FDIA intensity, the total cost is 2840.02 c/day. However, at 30% FDIA intensity with type 1 attack, it rises to 5138.21 c/day, indicating an 81% increase. Similarly, at 30% FDIA intensity with type 2 attack, it increases to 4324.38 c/day, representing a 52% increase. Load shedding occurs when the FDIA intensity is 10% or higher, and the FDIA time coincides with the islanded mode operation of the microgrid, resulting in an increase in the total cost considering penalties for load shedding. At 0% FDIA intensity, there is no load shedding, while at 30% FDIA intensity with type 1 attack, it rises to 2.22%, and at 30% FDIA intensity with type 2 attack, it rises to 1.51%.

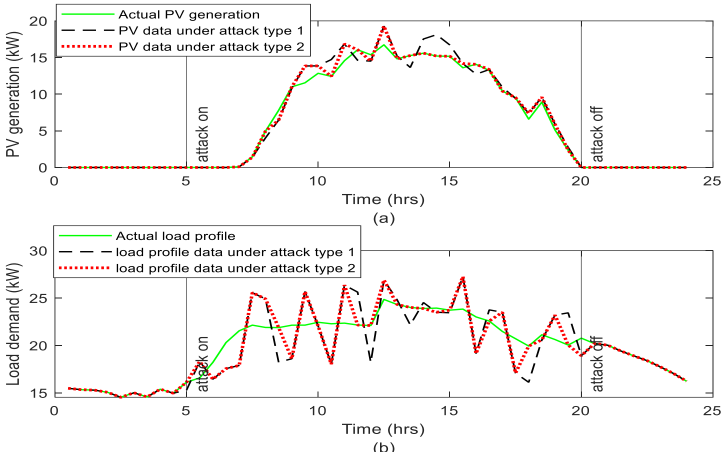


Figure 34.(a) PV generation data under 20% FDIA, (b) Load profile data under 20% FDIA

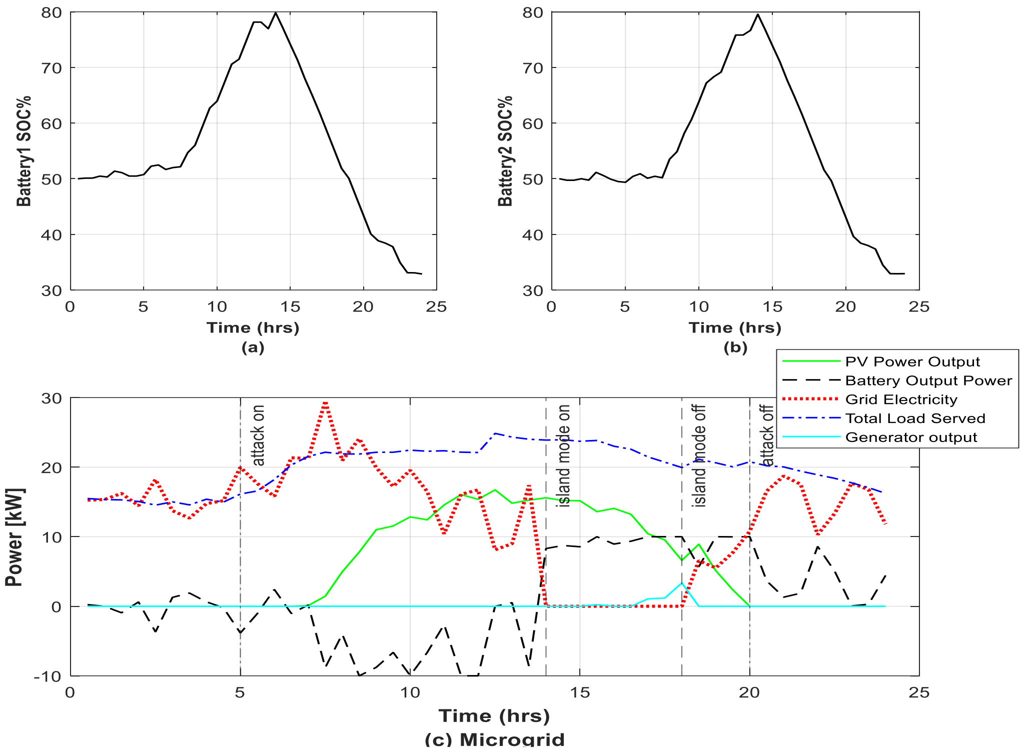
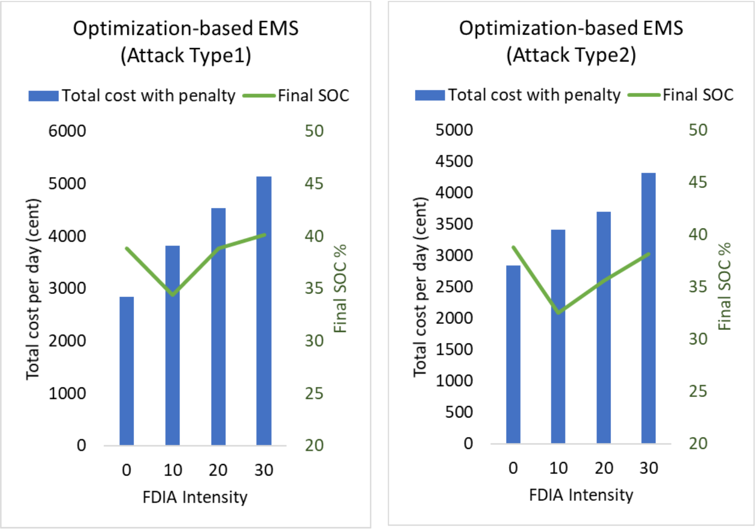


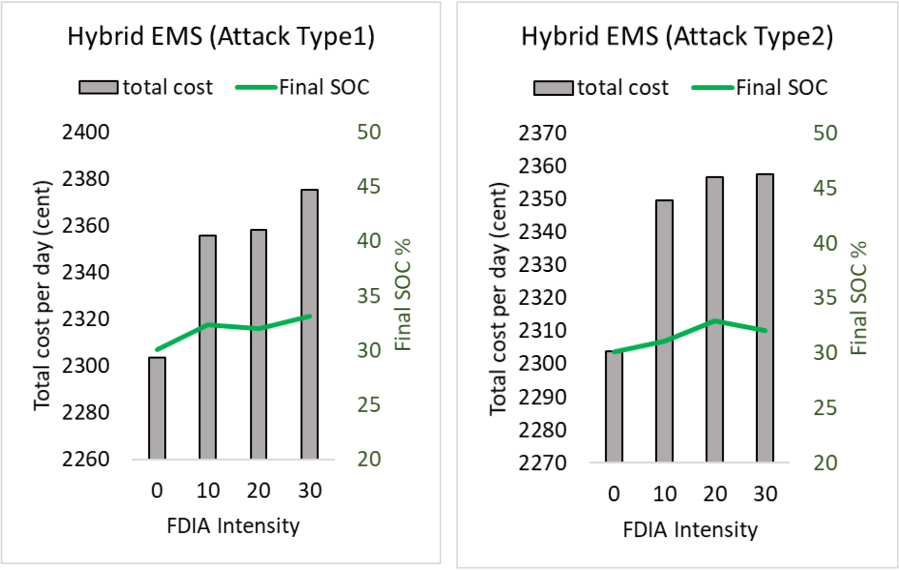
Figure 35. (a) SOC of BESS1, (b) SOC of BESS2, (c) Power profiles of PV generation, battery output, grid electricity, generator output and total load over time using hybrid EMS method under FDIA type 1

Similar to the optimization-based EMS, in the hybrid approach, increasing FDIA intensity leads to a rise in the total cost for electricity per day. In Figure 37 and Table XXI, we observe that at 0% FDIA intensity, the total cost is 2303.74 c/day. However, at 30% FDIA intensity with type 1 attack, it rises to 2375.28 c/day, indicating a 3.1% increase. Similarly, at 30% FDIA intensity with type 2 attack, it rises to 2357.5 c/day, representing a 2.33% increase. There is no load-generation mismatch across all FDIA intensities, resulting in no change in the total cost. The BESS SOC varies marginally across different FDIA intensities, with no significant trends observed. From Table XXI, it is evident that the hybrid EMS generally exhibits lower total costs compared to the optimization-based EMS across various FDIA intensities, as there are no generation-load mismatches for the hybrid EMS, resulting in no additional penalty cost. On the other hand, the optimization-based EMS approach results in a higher final SOC of the BESS systems at the end of the day compared to the hybrid approach, which is desirable for the next day's operation as this approach optimizes microgrid operation considering 24-hour horizon data. However, the optimization- based EMS is more sensitive to FDIA than the hybrid EMS approach, particularly when the attack time coincides with the islanded mode operation of the microgrid. As for attack model, FDIA type 1 tends to result in more frequent load shedding and higher costs compared to type 2. When the FDIA occurrence did not align with the islanded mode operation, the optimization-based EMS exhibited no generation-load mismatch.



(a) (b)

Figure 36. Total electricity cost and final SOC with increasing intensity of FDIA type 1(a) & type 2(b) in 24-hour microgrid operation for optimization-based EMS



(a) (b)

Figure 37. Total electricity cost and final SOC with increasing intensity of FDIA type 1(a) & type 2(b) in 24-hour microgrid operation for hybrid EMS

Table XXI. Summary of Microgrid Operation Under Various FDIA Scenarios

Microgrid Operation Method	FDIA time	FDIA intensity (%)	FDIA type	Islanded mode operation time	Total cost for electricity per day (c/day)	SOC of BESS (%) at the end of the day	Load shedding (%)	Total cost considering penalty for load shedding (c/day)
Optimization based EMS	5:00 am – 8:00pm	0	1/2	2:00pm – 6:00pm	2840.02	38.84	0	2840.02
		10	1		2457.88	34.40	1.18	3810.43
		20			2602.97	38.86	1.69	4542.23
		30			2585.11	40.11	2.22	5138.21
		10	2		2449.58	32.54	0.84	3419.93
		20			2502.83	35.62	1.04	3701.47
		30			2593.74	38.18	1.51	4324.38
Hybrid EMS		0	1/2		2303.74	30.11	0	2303.74
		10	1		2355.55	32.31	0	2355.55
		20			2358.37	32.00	0	2358.37
		30			2375.28	33.12	0	2375.28
		10	2		2349.81	31.11	0	2349.81
		20			2356.84	32.94	0	2356.84
		30			2357.51	32.04	0	2357.51

The successful implementation of our hybrid approach in real-world grid applications hinges on the validation of our model with real-world scenario data. Access to data on FDIAs in microgrid applications is crucial for validating the effectiveness and reliability of our model under actual operating conditions. By leveraging real-world data to validate our model, we can ensure its applicability and robustness in practical grid environments. Additionally, further study is needed to explore other attack models, attack scenarios, and more complex microgrid topologies. Conducting additional research on different types of cyber-attacks and their potential impacts on microgrid operations will enhance our understanding of grid vulnerabilities and resilience. By expanding the scope of our study to encompass a broader range of attack scenarios and microgrid configurations, we can develop more comprehensive and effective solutions to address cyber threats in grid environments. In summary, the validation of our model with real-world data and further study on other attack models and scenarios are essential steps for ensuring the successful implementation of our hybrid approach in real-world grid applications. By addressing these needs, we can enhance the reliability, security, and resilience of microgrid operations in the face of evolving cyber threats.

4.8. Summary

In conclusion, our study dives into the multifaceted challenges posed by data loss and false data injection attacks on microgrid energy management systems, offering insights and strategies to enhance system resilience and performance.

Our analysis emphasizes the significant impacts of data loss on the economic performance and operational costs of microgrids. Timing emerges as a critical factor, with data loss potentially leading to suboptimal control actions during periods of high-priced grid electricity or peak load demands. Moreover, the relationship between data loss and operational costs is nuanced, with even minor instances of data loss during critical time slots resulting in higher costs. These findings underscore the importance of robust optimization techniques and data loss mitigation strategies in microgrid energy management systems. By integrating reliable forecasting techniques and addressing data loss challenges, microgrid operators can bolster the efficiency and resilience of their systems.

Examining the effects of FDIA on microgrid operation, we introduced a hybrid EMS strategy to ensure stability and reliability across diverse scenarios. Our findings reveal potential load balance discrepancies during islanded microgrid operation under FDIA, emphasizing the necessity for adaptive control methods. While the optimization-based EMS exhibited sensitivity to FDIA, the hybrid approach offered promising results, albeit with a trade-off in battery energy storage system, state of charge levels. The successful implementation of our hybrid approach in grid applications requires further infrastructure like FDIA detection model and redundancy in sensor and communication structure. Also, this model requires validation with real-world data and further study to explore additional attack models and scenarios. By addressing these needs, we can ensure the reliability, security, and resilience of microgrid operations in the face of evolving cyber threats. Our study lays the groundwork for future research aimed at incorporating artificial intelligence techniques to detect and resolve attacked data, thus enhancing the resilience of microgrid operation against FDIA and other cyber threats.

5. CONCLUSION AND FUTURE WORK

This dissertation presents a comprehensive analysis of power grid vulnerabilities, focusing on the integration of renewable energy, cascading failures, and microgrid resilience. Through a series of investigations, the research aims to uncover the intricacies of modern power systems and propose effective mitigation strategies to enhance their reliability and security.

The research begins with an exploration of power grid vulnerabilities in the context of increasing renewable energy integration. A full ACPF model with modified OPF for power balance has been used in the simulation process to accurately mimic the most likely evolution path of CF process and to make the study more accurate. Blackout size and number of tripped lines have been used as measuring tools to assess vulnerability to CF. It is found that higher penetration from renewable energy leads to higher number of trip count and larger amount of load shedding. The proposed model has also been able to identify that after a certain level of RE penetration, some system may deteriorate rapidly and preventive measures should be taken if and when RE penetration level exceeds that limit. This initial investigation sets the stage for a deeper exploration into cascading failure risk analysis, which involves statistically analyzing key metrics using historical utility data and simulation data. The severity of a cascading failure process in the power grid can be measured by the number of lines that got tripped during the event, the duration of the whole CF process, and the amount of load needed to be shed to restore the balance of the system. In this study, we have analyzed these different parameters of a cascading failure process using historical utility data and two synthetic test cases. We have considered both uniform and non-uniform probability distribution of initial line trips and compared our results with the results from historical data. It is found that non-uniform distribution of initial line trips gave better estimations on mean outage number and cascade duration. Additionally, by validating our findings with real-world outage data, we have gained valuable insights into the distribution of risk factors, such as the duration and number of outage lines, associated with cascading failure events. This validation process strengthened the credibility and practical relevance of our simulation model.

Shifting focus to microgrid resilience, the research meticulously explores data integrity attacks and proposes mitigation strategies to safeguard microgrid operations. A multi-layered microgrid simulation model with an optimization-based energy management system is developed to investigate the impact of renewable energy penetration and data loss. Additionally, two practical FDIA model have been developed to simulate attack scenarios in microgrid operation and a hybrid approach is proposed to ensure stable microgrid operation in the face of false data injection attacks, integrating optimization-based energy management with adaptive control schemes. Through simulation analyses, we have demonstrated the effectiveness of our strategy in safeguarding microgrid operation, while also paving the way for further enhancement of our initial model through the integration of AI techniques for real-time detection and resolution of FDIAs.

While this dissertation has made significant strides in understanding power grid vulnerabilities, cascading failures, and microgrid resilience, there are numerous avenues for future research and exploration. The field of microgrids, in particular, offers a wealth of opportunities for further investigation and innovation. Below are some potential areas for future research:

1. Enhancing microgrid resilience through the integration of AI techniques for cyber threat detection and mitigation. Real-time analysis of system behavior by AI algorithms can effectively identify anomalies and potential security breaches, bolstering system resilience.

2. Validating research findings and simulation models using real-life microgrid data will provide critical insights into the applicability and robustness of proposed strategies and algorithms in practical scenarios.
3. Exploring the potential benefits and challenges of interconnected microgrid systems to understand how cooperation between grids can enhance overall system resilience and reliability.
4. Assessing the impact of emerging technologies like blockchain and IoT on microgrid operation and cybersecurity to leverage their potential benefits while addressing any associated challenges.
5. Conducting additional simulations across diverse test cases to gain a deeper understanding of threshold levels and system vulnerabilities to cascading failures with increasing RE penetration. This will involve considering the unique characteristics of each power system to ensure accurate vulnerability assessments.
6. Further simulations are required to compare different probability distribution functions accurately for cascading failure risk analysis. Obtaining detailed information about BPA control area load will enhance test case accuracy, while exploring the impact of renewable energy penetration levels on cascading failure risk analysis will contribute to improved grid resilience.

Addressing these areas of future research will enable researchers to advance the field of microgrid technology, vulnerability analysis regarding renewable energy penetration, and cascading failure risk analysis. This will enhance the power grid's capabilities and resilience, allowing it to adapt to evolving challenges and opportunities in the energy landscape.

REFERENCE

[1] Social Development for Sustainable Development | DISD, (n.d.). https://www.un.org/development/desa/dspd/2030agenda-sdgs.html (accessed November 5, 2020).

[2] Cascading failure - Wikipedia, (n.d.). https://en.wikipedia.org/wiki/Cascading_failure (accessed August 12, 2021).

[3] H. Guo, C. Zheng, H.H.C. Iu, T. Fernando, A critical review of cascading failure analysis and modeling of power system, Renewable and Sustainable Energy Reviews 80 (2017) 9–22. https://doi.org/10.1016/J.RSER.2017.05.206.

[4] D.T. Ton, M.A. Smith, The U.S. Department of Energy's Microgrid Initiative, Electricity Journal 25 (2012) 84–94. https://doi.org/10.1016/J.TEJ.2012.09.013.

[5] F. Pasqualetti, F. Dorfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Trans Automat Contr 58 (2013) 2715–2729. https://doi.org/10.1109/TAC.2013.2266831.

[6] Energy management system - Wikipedia, (n.d.). https://en.wikipedia.org/wiki/Energy_management_system (accessed April 13, 2023).

[7] M. Saleh, Y. Esaahmed, A. Mohamed, H. Grebel, R. Rojas-Cessa, Energy management algorithm for resilient controlled delivery grids – IEEE Conference Publication, Publications and Research 2017-January (2017) 1–8. https://doi.org/10.1109/IAS.2017.8101777.

[8] W. Su, J. Wang, Energy Management Systems in Microgrid Operations, The Electricity Journal 25 (2012) 45–60. https://doi.org/10.1016/J.TEJ.2012.09.010.

[9] Y. Mo, T.H.J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure, Proceedings of the IEEE 100 (2012) 195–209. https://doi.org/10.1109/JPROC.2011.2161428.

[10] H. Guo, C. Zheng, H.H.C. Iu, T. Fernando, A critical review of cascading failure analysis and modeling of power system, Renewable and Sustainable Energy Reviews 80 (2017) 9–22. https://doi.org/10.1016/J.RSER.2017.05.206.

[11] I. Dobson, B.A. Carreras, D.E. Newman, A branching process approximation to cascading load-dependent system failure, Proceedings of the Hawaii International Conference on System Sciences 37 (2004) 915–924. https://doi.org/10.1109/HICSS.2004.1265185.

[12] K. Sun, Complex networks theory: A new method of research in power grid, Proceedings of the IEEE Power Engineering Society Transmission and Distribution Conference 2005 (2005) 1–6. https://doi.org/10.1109/TDC.2005.1547099.

[13] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys Rev E 66 (2002) 065102. https://doi.org/10.1103/PhysRevE.66.065102.

[14] P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Attack vulnerability of complex networks, Phys Rev E 65 (2002) 056109. https://doi.org/10.1103/PhysRevE.65.056109.

[15] E. Cotilla-Sanchez, P.D.H. Hines, C. Barrows, S. Blumsack, Comparing the topological and electrical structure of the North American electric power infrastructure, IEEE Syst J 6 (2012) 616–626. https://doi.org/10.1109/JSYST.2012.2183033.

[16] H.P. Ren, J. Song, R. Yang, M.S. Baptista, C. Grebogi, Cascade failure analysis of power grid using new load distribution law and node removal rule, Physica A: Statistical Mechanics and Its Applications 442 (2016) 239–251. https://doi.org/10.1016/J.PHYSA.2015.08.039.

[17] L.R. Ford, D.R. Fulkerson, Maximal Flow Through a Network, Canadian Journal of Mathematics 8 (1956) 399–404. https://doi.org/10.4153/CJM-1956-045-5.

[18] A. Dwivedi, X. Yu, A maximum-flow-based complex network approach for power system vulnerability analysis, IEEE Trans Industr Inform 9 (2013) 81–88. https://doi.org/10.1109/TII.2011.2173944.

[19] J. Fang, C. Su, Z. Chen, H. Sun, P. Lund, Power system structural vulnerability assessment based on an improved maximum flow approach, IEEE Trans Smart Grid 9 (2018) 777–785. https://doi.org/10.1109/TSG.2016.2565619.

[20] W. Fan, S. Huang, S. Mei, Invulnerability of power grids based on maximum flow theory, Physica A: Statistical Mechanics and Its Applications 462 (2016) 977–985. https://doi.org/10.1016/J.PHYSA.2016.06.109.

[21] D.A. Av, V. Vi, I. Id, E. Ne, E. Ew, W. Wm, M. Ma A An N N, A LOADING-DEPENDENT MODEL OF PROBABILISTIC CASCADING FAILURE, Probab Eng Inf Sci 19 (2005) 15–32. https://doi.org/10.1017/S0269964805050023.

[22] I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization, Chaos 17 (2007). https://doi.org/10.1063/1.2737822/934765.

[23] I. Dobson, Estimating the propagation and extent of cascading line outages from utility data with a branching process, IEEE Transactions on Power Systems 27 (2012) 2146–2155. https://doi.org/10.1109/TPWRS.2012.2190112.

[24] I. Dobson, J. Kim, K.R. Wierzbicki, Testing Branching Process Estimators of Cascading Failure with Data from a Simulation of Transmission Line Outages, Risk Analysis 30 (2010) 650–662. https://doi.org/10.1111/J.1539-6924.2010.01369.X.

[25] J. Qi, W. Ju, K. Sun, Estimating the Propagation of Interdependent Cascading Outages with Multi-Type Branching Processes, IEEE Transactions on Power Systems 32 (2017) 1212–1223. https://doi.org/10.1109/TPWRS.2016.2577633.

[26] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, P. Zhang, Risk assessment of cascading outages: Methodologies and challenges, IEEE Transactions on Power Systems 27 (2012) 631–641. https://doi.org/10.1109/TPWRS.2011.2177868.

[27] J. Song, E. Cotilla-Sanchez, G. Ghanavati, P.D.H. Hines, Dynamic modeling of cascading failure in power systems, IEEE Transactions on Power Systems 31 (2016) 2085–2095. https://doi.org/10.1109/TPWRS.2015.2439237.

[28] M.H. Athari, Z. Wang, Impacts of wind power uncertainty on grid vulnerability to cascading overload failures, IEEE Trans Sustain Energy 9 (2018) 128–137. https://doi.org/10.1109/TSTE.2017.2718518.

[29] M.H. Athari, Z. Wang, Studying cascading overload failures under high penetration of wind generation, in: IEEE Power and Energy Society General Meeting, IEEE Computer Society, 2018: pp. 1–5. https://doi.org/10.1109/PESGM.2017.8274358.

[30] H. Cetinay, S. Soltan, F.A. Kuipers, G. Zussman, P. Van Mieghem, Analyzing cascading failures in power grids under the AC and DC power flow models, Performance Evaluation Review 45 (2018) 198–203. https://doi.org/10.1145/3199524.3199559.

[31] W. Ju, K. Sun, R. Yao, Simulation of cascading outages using a power-flow model considering frequency, IEEE Access 6 (2018) 37784–37795. https://doi.org/10.1109/ACCESS.2018.2851022.

[32] M.H. Athari, Z. Wang, Stochastic cascading failure model with uncertain generation using unscented transform, IEEE Trans Sustain Energy 11 (2020) 1067–1077. https://doi.org/10.1109/TSTE.2019.2917842.

[33] D. Liu, X. Zhang, C.K. Tse, Effects of High Level of Penetration of Renewable Energy Sources on Cascading Failure of Modern Power Systems, IEEE J Emerg Sel Top Circuits Syst 12 (2022) 98–106. https://doi.org/10.1109/JETCAS.2022.3147487.

[34] M. Adnan, M.G. Khan, A.A. Amin, M.R. Fazal, W.S. Tan, M. Ali, Cascading Failures Assessment in Renewable Integrated Power Grids under Multiple Faults Contingencies, IEEE Access 9 (2021) 82272–82287. https://doi.org/10.1109/ACCESS.2021.3087195.

[35] S. Yang, W. Chen, X. Zhang, W. Yang, A Graph-based Method for Vulnerability Analysis of Renewable Energy integrated Power Systems to Cascading Failures, Reliab Eng Syst Saf 207 (2021) 107354. https://doi.org/10.1016/J.RESS.2020.107354.

[36] I. Dobson, D.E. Newman, B.A. Carreras, V.E. Lynch, An initial complex systems analysis of the risks of blackouts in power transmission systems, Power System and Communications Infrastructures for Future (2002) 1–7.

[37] I. Dobson, B.A. Carreras, D.E. Newman, J.M. Reynolds-Barredo, Obtaining Statistics of Cascading Line Outages Spreading in an Electric Transmission Network from Standard Utility Data, IEEE Transactions on Power Systems 31 (2016) 4831–4841. https://doi.org/10.1109/TPWRS.2016.2523884.

[38] S. Soltan, D. Mazauric, G. Zussman, Cascading Failures in Power Grids-Analysis and Algorithms, 14 (n.d.). https://doi.org/10.1145/2602044.2602066.

[39] S. Das, Z. Wang, Power grid vulnerability analysis with rising renewables infiltration, IMCIC 2021 - 12th International Multi-Conference on Complexity, Informatics and Cybernetics, Proceedings 2 (2021) 157–162.

[40] S. Das, Z. Wang, Estimating Distribution of Cascaded Outages Using Observed Utility Data and Simulation Modeling, 2021 North American Power Symposium, NAPS 2021 (2021) 5–10. https://doi.org/10.1109/NAPS52732.2021.9654745.

[41] M.F. Zia, E. Elbouchikhi, M. Benbouzid, Microgrids energy management systems: A critical review on methods, solutions, and prospects, Appl Energy 222 (2018) 1033–1055. https://doi.org/10.1016/J.APENERGY.2018.04.103.

[42] R. Palma-Behnke, C. Benavides, E. Aranda, J. Llanos, D. Sáez, Energy management system for a renewable based microgrid with a demand side management mechanism, IEEE SSCI 2011 - Symposium Series on Computational Intelligence - CIASG 2011: 2011 IEEE Symposium on Computational Intelligence Applications in Smart Grid (2011) 131–138. https://doi.org/10.1109/CIASG.2011.5953338.

[43] R. Palma-Behnke, C. Benavides, F. Lanas, B. Severino, L. Reyes, J. Llanos, D. Saez, A microgrid energy management system based on the rolling horizon strategy, IEEE Trans Smart Grid 4 (2013) 996–1006. https://doi.org/10.1109/TSG.2012.2231440.

[44] J.B. Almada, R.P.S. Leão, R.F. Sampaio, G.C. Barroso, A centralized and heuristic approach for energy management of an AC microgrid, Renewable and Sustainable Energy Reviews 60 (2016) 1396–1404. https://doi.org/10.1016/J.RSER.2016.03.002.

[45] C. Wang, T. Zhang, F. Luo, F. Li, Y. Liu, Impacts of Cyber System on Microgrid Operational Reliability, IEEE Trans Smart Grid 10 (2019) 105–115. https://doi.org/10.1109/TSG.2017.2732484.

[46] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, K. Butler-Purry, Towards modelling the impact of cyber attacks on a smart grid, Int. J. Security and Networks (2011).

[47] S. Suprabhath Koduru, V.S.P. Machina, S. Madichetty, Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review, Energies 2023, Vol. 16, Page 4573 16 (2023) 4573. https://doi.org/10.3390/EN16124573.

[48] P.S. Tadepalli, D. Pullaguram, Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies, IEEE Trans Signal Inf Process Netw 8 (2022) 1008–1023. https://doi.org/10.1109/TSIPN.2022.3230562.

[49] S.N. Islam, M.A. Mahmud, A.M.T. Oo, Impact of optimal false data injection attacks on local energy trading in a residential microgrid, ICT Express 4 (2018) 30–34. https://doi.org/10.1016/J.ICTE.2018.01.015.

[50] X.K. Liu, C. Wen, Q. Xu, Y.W. Wang, Resilient Control and Analysis for DC Microgrid System under DoS and Impulsive FDI Attacks, IEEE Trans Smart Grid 12 (2021) 3742–3754. https://doi.org/10.1109/TSG.2021.3072218.

[51] X. Lin, D. An, F. Cui, F. Zhang, False data injection attack in smart grid: Attack model and reinforcement learning-based detection method, Front Energy Res 10 (2023) 1104989. https://doi.org/10.3389/FENRG.2022.1104989/BIBTEX.

[52] H. Zhang, W. Meng, J. Qi, S. Member, X. Wang, W. Xing Zheng, W.H. Xing Zheng Zhang, W. Meng, X. Wang, W.X. Zheng, Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS 66 (2019) 1543. https://doi.org/10.1109/TIE.2018.2793241.

[53] M.M. Rana, L. Li, S.W. Su, Cyber attack protection and control of microgrids, IEEE/CAA Journal of Automatica Sinica 5 (2018) 602–609. https://doi.org/10.1109/JAS.2017.7510655.

[54] A. Mustafa, B. Poudel, A. Bidram, H. Modares, Detection and Mitigation of Data Manipulation Attacks in AC Microgrids, IEEE Trans Smart Grid 11 (2020) 2588–2603. https://doi.org/10.1109/TSG.2019.2958014.

[55] S. Das, Z. Wang, Optimizing Microgrid Energy Management Systems with Variable Renewable Energy Penetration: Analysis of Data Loss Effects, Lecture Notes in Networks and Systems 814 LNNS (2023) 357–374. https://doi.org/10.1007/978-3-031-47451-4_26/TABLES/2.

[56] Y. Wang, C. Deng, Y. Liu, Z. Wei, A cyber-resilient control approach for islanded microgrids under hybrid attacks, International Journal of Electrical Power & Energy Systems 147 (2023) 108889. https://doi.org/10.1016/J.IJEPES.2022.108889.

[57] K. Mets, J.A. Ojea, C. Develder, Combining power and communication network simulation for cost-effective smart grid analysis, IEEE Communications Surveys and Tutorials 16 (2014) 1771–1796. https://doi.org/10.1109/SURV.2014.021414.00116.

[58] P.T. Mana, K.P. Schneider, W. Du, M. Mukherjee, T. Hardy, F.K. Tuffner, Study of Microgrid Resilience through Co-Simulation of Power System Dynamics and Communication Systems, IEEE Trans Industr Inform 17 (2021) 1905–1915. https://doi.org/10.1109/TII.2020.2989107.

[59] R. Mao, H. Li, Y. Xu, H. Li, Wireless communication for controlling microgrids: Co-simulation and performance evaluation, in: IEEE Power and Energy Society General Meeting, 2013. https://doi.org/10.1109/PESMG.2013.6673056.

[60] D. Niyato, P. Wang, Z. Han, E. Hossain, Impact of packet loss on power demand estimation and power supply cost in smart grid, in: 2011 IEEE Wireless Communications and Networking Conference, WCNC 2011, 2011: pp. 2024–2029. https://doi.org/10.1109/WCNC.2011.5779440.

[61] S. Das, Z. Wang, Power Grid Vulnerability Analysis with Rising Renewables Infiltration, J Syst Cybern Inf 19 (2021) 23–32. http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA338SI21 (accessed September 20, 2021).

[62] M.H. Athari, Z. Wang, Modeling the uncertainties in renewable generation and smart grid loads for the study of the grid vulnerability, in: 2016 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2016, Institute of Electrical and Electronics Engineers Inc., 2016. https://doi.org/10.1109/ISGT.2016.7781265.

[63] S.J. Huang, K.R. Shih, Short-term load forecasting via ARMA model identification including non-Gaussian process considerations, IEEE Transactions on Power Systems 18 (2003) 673–679. https://doi.org/10.1109/TPWRS.2003.811010.

[64] S.J. Julier, J.K. Uhlmann, Unscented Filtering and Nonlinear Estimation, (2004). https://doi.org/10.1109/JPROC.2003.823141.

[65] M. Aien, M. Fotuhi-Firuzabad, F. Aminifar, Probabilistic load flow in correlated uncertain environment using unscented transformation, IEEE Transactions on Power Systems 27 (2012) 2233–2241. https://doi.org/10.1109/TPWRS.2012.2191804.

[66] Z. Wang, A. Scaglione, R.J. Thomas, A Markov-transition model for cascading failures in power grids, in: Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE Computer Society, 2012: pp. 2115–2124. https://doi.org/10.1109/HICSS.2012.63.

[67] ISBN 9780979142703 - Overhead Conductor Manual 2nd Edition Direct Textbook, (n.d.). https://www.directtextbook.com/isbn/9780979142703 (accessed November 22, 2020).

[68] Description of case118, (n.d.). https://matpower.org/docs/ref/matpower5.0/case118.html#_top (accessed November 21, 2020).

[69] IEEE 300-Bus System, (n.d.). https://electricgrids.engr.tamu.edu/electric-grid-test-cases/ieee-300-bus-system/ (accessed December 29, 2020).

[70] SouthCarolina 500-Bus System: ACTIVSg500, (n.d.). https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg500/ (accessed May 11, 2021).

[71] S. Das, Z. Wang, Cascading Failure Risk Analysis of Electrical Power Grid, Lecture Notes in Networks and Systems 559 LNNS (2023) 906–923. https://doi.org/10.1007/978-3-031-18461-1_60/TABLES/12.

[72] BPA.gov - Bonneville Power Administration - Bonneville Power Administration, (n.d.). https://www.bpa.gov/ (accessed April 24, 2022).

[73] S. Das, Z. Wang, Study of Cascading Failure Duration in Power Grid using Historical Outage Data and Simulation Model, 2022 IEEE Conference on Technologies for Sustainability, SusTech 2022 (2022) 114–119. https://doi.org/10.1109/SUSTECH53338.2022.9794272.

[74] A.B. Birchfield, T. Xu, K.M. Gegner, K.S. Shetye, T.J. Overbye, Grid Structural Characteristics as Validation Criteria for Synthetic Networks, IEEE Transactions on Power Systems 32 (2017) 3258–3265. https://doi.org/10.1109/TPWRS.2016.2616385.

[75] H. Sadeghian, Z. Wang, AutoSynGrid: A MATLAB-based toolkit for automatic generation of synthetic power grids, International Journal of Electrical Power and Energy Systems 118 (2020). https://doi.org/10.1016/j.ijepes.2019.105757.

[76] S. Diego, Office of Electricity Delivery and Energy Reliability Smart Grid R&D Program DOE Microgrid Workshop Report, (n.d.).

[77] A.C. Zambroni de Souza, M. Castilla, Microgrids design and implementation, Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-98687-6.

[78] H. Farhangi, Smart microgrids : lessons from campus microgrid design and implementation, CRC Press, 2017.

[79] M.S. Saleh, A. Althaibani, Y. Esa, Y. Mhandi, A.A. Mohamed, Impact of clustering microgrids on their stability and resilience during blackouts, International Conference on Smart Grid and Clean Energy Technologies (2015) 195–200. https://doi.org/10.1109/ICSGCE.2015.7454295.

[80] Y. Shen, Y. Peng, Z. Shuai, Q. Zhou, L. Zhu, Z.J. Shen, M. Shahidehpour, Hierarchical Time-Series Assessment and Control for Transient Stability Enhancement in Islanded Microgrids, IEEE Trans Smart Grid 14 (2023) 3362–3374. https://doi.org/10.1109/TSG.2023.3237965.

[81] S.L.L. Wynn, T. Boonraksa, B. Marungsri, Optimal Generation Scheduling with Demand Side Management for Microgrid Operation, International Electrical Engineering Congress (2021) 41–44. https://doi.org/10.1109/IEECON51072.2021.9440356.

[82] B. Hartmann, I. Táczi, A. Talamon, I. Vokony, Island mode operation in intelligent microgrid—Extensive analysis of a case study, International Transactions on Electrical Energy Systems 31 (2021). https://doi.org/10.1002/2050-7038.12950.

[83] Liege Microgrid Open Data | Kaggle, (n.d.). https://www.kaggle.com/datasets/jonathandumas/liege-microgrid-open-data (accessed April 10, 2023).

[84] K.H. LaCommare, J.H. Eto, L.N. Dunn, M.D. Sohn, Improving the estimated cost of sustained power interruptions to electricity customers, Energy 153 (2018) 1038–1047. https://doi.org/10.1016/J.ENERGY.2018.04.082.

[85] P.J. Balducci, J.M. Roop, L.A. Schienbein, J.G. DeSteese, M.R. Weimar, Electric Power Interruption Cost Estimates for Individual Industries, Sectors, and U.S. Economy, (2002). https://doi.org/10.2172/926127.

[86] A Framework and Review of Customer Outage Costs: Integration and Analysis of Electric Utility Outage Cost Surveys | Energy Markets & Policy, (n.d.). https://emp.lbl.gov/publications/framework-and-review-customer-outage (accessed February 28, 2024).

LIST OF PUBLICATIONS

[1] S. Das and Z. Wang, “Power Grid Vulnerability Analysis with Rising Renewables Infiltration,” J. Syst. Cybern. Informatics, vol. 19, no. 3, pp. 23–32, 2021.” DOAJ, Jun. 2021, [Online]. Available: https://doaj.org/article/5244fe4ff3524297b3b9ec2caedd54c6

[2] S. Das and Z. Wang, "Estimating Distribution of Cascaded Outages Using Observed Utility Data and Simulation Modeling," 2021 North American Power Symposium (NAPS), College Station, TX, USA, 2021, pp. 1-6, doi: 10.1109/NAPS52732.2021.9654745.

[3] S. Das and Z. Wang, "Study of Cascading Failure Duration in Power Grid using Historical Outage Data and Simulation Model," 2022 IEEE Conference on Technologies for Sustainability (SusTech), Corona, CA, USA, 2022, pp. 114-119, doi: 10.1109/SusTech53338.2022.9794272.

[4] Das, S., Wang, Z. (2023). Cascading Failure Risk Analysis of Electrical Power Grid. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2022, Volume 1. FTC 2022 2022. Lecture Notes in Networks and Systems, vol 559. Springer, Cham. https://doi.org/10.1007/978-3-031-18461-1_60

[5] Das, S., Wang, Z. (2023). Optimizing Microgrid Energy Management Systems with Variable Renewable Energy Penetration: Analysis of Data Loss Effects. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2023, Volume 2. FTC 2023. Lecture Notes in Networks and Systems, vol 814. Springer, Cham. https://doi.org/10.1007/978-3-031-47451-4_26

[6] S. Das and Z. Wang, "Enhancing Microgrid Resilience to False Data Injection," 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oslo, Norway, 2024 [Under review].

VITA

SAIKAT DAS

✉ dass10@vcu.edu 📍 Richmond, Virginia
Virginia Commonwealth University, ECE Department

Education

Virginia Commonwealth University, Richmond, VA, USA Fall 2019 - Present
PhD Candidate, Electrical Engineering
Research area: Renewable Energy Integration, Microgrid resilience
Advisor: Dr. Zhifang Wang
GPA: 4.0/4.0

Bangladesh University of Engineering and Technology (BUET), 2012-2017
Dhaka, Bangladesh
B.Sc. in Electrical and Electronic Engineering
Thesis: Transmission Line Reliability Evaluation
Advisor: Dr. Abdul Hasib Chowdhury
GPA**:** 3.52/4

Professional Experience

Graduate Assistant, Virginia Commonwealth University, Richmond, VA Aug 2019 - Present

Graduate Intern, Electric Transmission Systems Operations Engineering, Dominion Energy, Magnolia, Richmond, VA (Manager: Scott P. Adams) May 2023 -Aug 2023

- Developed a historical n-1 contingency analysis database for data driven insights and decision-making using python, Microsoft access and power bi.

Graduate Intern, Electric Transmission Planning, Dominion Energy, Glen Allen, VA (Manager: Francisco G. Velez-Cedeno) Jun 2022 – Aug 2022

- Develop and improve a component based dynamic load model for transmission planning studies incorporating updated datasets, CMLD version, MMWG cases using PSS/E and python.

Senior Officer, Infrastructure Development Company Limited (IDCOL), Renewable Energy Department, Dhaka, Bangladesh Nov 2018- Jul 2019

Junior Officer, Infrastructure Development Company Limited (IDCOL), Renewable Energy Department, Dhaka, Bangladesh Sep 2017- Nov 2018

Academic Projects

- Power Grid Vulnerability Analysis to Cascading Failure with Uncertain Renewable Generation
- Cascading Failure Risk Analysis with Real World Outage Data and Simulation Model
- Microgrid Resilience

Research Interest

- Power System Vulnerability Analysis
- Modeling and Integration of Distributed Renewable Energy
- Power System Reliability Evaluation
- Power system modeling and optimization
- Application of intelligent methods in power system
- Electricity market and economy

Relevant Course work

- Power System Analysis
- Sustainable and Efficient Power System
- Applied Data Analysis
- Knowledge Discovery and Data Mining
- Power Electronics
- Power System Operation and Control
- Machine Learning Algorithms
- Power System Protection

Publications

- S. Das and Z. Wang, “Power Grid Vulnerability Analysis with Rising Renewables Infiltration,” J. Syst. Cybern. Informatics, vol. 19, no. 3, pp. 23–32, 2021.” DOAJ, Jun. 2021.
- S. Das and Z. Wang, "Estimating Distribution of Cascaded Outages Using Observed Utility Data and Simulation Modeling," 2021 North American Power Symposium (NAPS), College Station, TX, USA, 2021, pp. 1-6.
- S. Das and Z. Wang, "Study of Cascading Failure Duration in Power Grid using Historical Outage Data and Simulation Model," 2022 IEEE Conference on Technologies for Sustainability (SusTech), Corona, CA, USA, 2022, pp. 114-119.
- Das, S., Wang, Z. (2023). Cascading Failure Risk Analysis of Electrical Power Grid. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2022, Volume 1. FTC 2022 2022. Lecture Notes in Networks and Systems, vol 559. Springer, Cham.
- Das, S., Wang, Z. (2023). Optimizing Microgrid Energy Management Systems with Variable Renewable Energy Penetration: Analysis of Data Loss Effects. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2023, Volume 2. FTC 2023. Lecture Notes in Networks and Systems, vol 814. Springer, Cham.
- S. Das and Z. Wang, "Enhancing Microgrid Resilience to False Data Injection," 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oslo, Norway, 2024 [Under review].

Awards

- VCU 2021 ECE Outstanding Graduate Teaching Assistant, Sep. 2021

Skills

- *Programming Language & Software:* MATLAB, PSS/E, Python, R, C/C++, Power bi
- *Data analysis and Machine learning*