2018

Cyber-Based Contingency Analysis and Insurance Implications of Power Grid

Zhiyuan Yang
Michigan Technological University, yzhiyuan@mtu.edu

CYBER-BASED CONTINGENCY ANALYSIS AND INSURANCE IMPLICATIONS OF POWER GRID

By

Zhiyuan Yang

A DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

In Electrical Engineering

MICHIGAN TECHNOLOGICAL UNIVERSITY

2018

This dissertation has been approved in partial fulfillment of the requirements for the Degree of DOCTOR OF PHILOSOPHY in Electrical Engineering.

Department of Electrical and Computer Engineering

Dissertation Advisor:	*Dr. Chee-Wooi Ten*
Committee Member:	*Dr. Soummya Kar*
Committee Member:	*Dr. Laura E. Brown*
Committee Member:	*Dr. Yeonwoo Rho*
Department Chair:	*Dr. Daniel R. Fuhrmann*

Dedication

To my parents —

Jingshun Yang and Jing Zhang

I love you all dearly :-)

Contents

List of Figures

List of Tables

Acknowledgments

First and foremost I would like to submit my heartiest gratitude to my principal advisor professor Chee-Wooi Ten. He has guided me to keep diligent and disciplined for my research and encourage me to move forward in hardship. His enthusiasm for academic research has greatly affected me and, unconsciously, has taught me what makes a good researcher. I very much appreciate all his contributions of time, efforts, and funding to finish my Ph.D. degree. I am thankful for this great experience working with him. His advice on both my research and career are invaluable and would be sincerely appreciated.

I would also like to express my cordial gratitude to my other committee members, professor Laura E. Brown, professor Soummya Kar, and professor Yeonwoo Rho for generously offering their time, guidance, and brilliant comments on this work.

Some faculty members in Michigan Tech have contributed immensely to both my personal and professional growth. I would acknowledge professor Sumit Paudyal, who offered me my first lecture at Michigan Tech and gave me a great start on my Ph.D. career. I would also like to thank professor Donald L. Kreher for clarifying my doubts and providing me with textbooks and critical references on my preparation of research proposal. Furthermore, I am grateful to professor Zhuo Feng for introducing

me the algebraic methods to broaden my knowledge by connecting the graph theory and algebraic matrix. I would like to thank professor Bruce A. Mork as well, for offering professional courses which have significantly consolidated my understanding of the power system. Also, I am grateful to professor Yeonwoo Rho, who is very generous to extend her support, for providing intensive and detailed discussions on the insurance premium framework in the thesis.

This work would not be successfully completed without the help I received from my co-workers. I deeply acknowledge their time and efforts on the completion of papers. Their contributions to my dissertation are greatly appreciated. I would also like to thank my friends, who share me with both enjoyable and frustrating moments. Their concerns always cheer me up.

Last but not the least, I would extend my special thanks to my parents—words could never express my gratitude—this humble work is just a sign of my love for them, Jingshun Yang and Jing Zhang.

Abstract

Cybersecurity for power communication infrastructure is a serious subject that has been discussed for a decade since the first North American Electric Reliability Corporation (NERC) critical infrastructure protection (CIP) initiative in 2006. Its credibility on plausibility has been evidenced by attack events in the recent past. Although this is a "very high impact, rare probability" event, the establishment of quantitative measures would help asset owners in making a series of investment decisions.

First, this dissertation tackles attackers' strategies based on the current communication architecture between remote IP-based (unmanned) power substations and energy control centers. Hypothetically, the identification of intrusion paths will lead to the worst-case scenarios that the attackers could do harm to the grid, e.g., how this switching attack may perturb to future cascading outages within a control area when an IP-based substation is compromised. Systematic approaches are proposed in this dissertation on how to systematically determine pivotal substations and how investment can be prioritized to maintain and appropriate a reasonable investment in protecting their existing cyberinfrastructure.

More specifically, the second essay of this dissertation focuses on digital protecting relaying, which could have similar detrimental effects on the overall grid's stability.

The $\hat{R}-k$ contingency analyses are proposed to verify with steady-state and dynamic simulations to ensure consistencies of simulation outcome in the proposed modeling in a power system. This is under the assumption that attackers are able to enumerate all electronic devices and computers within a compromised substation network. The essay also assists stakeholders (the defenders) in planning out exhaustively to identify the critical digital relays to be deployed in substations. The systematic methods are the combinatorial evaluation to incorporate the simulated statistics in the proposed metrics that are used based on the physics and simulation studies using existing power system tools.

Finally, a risk transfer mechanism of cyber insurance against disruptive switching attacks is studied comprehensively based on the aforementioned two attackers' tactics. The evaluation hypothetically assesses the occurrence of anomalies and how these footprints of attackers can lead to a potential cascading blackout as well as to restore the power back to normal stage. The research proposes a framework of cyber insurance premium calculation based on the ruin probability theory, by modeling potential electronic intrusion and its direct impacts. This preliminary actuarial model can further improve the security of the protective parameters of the critical infrastructure via incentivizing investment in security technologies.

Chapter 1

Introduction

Stratagems of attackers have gradually advanced with highly sophisticated domain knowledge. The evolution of intelligent attack agents in cyberspace is evident by the public disclosure of recent events [2, 3, 4]. There was estimated statistically more than 160 break-ins reported by U.S. Department of Energy (DOE) between years of 2010 and 2014 [5]. Among them, 10 of them are discovered in the operational environment. National Nuclear Security Administration, a quasi-autonomous agency within DOE, reported 19 successful cyber-based infiltrations over those 4 years [5]. The rise of cyber threats in the near horizon has become the critical issues in system planning [6]. It was reported that the "WannaCry" attack is probably the worst ransomware thus far, which affected over 200,000 people across over 150 countries and cost 1.5

billion dollars lost in the year of 2016 [7]. On December 24, 2015, the first-ever cyber-attack on the Ukraine power grid caused 225,000 people to lose power for more than 6 hours [8, 9, 10]. Although the cyberattack shows the credibility of security threats, the forensic team continues to investigate by piecing evidence together for a study of event reconstruction with potential mitigation strategies [11]. Potential cyber vulnerabilities of the power grid could be adversely manipulated by attackers, which may significantly threaten the system stability operated by power utilities. The bidirectional remote access between substations and control center as well as protection limitation across the boundary firewalls leave loopholes for attackers to sneak in when the configuration rules are weakly enforced [12]. Addressing integrated cyber-physical system (CPS) security in the control environment has become a pressing issue due to the exposure of power automation between the computerized control management system and the switchgear in power substations. This work proposes a risk-based assessment model by formulating the hypothesized substation outages, with overload implications, and extending to investigate the contingency with compromised digital relays. The cyber risk management framework is also discussed with the introduction of the cyber insurance premium.

1.1 Extended Enumerations of Hypothesized Substation Outages

The emergence of IP-based solutions in power automation has revolutionized industrial control systems. The cybersecurity of a power infrastructure relies on the technologically enhanced communication infrastructure to synthesize geographically dispersed substation information [13]. Most substations are upgraded with IP-based solutions, integrating with microprocessor-based protective relays as well as connecting to high traffic network between control centers and substations [13, 14]. The lack of auditing on remote substations and security protection can be the loophole as a backdoor for attackers. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance has now included more concrete clauses with possible technologies in the documents for improving protection implementation [15]. In addition, the presidential policy directive (PPD) 21 and executive order (EO) 13636 has enumerated the roles and responsibilities of the Department of Homeland Security [16].

In the parallel effort to compliance policies, National Institute of Standards and Technology (NIST)'s preliminary cybersecurity framework has envisioned five major components of the best practice to (1) identify, (2) protect, (3) detect, (4) respond, and

(5) recover [17]. Identification is the first step of all where organizations should determine deficiencies of security protection. However, ongoing efforts committed to the procedural compliance in security planning may not directly thwart the attack possibilities with potential security technologies in the substation control system.

Remote access to unmanned substation networks provides a convenient way to maintain the system by directly connecting from the authorized computers to the site. This is a security concern as the majority of security protection in substations are often deployed with commercial-grade firewalls. These are the routers with limitations that can be subject to intrusion if the whitelisting of firewalls is not properly maintained and audited. Generally, attackers plot for a cyberattack when they successfully intrude to a network. There are the attacks that may mislead operators that do not immediately affect the operation such as false injection [18, 19]. However, disruptive switching attacks can implicate operation that can be catastrophic. In 2013, NERC conducted hypothetically a drill exercise that would plunge millions of Americans into darkness. A year later, the Federal Energy Regulatory Commission (FERC) disclosed a combination of 9 key substations would be sufficient for such kind of widespread outage [20, 21]. This is one of the many combination cases that can have cascading consequences to the grid. Intrusion-based switching attacks affect substation reliability and can lead to cascading failure due to protective relaying within the network that can weaken system operating conditions [22, 23, 24].

With the aforementioned issues and significant development in recent years, the power grid has undergone a substantial upgrade with renewable sources and advanced communication infrastructure [25, 26]. This new normal has been anticipated with extreme threats such as natural disaster or cyberterrorism. The traditionally established N-1 contingency analysis shall be revisited to study the root cause effect. Research in the area of contingency extremism has been further investigated [25, 27, 28]. However, these approaches do not include the incurring failure effect in the CPS security-related contingencies that captures the potential cascades under abnormal operating circumstances. A causal inference framework, based on anomaly correlation, is prototyped to detect malicious activities by synthesizing cyber- and power-related sensor information [29]. The reversed pyramid model (RPM) has shown the promise of effective elimination of combinatorial worst cases [25, 30]. However, the proposed method is limited by the enumerative methods that may not explore the solution space with the segmentation approach, which may contain certain combinations with potential uncertainties that can lead to system-wide instability.

An enumerative framework is needed to evaluate the criticality of any combination. Table 1.1 specifies the differences between the solution spaces of weather-related and cyber-induced contingency analysis. It can be observed from the table that the weather-related contingency analysis usually is studied with a low level of the order, i.e., N-1 is the most common enumeration of presumed electrical faults. The contingency of N-2 is less likely to occur with multiple locations concurrently and so

as the higher order of N-k contingencies where it is often to model a double-circuit line under the same tower [31, 32]. The number of contingency selection is often based on a specific combination of the component outage which is based on the organizational practice in planning.

Table 1.1
Comparison of combination spaces between N-1, N-2, N-k, and sum of S-k contingency analysis

Contingency	50-substation system	Solution Space
Weather-related	Single-element failure (N-1)	50
	Double-element failure (N-2)	1225
	Multiple-element failure (N-k)	$\cong 10^8$
Cyber-induced	Exhaustive enumeration($\sum$ S-k)	$\cong 10^{15}$

The objective of this part of the research is to identify the pivotal substations by establishing enhanced metrics to quantify the cyber risks of a power system, which exhaustively enumerates all the possibilities. The approach we employ here is the combinations of IP-based substations that are connected with the lines, transformers, and generators. We assume that firewalls have limitations and so cyberintrusion can occur at any IP-based substations to be executed by attackers to disconnect lines, loads, and generators using the compromised substation control networks. This enumeration is a combinatorial problem where defenders would need to identify exhaustively the IP-based substations and hypothesized substation outages that can be detrimental to the power grid operation [1]. The major contribution of this work is to re-establish the cyber-based contingency approach to extensively enumerate (sum of S-k contingencies) by incorporating the overloaded lines based on a hypothesized outages of the substations. For the improvements of cyber-situation awareness, the

combinatorial model is two-fold: First, all worst-case scenarios are enumerated with an increase of k from 1 to S'. Then, each converged case is re-evaluated with the incurring lines that are electrically disconnected due to overloads.

1.2 Switching Attack through Compromised Relays

Technology in relays has evolved and has been transformed into full automation. Most substations have been gradually upgraded with the integration of the digital protective relays and IP-based solutions. These relays are the intelligent electronic devices (IEDs) that are part of the IEC61850 framework for substation automation [14, 33, 34]. Today, an average of medium-sized substations is deployed at about 50 protective IEDs. In most cases, the passwords are set up and maintained for those IEDs in substations. The sophistication of password management may also introduce inconvenience for maintenance where these tens of thousands of protective IEDs can be poorly managed. Each intentional trip manipulated by attackers can initiate detrimental effects. This cyber-physical tie must be studied carefully in order to understand associated risks and the attack implication [35, 36].

The cybersecurity of the power grid has been an emerging issue that is closely related to the reliability of the system. The North American Electric Reliability Corporation

(NERC) Critical Infrastructure Protection (CIP) compliance has introduced concrete standards for improvement of the cybersecurity level of power infrastructure [20, 37]. The French National Cybersecurity Agency (ANSSI) [38, 39] details the classification of the security measures in Industrial Control System (ICS) and specifies the vulnerabilities contained in the supervisory control and data acquisition (SCADA) network and the potential risks behind the operator behaviors. Additionally, National Institute of Standards and Technology (NIST) has published a preliminary cybersecurity framework with five major components [17] and introduced that the risk-based cybersecurity framework would be a benefit for cooperation between the customers, utilities, and vendors because an intensive discussion on the cybersecurity issue is required [40]. Recently, the Federal Energy Regulatory Commission (FERC) has issued an incident-report standard to strengthen the cybersecurity of the power grids [41].

In order to improve the risk-based assessment model, it is necessary to take the compromised IEDs into consideration in terms of the detrimental effects on the power system stability [42]. Additionally, as a defender, we might not be able to predict the attackers' motives but we could identify the critical protective IEDs which might lead to more devastating results than just disconnect electronically a substation, for example, if the protective relay is directly connecting to the switch of the load or generation unit, a suddenly disruptive change on the load and generation would cause steady-state instabilities and in worst case, transient-stability discussion is needed.

Additionally, when considering the influences of the diversity of the protective IEDs, several protective IEDs may cover the same protective zone and have similar events if compromised, which will also increase the difficulty of quantifying the effects for each IEDs. In terms of the combination complexity, compared with substation contingency S-k, an extensive evaluation of the protective IEDs would generate extremely large combination pool at 10 with the power of 30-100, which depends on the size of the studied case and number of protective IEDs that installed in each bus.

Despite technology introduced anomalies, the physics of the power grid with relaying remains, i.e., cascading will occur even if the initial cause of events has changed [43]. To quantify the potential cyber-based impact, the risk-based assessment towards the hypothesized substation outages have been studied in previous papers [26, 28, 29, 44] and a quantitative framework for determination of the criticality of each electrical component has been proposed in [1, 25, 45, 46]. Survey paper [1] categorizes the proposed framework into three main aspects: (1) critical/non-critical combination verification, (2) cascade confirmation and (3) combination re-evaluations with dynamic analysis. An extended enumerative framework is required to identify the worst-case scenario, which is an S-select-k enumeration. The extended evaluations of hypothesized substation outages are more complicated [1].

Defenders might not be able to predict the behavior of attackers and their strategies; however, defenders can plan exhaustively to identify the critical protective IEDs which

might initiate catastrophic consequence of a grid [47, 48]. The proposed method is to define the cyber-physical relay switching attack as the R-select-k problem, which verifies the simulation results on both the time-domain dynamic simulation and power flow analysis for the IED modeling. The cascading effect is studied to determine practical adaptability. The time-domain dynamic simulation model is implemented to check the consistency of the results between the power flow and tripping implication initiated by the plausible switching attacks through digital relays.

1.3 Cyber Insurance Framework

Insurance is a promising risk transfer tool against disruptive cyberattacks on power grids. Cyber insurance is proposed to cover the economic loss and liabilities due to the malicious cyberattack, which would incentivize utility owners to optimize their investment spending based on protective parameters and indirect benefits [49, 50, 51]. The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) has included stakeholders to work on the critical topics of risk management in security [52], which would help to improve the security posture in terms of (1) promoting the adoption of preventative measures; and (2) encouraging the integration of the best practice of self-protection based on their existing network architectures. Insurance, as a feasible method of risk transfer, is an in-developing stratagem, but still has attracted large attention from researchers in various fields

[53, 54]. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance has now published more clauses in order to implement necessary technologies for improving the cybersecurity of the control networks [15, 19, 20, 32]. Additionally, the recorded frequent attempts of intrusions into critical infrastructure networks reveal the cyber threats that the U.S power grid confronts now and the urgent need for improving cybersecurity [16, 17].

It is suggested that an internal failure of the information system can be modeled in a general insurance market with residual risk classification associated with security [55, 56]. The potential risk of vulnerable parameters is also identified using the provided framework in [56]. From the perspective of network security, stochastic processes have been employed to model the pricing based on security risks of information and communication technology (ICT) using the network topology [54]. However, security at the user level should be also incorporated as an integral part of the overall security modeling [57, 58]. The interdependency between the attackers' behavior and system architectures play an important role in this cyber insurance formulation in which it may generally lead to the competitiveness among insurers that would probably not be helpful for improving overall enterprise security. However, by integrating the physical impacts and mitigation strategies for a power grid with the cyber aspects, pricing for insurance premium can be accurately estimated [59].

The cyber insurance market for power grids remains in an emerging stage and it

is yet to mature. This new business opportunity is distinctive as compared to the traditional insurance mainly due to the lack of historical loss data [60, 61]. Another challenge is information asymmetry. As the insurance business in cybersecurity is not yet mandatory for power utilities, insurers would first need to establish a quantitative framework with the details of cyber-physical event replays to intertwine the potential cascading consequence of all possible outcomes in the premium calculation.

NERC CIP does not provide standardized metrics for quantifying residual risks associated with electronic intrusion to control networks. Most asset owners have their own way to secure their control networks [62]. However, if insurance companies can harness the digital evidence from the cyber systems and hypothetically enumerate some nightmare scenarios to replay the cascading outcomes, it would help to mature this emerging market. The risk theory can provide the quintessential basis for most insurance models and problems [63]. Estimating risks can be calculated using the ruin probability from the direct calculation method, which is known to be the basic risk model [63, 64, 65, 66].

This part of research proposes a framework for grid insurance against disruptive switching attacks, which is assumed to be determined by two major aspects: (1) the probability of successful intrusion into the substation(s) which will presumably result in disruptive switching attack from the compromised substation(s) and (2) the discrete distribution of claim size of each potential attack scenario [64, 65, 66]. The

vulnerability and the steady-state probability of potential electronic intrusion to each power substation have been studied in the papers [67, 68], which are derived from the firewall and password models using Markov chain. The steady-state probability [67] is assumed to be effective to generate the discrete distribution of the hypothesized scenario.

The organization of the thesis is organized as follows. Chapter 2 summarizes the literature surveys on the cyber-related contingencies of the power system. Chapter 3 introduces the risk-based assessment model with both hypothesized substation outages and switching attack through digital relays. Chapter 4 introduces a risk-management framework of cyber insurance premium calculation by modeling potential electronic intrusion and its direct impacts. Chapter 5 concludes the dissertation.

1.4 Publications

Papers:

† Z.Yang, C.-W. Ten, and A. Ginter, "Extended enumeration of hypothesized substations outages incorporating overload implication," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6929-6938, Nov. 2018.

† C.-W. Ten, K. Yamashita, Z. Yang, A. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405-4425, Sep. 2018.

† Z. Yang and C.-W. Ten, "Cyber-induced risk modeling for microprocessor-based relays in substations," in *Proc. 2018 IEEE Conf. Innov. Smart Grid Technol.-Asia (ISGT-Asia)*, Singapore. May 2018, pp. 856-861.

† Z. Yang and C.-W. Ten, "Assessment of hypothesized substation cyberattack using linearized power flow approach," in *Proc. 2017 IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Washington, DC, Apr. 2017, pp. 1-5.

Papers under review:

† Z. Yang, A. Y. Liu, M. Campbell, C.-W. Ten, Y. Rho, and L. Wang, "Cyber insurance premium for power grids," submitted to *IEEE Trans. Power Syst.*

† Z. Yang, K. Yamashita, C.-W. Ten, S. Kar, and A. Ginter, "Cascading verification initiated by the switching attacks through compromised digital relays," submitted to *IEEE Trans. Power Syst.*

Chapter 2

Risk Evaluations and Management of Cyberattacks on Power Grid

2.1 Introduction

The power grid has now emerged into one of the largest, most complex systems of human invention in all of history, involving tremendous communication bandwidth for the interactions between cyberinfrastructure and physical systems. SCADA systems are an essential part of power communication infrastructures and play a central role in ensuring effective operations of bulk power systems. SCADA systems have helped

to achieve new levels of system reliability and meet improved power quality requirements, especially when distributed energy systems have been incorporated in the grid [69, 70]. The use of IP-based communication frameworks though, has brought about concerns over cybersecurity issues. As a result, the operational reliability of a power grid requires new methodological developments to align reliability goals with emerging risks of new communications technologies [71, 72, 73, 74]. Currently there are no comprehensive techniques and tools available to model and evaluate the hypothetical impacts of cyberattacks. The abrupt disruption or disconnections of nodes corresponding to load and generation can result in detrimental effects to the power grid. A US Government report published in 2007 reported several incidents of cybersecurity penetration in control system of different critical infrastructure [75].

2.2 Power Control Center Framework

Power infrastructure communication is integral to a nation's critical infrastructure [76]. As early as the 1980s, the revolution of information communication technology (ICT) for power grid operation started changing how critical infrastructures are managed [77]. As shown in the Fig. 2.1, ICT consists of generation local area network (LAN), transmission LAN and wide area network (WAN), distribution LAN and WAN, distributed generation LAN and WAN and Customer LAN networks. Different LANs are connected through public communication networks that are generally

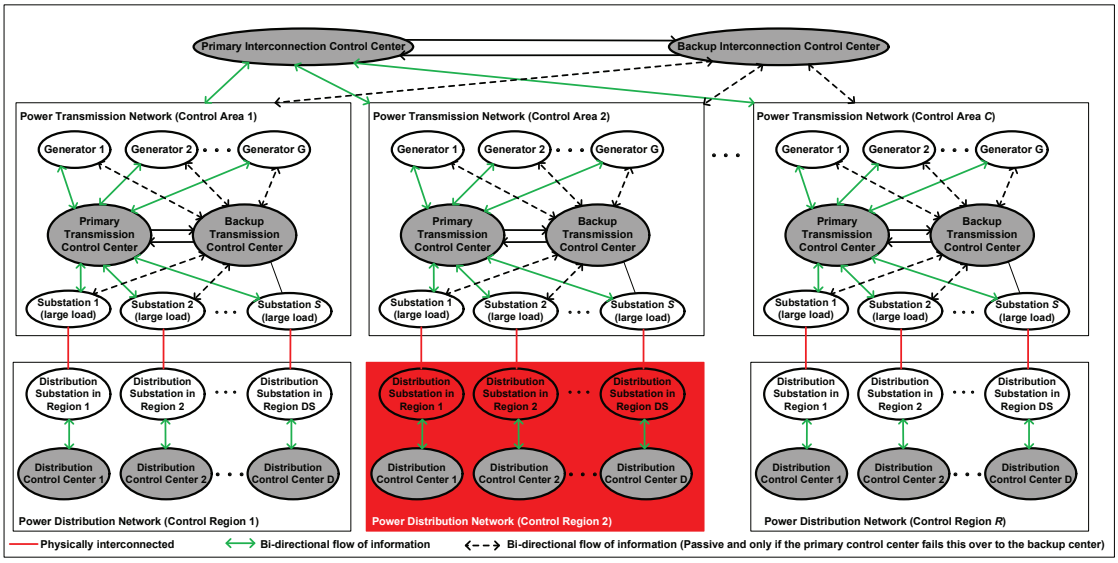

Figure 2.1: Generalized wide-area SCADA network connectivity between generation, transmission, and distribution systems of a power interconnection

managed by telecommunication companies. There are often three hierarchical control centers: (1) a national control center, (2) regional control centers, and (3) local control centers. Each local control center collects real-time data from physical systems of substations and transmits that data to regional control center after processing the data. Distribution Control Centers manage local control centers for the largest substations in the distribution system. The Ukraine cyberattack compromised the distribution control center as highlighted with a red box in Fig. 2.1. This would impact significantly the overall grid operation in a global sense of potential cascading in case of generation-load mismatch. Regional Control Centers are associated with managing high-voltage transmission lines and have supervisory control of all local control centers in that particular region. Regional control centers act as middleman between local control centers, distribution control centers and national control

centers. Regional control centers mainly control transmission substations. National control centers play a vital role in power system operation and controls. Such centers control the extra high voltage (EHV) transmission system, coordinate the activities of regional control centers, and are responsible for overall power system reliability and stability. National control centers collect real-time data from regional control centers and perform the function of EMS, state estimator and central network management of the overall power system [78]. Studies by the North American Electric Reliability Corporation (NERC) have shown that a simulated cyberattack drill demonstrates an absolute possibility to bring down the US power grids [79].

2.3 Past, Current, and Future Applications of Contingencies

The power grid is designed to withstand a single component outage (N-1 contingency), ensuring that operating limits are not violated by such outages [20, 80]. Power system reliability evaluation includes the integration of individual substation operating states and contingencies which are measured in terms of power frequency and duration of substation equipment outage events. Failure criteria for substations and violation thresholds of system reliability are defined based on substation size, location and functionality within the system [81, 82]. Literature review shows that there

have been a number of blackouts caused by cascading failures of transmission lines and generating units in recent years throughout the world [83]. If a substation is de-energized, the change in power flow is compensated by other substations, which must have enough spare capacity to carry the excess power. If they do not, transmission lines and transformers of those substations will be overloaded and overcurrent protection will trip those components to avoid thermal damage. This event will initiate a cascading failure as the excess power is switched onto neighboring circuits, which may also be running at or near their maximum capacity [84]. A probabilistic model can be used to estimate the cascading outages in high-voltage transmission network [85] and online dynamic security assessment in an EMS environment [86].

2.3.1 Single Contingency

Power system security is referred to the contingency analysis where an N-select-1 list of components is hypothesized as taken out of service to determine whether any such state results in a violation of voltage or power flow limits in a power grid [87]. In the 1970's, the traditional approach of steady-state contingency analysis is to test all contingencies, such as transmission line outage and loss of generation, that are predefined by system planner/operators experience and intuition [88]. Inadequacies of this traditional approach were later addressed and new techniques proposed to perform exhaustive testing, including both primary and secondary contingencies. Contingency

screening for fast realtime contingency analysis was proposed using modification of fast decoupled power flow algorithm [89]. An efficient contingency analysis method has been implemented to detect of flow violation for transmission lines[90].

2.3.2 Multiple Contingencies

To evaluate the contingency severity of removing any combination of substations from the system, an AC load flow method might be used [91]. Multiple contingency is seen to have largely prepared reliable systems to survive disasters [92, 93]. In North America, FERC has clarified that the list of the contingencies to be used in performing system operation and planning studies should include all the contingencies, N-1, N-1-1, N-2, as well as multiple contingencies [94]. As required by NERC reliability standards, the power system after a contingency should return to a secure, reliable state within 30 minutes [95].

Multiple contingencies have been researched since the late 1970s [88]. Since then, the main effort of such research is to reduce the computation burden caused by the tremendous number of contingency cases in bulk power system: the total number of N-k contingency cases is $N!/[k!(N-k)]$. Various screening and ranking techniques based on the theoretical approach and parallel computing techniques based on the simulation-based approach have been proposed and developed in the past five decades.

Conventional approaches related to the screening and ranking of contingencies are illustrated in [96, 97, 98, 99, 100]. After contingency studies for transmission planning were regulated by NERC in 2005 [95], research relevant to the NERC compliance study have accelerated and the techniques for searching for critical/credible contingencies which consists of N-2 contingencies and N-1-1 contingencies have been developed in industry as well as academia [95, 101]. Most of the approaches described by academia are based on network topology analysis [101, 102] and nonlinear optimization heuristics in terms of power planning perspectives. Because multiple contingencies could lead to cascading failures, multiple contingencies have also been studied in terms of wide area monitoring and protection with sensors such as PMUs in the wake of widespread blackouts affecting North America and Europe in 2003, 2004, and 2006. Since then, multiple contingencies and consecutive large blackouts have been a frequently discussed topic in industry. Information about past blackouts have been shared by industries and academia all over the world every two years during CIGRE Paris session since 2006 [103, 104, 105, 106, 107].

2.3.3 Cyber-Related Contingencies

As IP-based communications infrastructure is the trend for future deployments, expecting only N-1 contingencies is no longer be meaningful for both security analysts and power engineers [80]. As shown in the Fig. 2.2, a coordinated attack associated

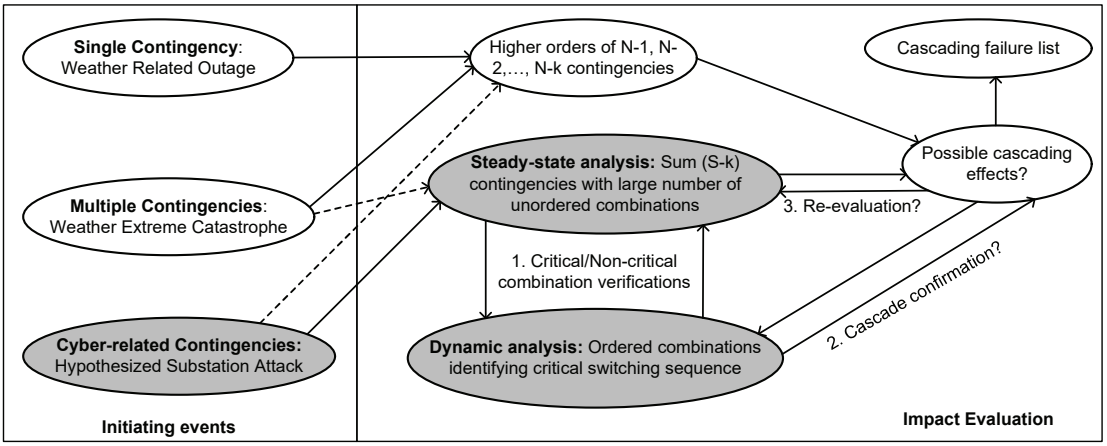

Figure 2.2: Conceptualization of impact evaluation

with compromised substations enables attackers to trip multiple generators, transmission lines, loads, or transformers nearly-simultaneously in a power grid, impairing system operating conditions. A more structured, integrated framework with high redundancy and defense mechanisms is required to face the challenges of intelligent coordinated cyberattacks, which can severely impact system operations [108]. Violation of predefined thresholds of substation voltages, system frequency, and branch flows may lead to cascading failure and a system blackout [109].

As system loading levels vary over time, the criticality of each substation (node) can be different at different times [110]. An approach to hypothesize multiple substation outages is proposed to presume that a set of combinations of IP-based substations are compromised by intruders and are electronically manipulated to abruptly isolate substations from the grid with disruptive switching actions [111, 112]. Combinatorial substation outages are the cyber-contingency analysis that enumerates the worst-case scenarios. Since the solution space of the sum of S-select-k problem can be

extremely large, a systematic elimination approach using power flow modules is used to validate each combination in order to capture the worst combinations [25, 30, 111, 112]. This process eliminates insignificant combinations, enumerating from the first-level substation list of the RPM. While this approach may not be exhaustively enumerated; it can be further enhanced with prioritization of substation selection criteria. This contingency analysis is based on the relationship between substation critical cyber systems that have direct interaction with the physical power grid, i.e., the cyber assets that would have control capability to disconnect local components from the grid. Based on the conclusion of previous work [111, 112], manipulation of microprocessorbased relays on bus differential protection would have a detrimental effect, able to disconnect large numbers of components from the system. At minimum, hypothesized cyber attacks would occur at multiple substations, as attackers would be able to intrude to the S number of IP-based substations. Under this assumption, at least one or more substation outages would occur, depending on the number of substations that have been compromised [30, 111, 112].

Preliminary investigation on system reliability and its resulting impacts have shown the effectiveness of the proposed algorithm with quantitative analysis on penetrated protective IED relays [113]. A small number of approaches exist to find critical substation combinations or collapse sequence of cascading failures, but none are in online environments, and all are applicable only to restricted numbers of combinations of

substations [91]. Since the event of simultaneous cyberattacks on 3 or more substations is rare, the worst case will be considered. Priority list 2 only evaluates the impact by de-energizing more than two substations that result in the impact factor of 1.0 and serves as a message to control centers [114]. Cyber-based contingency analysis is a fundamentally new way to assess the system stability by considering all plausible attack vectors. These attack vectors can be any combination of these: (i) distributed denial of service (DDoS) [115, 116, 117],(ii)alter and hide (AaH) [118], (iii) data integrity [119, 120], (iv) load altering [121], (v) disruptive switching [116].

2.3.4 Dynamics of Intelligent Cyberattack

The existing major entities of bulk power systems have been upgraded with IP-based communication infrastructure over the past decades. The manipulation using a compromised local control system can impair system operation due to the potential impacts on the physical system. The triggers of system dynamics, such as disconnections or abrupt shutdown of important elements within a power grid, can implicate the possibilities of system stability.

One of the worst-case scenarios is a widespread cascading failure that will lead to a power blackout costing tens or hundreds of billions of the dollars to an economy as large as that of the USA. The importance of considering power system dynamics

for cybersecurity issues has already been recognized. Power system dynamics can be significantly affected by network communication and control system infrastructure including generator controllers and protective relays. The establishment of a mathematical formulation for representing power system dynamics is a non-trivial task. Controllers and protections include non-linear behavior and discrete changes. In addition, any formulation must account for many interactions. There can be interaction between controllers and interaction between protection equipment. There can be interactions between controllers and protection, between controller and the grid, and between protection and the grid. This sub-chapter focuses on the review of the recent studies that are relevant to power system dynamics.

The recent research studies can be categorized as focused on either (1) Abnormal power system dynamic phenomena, or (2) Measurement of implementing cyber-physical security systems. Typically, an abnormal behavior of power system dynamics is classified into four phenomena that can result in a widespread power outage: voltage stability, frequency stability, transient stability and overload. The latest research studies cover the first three abnormal phenomena.

2.3.4.1 Transient Stability

Transient stability is examined using the undesired control of the semi-conductor-based reactive power compensators such as static var compensator (SVC) and static

synchronous compensator (STATCOM). References [115, 122, 123] exhibit the possibility of being out-of-step due to biased or delayed operation of SVC or STATCOM. The fundamental idea is to represent the same dynamic behavior, even when the improper control parameters are tuned. Modification attack is assumed to be responsible for the undesired control. This vulnerability is relevant only when a system fault occurs near the reactive power compensator.

2.3.4.2 Frequency Stability

Frequency stability is examined using undesired control of Automatic Generation Control (AGC) or falsified load change data. Because falsified load changes have the same effect as an undesired control signal of AGC, the two attack scenarios can be treated as the same one. References [119, 124] exhibit the possibility of frequency collapse which results in significant frequency change, such as 3 Hz or more. The fundamental idea is to represent the same dynamic behavior when the wrong/improper control parameters of AGC are tuned. Data integrity attacks are assumed for the undesired control and the falsified load changes. The sudden loss of generation/loads can also cause frequency instability [116, 117].

2.3.4.3 Short-Term Voltage Stability

Short-term voltage stability is examined using the undesired control of stepwise change in active or reactive power outputs. Reference [120] exhibits the possibility of short-term voltage collapse which is caused by a significant voltage drop. The fundamental idea is to change active or reactive power output in order to generate a growing power swing oscillation and/or to have a shortage of reactive power support in the whole grid. In this study, transient stability problems seem to occur when a voltage collapse occurs. In the case of large networks, the short-term voltage collapse in entire power system could lead to an outof-step condition in the entire network. Short-term voltage response is also examined using the non-operation of primary relay or unwanted operation of the back-up relay. Reference [120] also exhibits the possibility of large voltage excursion. The fundamental idea is to enlarge the impact of the fault via nonoperation of the primary protection or the unwanted operation of the back-up protection. However, the goal of the paper [1] does not represent blackouts, but to establish a complex cyberphysical system. Similar study includes using the undesired control of SVC caused by man-in-the-middle attack [125].

2.3.4.4 Slow Dynamics

Long-term dynamics is considered using the arbitrary load change by jamming the pricing signal in the electricity market. References [121, 126] studies the possibilities of unwanted slow dynamics caused by the delayed and distorted data-centric attack, which eventually causes the degradation of the controller performance and the negative impact on any kind of the power system stability. Smart meters in electrical distribution network which utilize wireless communication such as WiMAX is assumed to be used for this scenario and the jamming attack is applied to the electricity market in order to jam the power price signaling over a large area such as the load center. Such manipulation of the electricity market via the data-centric attack (or the false data injection attack) can bring the attacker to the profit and cause the significant impact on the stability of the power system.

2.4 Insurance Implications of Contingencies

Many research organizations and institutes are seeking for insurance model that would respond to cyberattack, which is believed to be an under-insured risk [60]. Financial and insurance incentives are believed to be another effective method to improve the security and resilience of the grid [59]. Understanding the impact of the severe

cyberattack event is particularly significant to develop insurance solutions. Though, currently, the insurance plays a limited role electricity area, in general, the insurance would be designed to reduce the liability or prevent catastrophic damage from cyberattack. Most large utilities have participated in a large mutual risk pool called Associate Electric & Gas Insurance Services Limited (AEGIS), which is an insurance company that has included entire energy infrastructure in North America and provides liability, property coverage, and related risk management services.

Cyber insurance is relatively new type of insurance that covers a broader range of issues related to cyber risk, which presents several challenges [59]: (1) Cyber risk is hard to measure, model, and price due to lack of actuarial data. (2) The consequences and the probability are hard to measure. (3) It is hard to assess the liability and risk when a cloud or third-party service provider is included. (4) "Cyber risk is a dynamic, evolving threat, which is not constrained by the conventional boundaries of geography, jurisdiction or physical laws." Additionally, the cyber insurer is also required to consider different types of coverage, including power generation company, utilities, companies losing power, and homeowners. Despite these challenges, the cyber insurance is a promising method to help to improve the cybersecurity and resilience of the power grid.

Chapter 3

Cyber-Risk Assessment Model

3.1 Introduction

The cyber risk assessment framework is introduced in this chapter with evaluations of the system instabilities in terms of the physical impacts that are caused by the cyber manipulations. The contingency planning study would include the "what if" attack scenarios that would disconnect compromised substation(s)/component(s) from the system, which would normally includes multiple N-k contingencies. The risk assessment model is validated using both the steady-state and dynamic methods with implications of the enumerative combinations.

The hypothesized substation outages are conducted in the chapter through evaluating

the risk of cascading outages, which is also associated with overloading consequences. As a result of electrical short circuits, protective relaying picks up the faults and electrically disconnects overloaded transmission lines through circuit breakers. With similar disturbance and implication, disruptive switching cyberattacks in one or more compromised substations can initiate such events that will aggravate system's operating conditions, leading to a widespread blackout. This chapter applies an extended enumeration of substation outages that excludes the overloaded lines from a power flow model, which is denoted as S-k contigency. First, the exhaustive combination which starts from the initial combination size k = 1 is enumerated searching for non-convergent solutions of the hypothesized contingencies associated with the outages of single or more substations. Once the critical substations are compromised, attack agents can coordinate among their peers to plot for maximizing disruption using local control devices.

Defenders might not be able to predict the behavior of attackers and their strategies; however, defenders can plan exhaustively to identify the critical protective IEDs which might initiate catastrophic consequence of a grid [47, 48]. It is also critical to enumerate and identify all digital relays to determine the systemic risks. Any combination of disruptive switching via the compromised relays can result in misoperation or immediate effect to the system. The resulting consequence of these attack's initial events would possibly incur cascading failure to a grid. This work also defines the cyber-physical relay switching attack as R-k contingency, which verifies the simulation

results on both the time-domain dynamic simulation and power flow analysis for the IED modeling. The cascading effect is studied to determine practical adaptability. The time-domain dynamic simulation model is implemented to check the consistency of the results between power flow and tripping implication initiated by the plausible switching attacks through digital relays.

Chapter 3.2 provides the modeling details of cyber-based substation outages with overloading implications. Chapter 3.3 introduces a linearized method to the modify the S-k model incorporating islanding issue. Chapter 3.4 introduces a probability-based framework to evaluate the potential impact of the outages of protective relays. Chapter 3.5 extends the R-k model by incorporating the static and dynamic validation. Chapter 3.6 presents the simulation results.

3.2 Extended Enumeration on Hypothesized Substation Outages

The purpose of this chapter is to re-establish the cyberbased contingency approach to extensively enumerate (sum of S-k contingencies) by incorporating the overloaded lines based on a hypothesized outages of the substations, using RPM method. For the improvements of cyber-situation awareness, the combinatorial model is two-fold: First, all worst case scenarios are enumerated with an increase of k from 1 to S'.

Then, each converged case is re-evaluated with the incurring lines that are electrically disconnected due to overloads.

3.2.1 Modeling of Hypothesized Nodal Outages

In this formulation, the initiating events are the disruptive switching cyberattack on those compromised IP-based substations that initiate cascading effect and disconnect sequential overloaded components, such as lines, transformers, or generators from a power system. Like many blackout events occurred in the past, line outages are often caused by the initial outage that can be modeled by overloaded lines. Generally, the protective relays will disconnect electrically those overloaded components when an electrical fault is detected between two substations based on pre-defined protection schemes.

The hypothesized nodal outage here is referred to any plausible cyberattack events associated with IP-based substations. This section is divided into two: (A) Extended enumerative approach and (B) Determination of nonconvergent power flow.

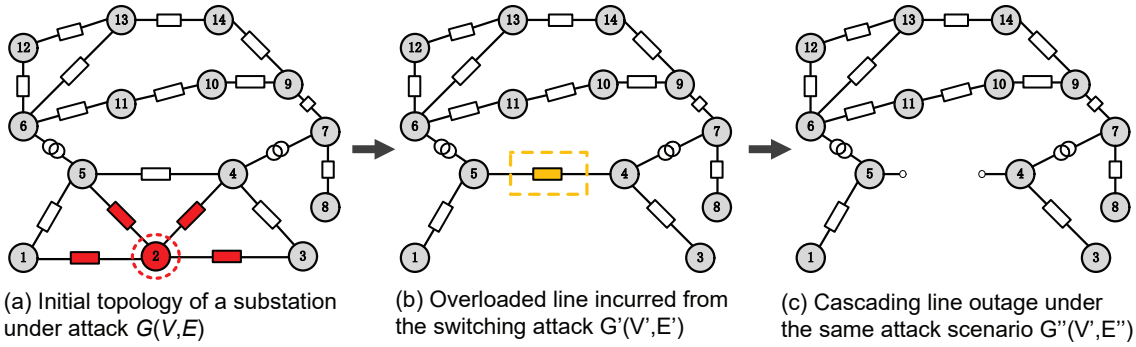

Figure 3.1: Graph representation for a hypothesized substation outage G' and its cascading outage G''

3.2.1.1 Extended Enumerative Approach

$$\underbrace{G(V,E)}_{\text{(a) Original } G} \xrightarrow[\text{cyberattack}]{\text{Switching}} \underbrace{V'(G') = V(G) \setminus V_k \subset S_{sub}}_{\text{(b) Hypothesized substations outages}} \xrightarrow[\text{overloading}]{\text{Potential}} \underbrace{E'(G'') = E(G') \setminus E_k \subset \mathcal{L}}_{\text{(c) Overloading outages}}$$

$$\Longrightarrow \underbrace{E'(G'') = E(G') \setminus E_k \subset \mathcal{L}}_{\text{(c) Overloading outages}} \xrightarrow[\text{power flow status}]{\text{Determine}} \mathbf{PF}_{failed} \tag{3.1}$$

A steady-state analysis using power flow module is employed to verify the overloading effect that characterizes the sequential outages by excluding those from the power flow model. To explicitly describe the topology statuses before a plausible cyberattack event, we represent a power system as a graph $G(V, E)$ depicted in Fig. 3.1(a). The graph consists of vertex set V and edge set E that corresponds to each of those as substations and transmission lines, respectively. Equation (3.1) describes generally the topology statuses for each transition of Fig. 3.1 in a graph where S_{sub} is a

set of total IP-based substations of the total number of substations S_{Total}, such as $S_{sub} \subseteq S_{Total}$. This implies that not all substations are IP-based but all substations can be upgraded with IP-based communication infrastructure in the future. The $\mathcal{L}$ is a set of total transmission lines associated with all substations S_{Total}. The prime ($'$) and double prime ($''$) represent an updated topology status of each transition from the causing to the incurring perspectives, i.e., parts (a)–(c). The motivation here is to determine if the power flow fails to converge $\mathbf{PF}_{failed} = 1$ for the combinatorial study of a power system under certain operating conditions.

The total number of combinations from $k = 1$ to the S'-th level is enumerated as $\mathbb{S}' = \sum_{k=1}^{S'} \mathbf{C}_k^S$[25], where S is the total number of IP-based substations in a power system, and k is a pointer of each k level as it increases closer to total number of substations S . The S' value introduced in this work is the depth level that is smaller than the total number of IP-based substations. The $\mathbb{S}'$ is the sum of total combinations for each level before level S. Fig. 3.2 shows the enumeration from $k = 1$ to S' with the demonstration of decreasing ratio $\psi(\cdot)$. As depicted on the left side of the figure, a substation outage ($k = 1$) is presumed. As the level k increases, so as the combinatorial complexity when more substations "goes south." Each level, it consists of two parts, i.e., ψ is denoted by the ratio of new reduced combination, the other part $1-\psi$ is the ratio of reduced combinations and $\mathbf{C}_k^{S'} \cdot (1-\psi)$ is a total combination to be reduced at the level of S'. To describe the cases between levels, the following

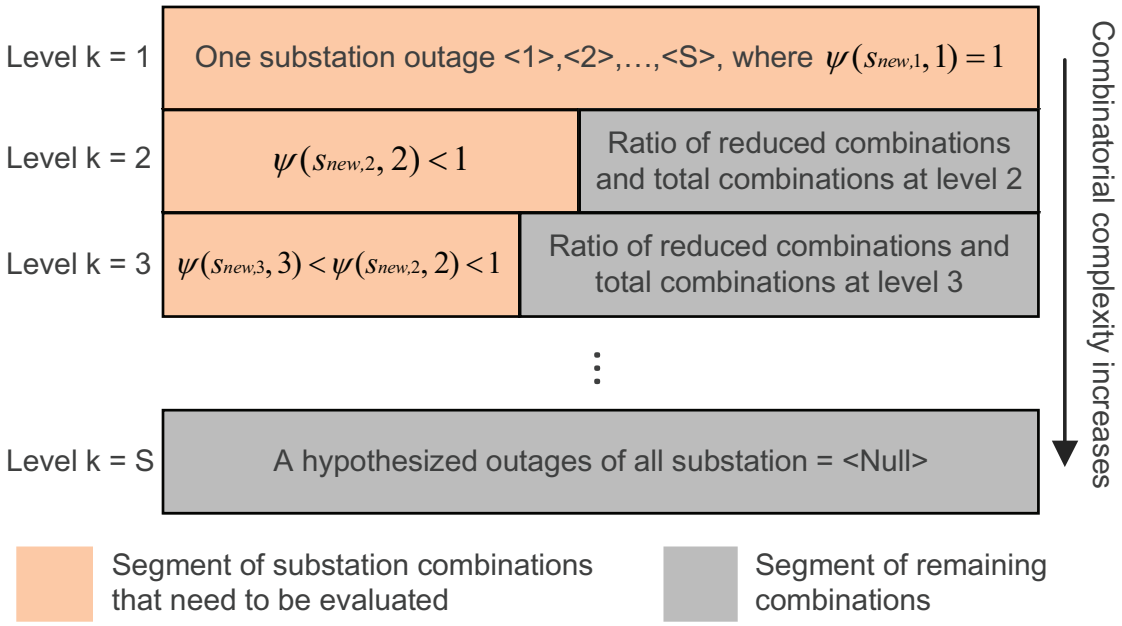

Figure 3.2: Enumeration from $k = 1$ to S' with decreasing ratio $\psi(\cdot)$

are generalized.

$$\psi(s_{new,k},k) = \begin{cases} \frac{s_{new,1}}{\mathbf{C}_1^S} = 1.0, & k = 1 \\ \frac{s_{new,2}}{\mathbf{C}_2^S} < 1.0, & k = 2 \\ \frac{s_{new,k}}{\mathbf{C}_k^S} < \frac{s_{new,k-1}}{\mathbf{C}_{k-1}^S} < 1.0, & k \geq 3 \end{cases} \tag{3.2}$$

At level one, the ratio of new reduced combination ψ dominates by 1.0. In the contrary, at the last level $k = S$, the $1-\psi$ will be 1.0. These ratios are the reflection of effective reduction of enumerated combinations at each level. Without eliminations from the previous level, the total combination of S-select-k will increase as k grows. Some nonconvergent combinations from the previous level will not carry on to the current level as these combinations can be the subsets of the new total combination

at the new level $k = k + 1$. The proposed ratios measure new reduced combinations for each level before power flow verification. For example, in the IEEE-39 case, 1,868 out of 888,030 combinations are required to be evaluated at the $k = 7$ and 886,162 combinations can be reduced. At the level of 8, which is the last level of the evaluation, only 424 out of 2,220,075 cases need to be tested and over 99.98% combinations are removed, where $\psi = 0.019\%$. For a larger system, the solution space will increase exponentially but the ratio ψ indicates the reduction of total combinations as the k increases. A smaller ratio ψ would indicate decreasing "worst case" combinations for the next levels of k using power flow module as the verification.

3.2.1.2 Determination of Nonconvergent Power Flow

Under the steady-state approach, it is an indication of instability under one single system when a power flow model fails to converge [25, 127, 128, 129]. Depending on the scenarios, sometimes it may require further investigation using dynamic simulation to confirm a potentially unstable case.

It could also imply other situations, such as transfer capability of the transmission grid is weakened by the protective relays with multiple electrical disconnections. Under certain circumstance, multiple islands may also form as a result of the initiating events. The errors are due to multiple subsystem split in which each of them requires a slack bus to be initialized. We denote the failure of power flow convergence by

$\mathbf{SS}_{failed}$.

$$\mathbf{SS}_{failed}(k) = \mathbf{PF}_{failed}\Big(G'(k)\Big) \bigcup \mathbf{PF}_{failed}\Big(G''(k)\Big) \tag{3.3}$$

where, $\mathbf{PF}_{failed}(\cdot) \in [0,1]$ indicates either a converged or diverged outcome, respectively. $\mathbf{SS}_{failed}(k)$ is the nonconvergent combination list at the level of k in the extended enumeration. $\mathbf{PF}_{failed}\Big(G'(k)\Big)$ and $\mathbf{PF}_{failed}\Big(G''(k)\Big)$ are the nonconvergent solutions based on steady-state power flow evaluation based on the topology statuses of hypothesized substation outages G' and cascading failure G'', accordingly.

$$ss_{failed} = \mathbf{SS}_{failed}(1) \cup \mathbf{SS}_{failed}(2) \cup \cdots \mathbf{SS}_{failed}(S') \tag{3.4}$$

where ss_{failed} is the final nonconvergent list that is derived from the $k = 1$ to $k = S'$ where S' is at the level where it stops for future determination of combinations.

The sum of new reduced combinations at each level k before power flow verification is estimated as follows:

$$s_{new,k} = \Big(\mathbf{C}_k^S - \chi\Big) \tag{3.5}$$

where χ is the total reduction number that was extracted from the last level of $\mathbf{SS}_{failed}(k-1)$ set. The count of all level combinations before power flow is determined as follows:

$$S_{new} = \sum_{k=1}^{S'} s_{new,k} \tag{3.6}$$

S_{new} is the summation of total combinations from levels $k = 1$ to $k = S'$. This total number before power flow is to determine nonconvergent combinations from the set of S_{new}. This is used as a denominator for a ratio to estimate proportional reduction from nonconvergent power flow cases.

The total sum S can be enormous when a larger power system is simulated. Determining the depth level of S' would avoid repeated enumeration of subsets. This terminates the combinatorial evaluation at that depth level to assure completeness of identifying the worst cases for computational effectiveness. The following is the criterion to determine S':

$$\text{Depth}\left\{\left(\mathbf{PF}(s_{new,k}) = \emptyset\right) \bigcup \left(\text{union}(ss_{failed}) = S_{sub}\right)\right\} \tag{3.7}$$

The conditions for these two to be met are based on combinatorial results from power flow evaluation as well as assuring the unique set of total IP-based substations are identified. Having this logical conditions would assure there are no other critical combinations that might be neglected at the higher order of k. By doing so, this would help to eliminate unnecessary enumerations as it approaches closer to S level, which can be computationally intensive. Chapter 3.2.2 will detail with the proposed enumeration algorithm to exclude the components in the power flow and overload model.

3.2.2 Incorporation of Switching Attack and Overloading Consequences

Chapter 3.2.1 illustrates the mathematical model of extensive enumeration and the computational complexity of hypothesized nodal outages shown in Fig. 3.1 (a) validated by power flow simulation. This section continues with the same scenario with incurring overloads on transmission line(s)/power transformer(s), which is later to be confirmed by power flow model on the potential system instability. Figs. 3.1 (b) and (c) shows the sequential events how overloaded components are excluded from a power flow model in 3 steps. The following subsections are the sequential examinations of power flow convergence.

3.2.2.1 Consideration of Protection Schemes

The stability evaluation of cascading outages is a dynamic-security analysis with variables in transient status such as time period, frequency and voltages instability, generation-load rebalance, and cost/benefit analysis[130, 131]. Our focus in this research does not include transient analysis and is not discussed here. The steady-state approach includes the overload model in our study to consider the effects of protection scheme on transmission line. The currents are determined by the voltages and the

power flow solution of each line [132]. Since the overcurrent is preset based on the rating of ampacity for a transmission line. The overcurrent scheme is also set as a primary protection with high sensitivity. We have selected this scheme in our relaying model, which will operate when the overcurrent magnitude exceeds the permissible level to electrically disconnect a line.

Other protection schemes may be considered but might not be feasible in our study. For example, the differential and pilot protection relays are measuring the variation of currents between the two ending points of a transmission line, which may not be triggered presumed fault within a particular line, i.e., our study simply does not inject short-circuit fault currents in the model. Phase distance protection relays are normally set as backup protection for transmission line with an extended time delay, which is not applicable in the steady-state analysis. Additionally, the ground distance protection is applied only when the phase and sequence data are available and the zero sequence current will be detected in asymmetrical fault analysis, which is not applicable in the steady-state evaluations. We assume that all overloaded lines would be disconnected by the primary protection relays and the time delay is not included.

In our simulation, both G' and G'' are considered as initial value for steady-state evaluation. The determination of potential line outages is modeled based on the thermal and ampacity limit of each branch [131, 133, 134]. For example, the hypothesized

nodal outages of substations A, B, and C, resulting in five transmission lines overloaded. If these branches met the tripping criteria of instantaneous overcurrent relay, we exclude those incurring branches out of the power flow model. The power flow at transmission line i is denoted by $\mathcal{L} = \{l_1, l_2, \cdots, l_i, \cdots, l_N\}$ where N is the total number of branches. The element v_{f,l_i} in the set $\mathcal{V}_{\mathcal{F}} = \{v_{f,l_1}, v_{f,l_2}, \cdots, v_{f,l_i}, \cdots, v_{f,l_N}\}$ denotes the voltage of the from-node corresponding to the transmission line i. It is noticed that both the set $\mathcal{L}$ and set $\mathcal{V}_{\mathcal{F}}$ acquire the same size of N. The current I_i that goes through transmission line i can be calculated through the set $\mathcal{L}$ and set $\mathcal{V}_{\mathcal{F}}$, which is saved in the set $\mathcal{I}$. Once it is detected that the $|I_l|$ exceeds the corresponding pickup value $|I_{p,l}|$ set by the instantaneous overcurrent relay, the transmission line l will be disconnected. The tripping condition can be written as:

$$\text{Condition\_A} : \Big(|I_l| > |I_{p,l}| \Big) \tag{3.8}$$

The flow of power at each transmission line l from power flow calculation is denoted by $\mathcal{L}_{\mathbf{PF}} = \{l_{\mathbf{PF},1}, l_{\mathbf{PF},2}, \cdots l_{\mathbf{PF},N}\}$ where N is the total number of branches and $\mathbf{PF}$ is the thermal and capacity magnitude of lines from power flow calculation. The removal of an overloaded branch is based on the following two conditions:

$$\text{Condition\_B} : \Big(\mathcal{L}_{\mathbf{pf}} > O_{limit,S}(\mathcal{L}) \Big) \tag{3.9}$$

$$\text{Condition\_C}: \Big(\mathcal{L}_{\mathbf{pf}} > C_l\Big) \bigwedge \Big(O_{limit,L}(\mathcal{L}) < O(l,\tau)\Big) \tag{3.10}$$

where $O(l,\tau)$ is $\int [\mathcal{L}_{\mathbf{pf}}(\tau) - C_l] d\tau$ and C_l is the ampacity rating for each transmission line. The relationship between short-term and long-term ratings are denoted by $O_{limit,S}$ and $O_{limit,L}$, respectively, $O_{limit,S} = \kappa \cdot O_{limit,L}$ and $\kappa > 1.0$. The τ defined here is a small time window in between any causing or incurring event of *pre* and *post* conditions. The relationship between this small time interval can have an abrupt change in current magnitude either increase or decrease. Since the τ value is relatively insignificant, we assume that the *pre* and *post* conditions can be modeled in a step function for the two-period transition. The "tripped signals" be sent by the protective relays will exclude those components as follows:

$$(\text{Cond.\_A} \bigvee \text{Cond.\_B} \bigvee \text{Cond.\_C}) \rightarrow l_{trip},\ l \in \mathcal{L} \tag{3.11}$$

The additional short-term (condition B) and long-term (condition C) ratings of the two operating limits are verified when there is a power flow solution. Under certain conditions, we might encounter the situation of hypothesized substations outage that does not contribute to the reduction of total generation and load, i.e., the hypothesized substations outage associated with no load or generators may incur overloading conditions to other transmission lines that may not exceed the long-term limit but short-term one. This OR logic of (3.11) indicates either one or more of the two conditions.

3.2.2.2 Detection of Islanding

In a larger system, the initiating event of switching cyberattacks upon those substations may incur overloading, resulting in multiple islands, which requires necessary modifications on risk index[25]. For a smaller system, it may not necessarily split the system into two or more islands; however, the power flow verification may disagree with a diverged outcome. Combining equations 3.3 and 3.4, the result ss_{failed} contain the nonconvergent combinations with a potential overload.

The binary outcome for each power flow result does not indicate the root cause of problem. Under the observation of this study, the initiating events of plausible cyberattacks can result in splitting a power grid into multiple islands. Detecting the number of islands is crucial for the proposed stability study in terms of modification of risk index[25], which is a measure that quantifies the impact level of each hypothesized combination of outages for the IP-based substations. The islands might not enable power flow verification due to the lack of slack bus for each island and shall be handled individually in order to power flow solutions.

Below are the steps to determine a case with more than two islands:

1. Initialize from the power flow calculation under the topology status of G''.
2. Identify all excluded lines from power flow models.

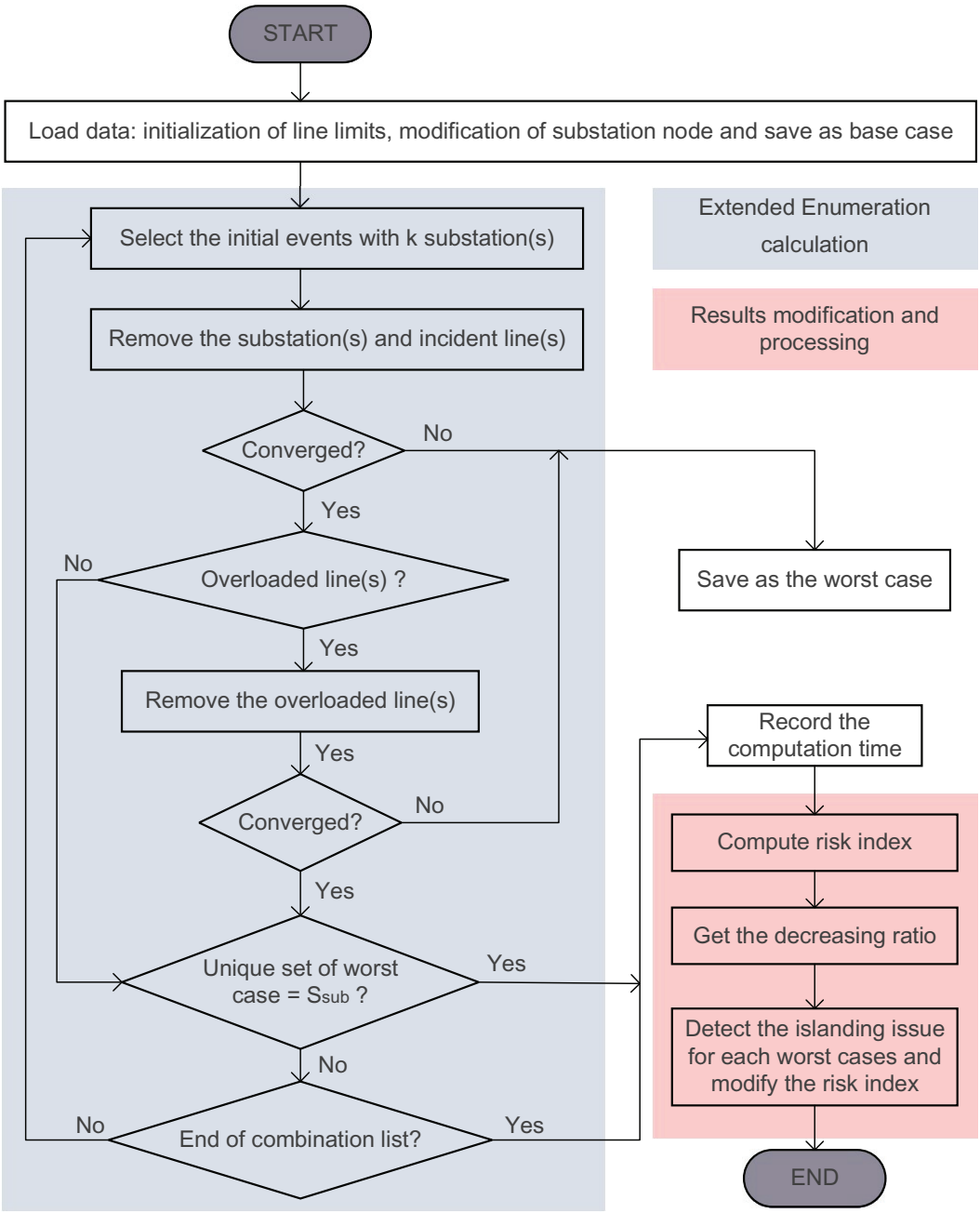

Figure 3.3: Flowchart of extended enumeration incorporating the potential overloads

3. Modify existing adjacent matrix $A(G'')$.

4. Determine the depth matrix $\hat{A}(G'')$ of $A(G'')$ where $\hat{A}(G'') = A(G'')^Q$ and

$Q = 1, 2, \cdots, \xi$.

5. Find unique vector, row by row, from $\hat{A}(G'')$.

6. The total number of islands is determined from the total number of unique vector.

As this may require future investigation, regardless of the number of islands formed, we relate the risk of such case to be discounted for the risk metric $\tilde{R} = .5R$ [25]. The one-half constant indicates the uncertainty between the worst case and benign situation associated with each substation outage.

Fig. 3.3 summarizes the proposed algorithm incorporated with an overload implication, which includes 2 main parts. Part (a) contains the combinatorial enumeration of power flow evaluation with overloading implication. Part (b) contains the modification of risk index after an island is detected.

3.3 Improved Risk Metric with Islanding Consideration

The microprocessor-based protective relays will trip when a disturbance occurs and will disconnect the line from a network. The disconnection of any single component by

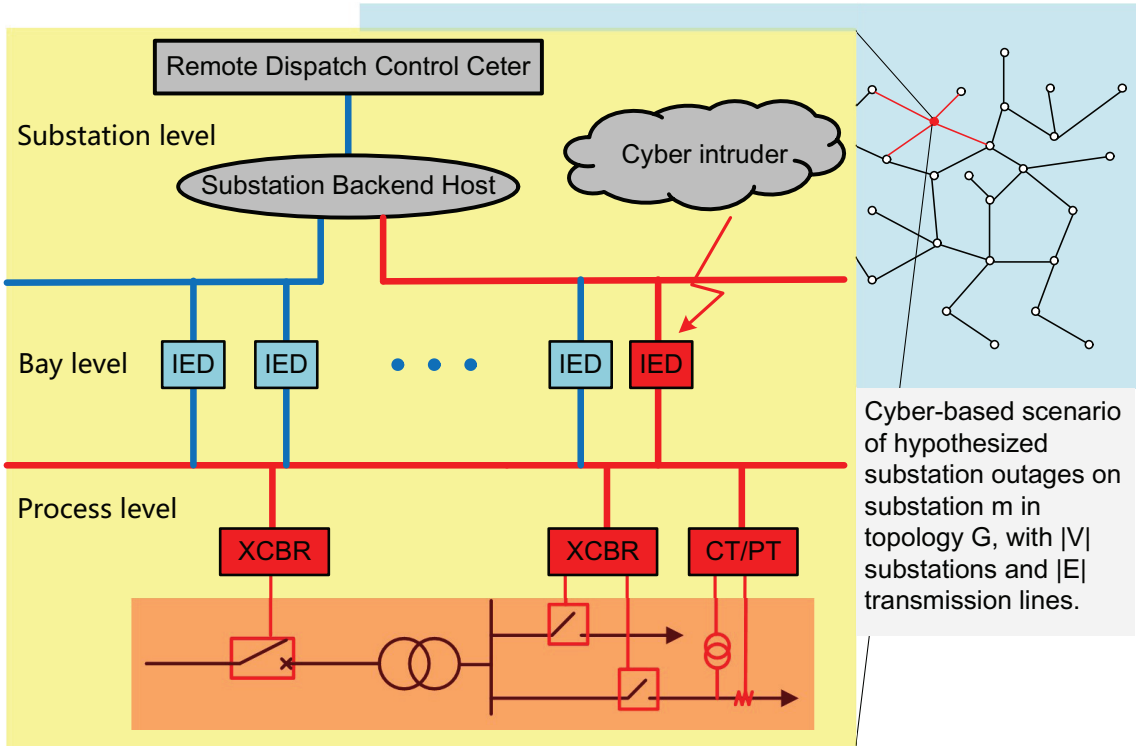

Figure 3.4: Possible intrusion paths within a substation network where the microprocessor-based relays are instrumented to the physical facilities

the protection scheme is referred to a single component outage N-1 for the contingency analysis. The setup of IP-based solutions is configured in each power substation. Fig. 3.4 depicts scenarios of an intrusion path on an IP-based substation and the critical cyber assets within the substation control network. The hypothetical scenarios here are the electronic intrusion by the attackers would help them to discover the IED within the network that may further lead to execute manipulative switching operation. We hypothesize the worst case outcome based on the intent of attackers' motive, i.e., to disrupt operations by disconnecting large number of switches within the substation from a power grid. We also assume that the hypothesized substation outage shall not restrict to a single substation as the attackers may be able to compromise multiple

Algorithm 1 The extended enumeration method

```
1: Load data
2: for k = 1 : S do
3:    Initialize S-select-k combinations
4:    r ← run power flow of case[G(V\K)]
5:    if r = 0 then
6:       save it in the set S
7:    else
8:       remove the overloaded line(s) L
9:       r' ← run power flow of case[G(V\K, E\L)]
10:      if r' = 0 then
11:         save the case in S
12:      else
13:         continue
14:      end if
15:   end if
16:   set T ← unique (S(1) ⋃ S(2)···S(k))
17:   if T = V then
18:      return worst-case list S
19:   end if
20: end for
```

substations and execute their attack plan. We denote the total number of substations in a power grid as S, where $N > S$. We represent G as the topological status of the grid, where substation set V and branch set E.

A pseudocode of the hypothesized substation outages is given in Algorithm 1. This extended algorithm of [25] emumerates with $k = 1$ to S. The steady-state analysis is applied for the verification of critical scenarios of substation outages. The binary results $[0, 1]$ denote the convergent and nonconvergent solutions, respectively. Note that K is a set of substations with size $|K| = k$, which is derived from the list of complete combinations of S-select-k contingencies. The overloaded lines are the elements in the set denoted by L that are presumably tripped by relays. We describe

the topological status as $G(V\backslash K, E\backslash L)$ with the elimination of K substations and L branches. The binary results of power flow evaluation are defined by r and r'. A worst-case list $\mathbf{S}$ is added with new cases during each iteration of selected outages based on the results of power flow where row k is the array of the list $\mathbf{S}(k)$. All unique substations T are recorded denoted by $T \subset \mathbf{S}$. This extended enumeration algorithm verifies cases with multiple islands with an incorporation of overloading effects. This also improves the accuracy by eliminating the potential uncertainty of unevaluated combinations. The algorithm creates a worst-case combination list, which helps to determine the criticality of each substation under the proposed model.

This chapter provides a scenario where a power system is separated into two or more subsystems while the substations under attack have been disruptively disconnected from the grid through the local control console. As mentioned in the previous section, we employ a steady-state power flow solution to verify critical scenarios (islanding combinations). The outcome from the evaluation of a split system will not necessarily agree with a converged solution because the slack bus may not able to balance the generation-load difference within a power system.

A simplified DC power flow evaluation model is proposed in [131] to address cascading scenario with elimination of the numerical inaccuracy with respect to a diverged solution using AC power flow. In our study, we assume that the influence of the power loss in a subsystem is reflected by the loss of active load, which is determined

by accumulating the power loss of each isolated subsystems. A weighting factor w_i is introduced to quantify the impacts of the isolated subsystems based on the entire power system by formulating the ratio of total power loss over the sum of the load consumption which is defined as:

$$\begin{aligned} w_i &= \frac{\Sigma P_{loss,j}}{\Sigma P_D} = \frac{\Sigma P_D - \Sigma P_{d,j} \cdot \phi_j}{\Sigma P_D} \\ &= 1 - \frac{\Sigma P_{d,j} \cdot \phi_j}{\Sigma P_D} \qquad \in [0,1] \end{aligned} \tag{3.12}$$

where i denotes an order of the cases that need to be evaluated in the list and j is the sequential order of subsystems in each case. $P_{loss,j}$ represents the active power loss in the subsystem j. $P_{d,j}$ indicates the outcome of load demand after the linearized power flow evaluation in the subsystem j. The binary function $\phi(\cdot)$ provides results that can be either 0 or 1, representing the convergence status of the subsystem j. The total amount of system load demand ΣP_D is the denominator of the ratio, which is derived from the initial steady-state model before the hypothesized substation outages. A column vector given below corresponds to the maximum length of s:

$$\boldsymbol{w} = [w_1, w_2, \ldots, w_i, \ldots, w_s]^T$$

The flowchart in Fig. 3.5 describes a mechanism to handle subsystem of a hypothetical attack scenario. Notice that in the data initialization, the bus and branch set of

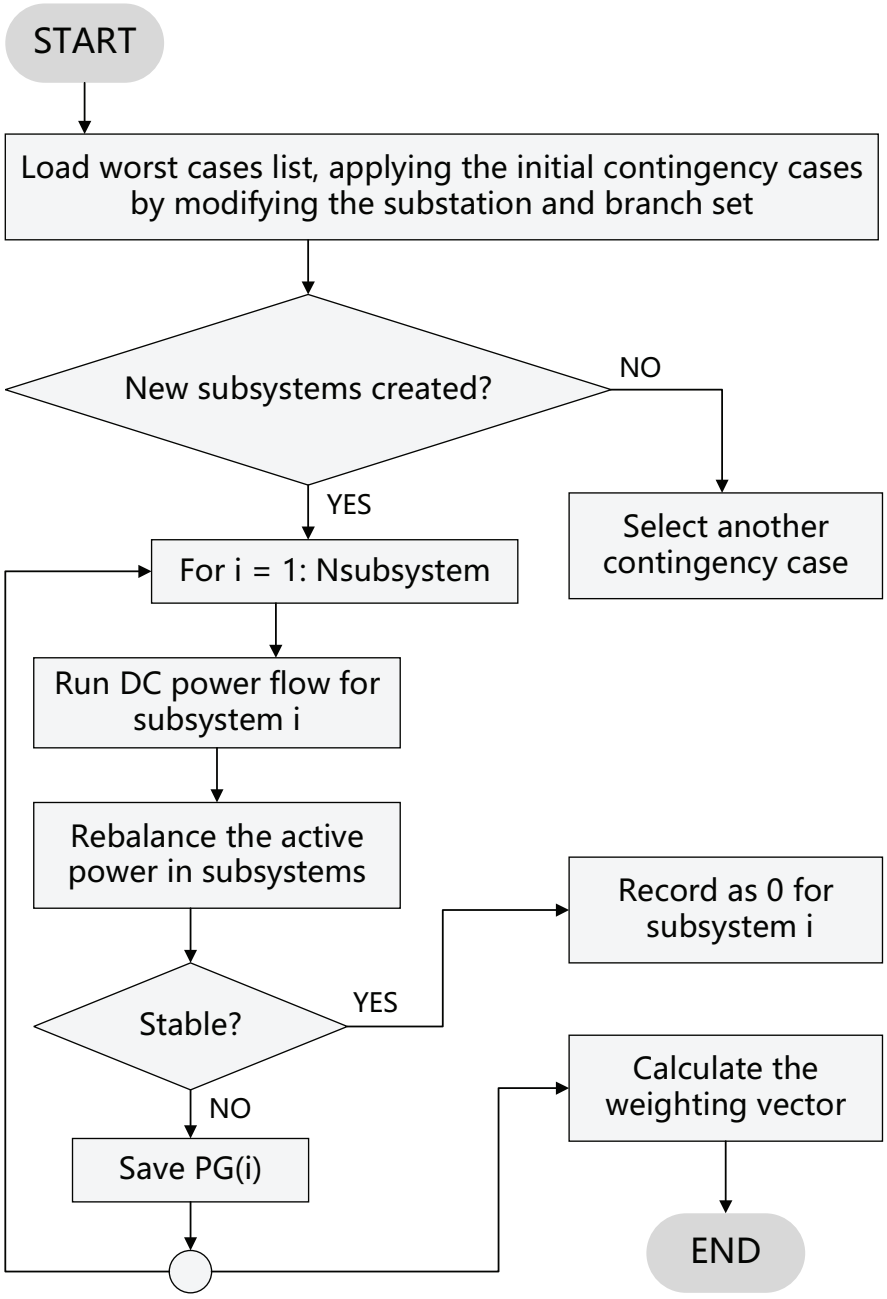

Figure 3.5: Flowchart of islanding identification

the base case need to be modified by removing faulted components according to the hypothesized substation outages. With implementation of power-flow evaluation method, the criteria for determining the operation status of subsystem is defined

by 2 perspectives: the generation-load difference and the ramping-up/down ability of generation units within 1 minute. As depicted in the Fig. 3.5, the proposed weighting vector assesses the impacts of the islanding issue on the entire power system, by separately evaluating the load-generation balance and the portion of active power loss in each isolated subsystem. The weights are directly related to the linearized evaluation outcomes: ϕ and stable load demand of each subsystem $P_{d,j}$, which are decided by the topology of the system and the initial results that we aforementioned in previous chapter after applying the hypothesized contingency cases. Once the topology and initial case are changed, the weighting vector would be renewed with the corresponding updates of worst-case list.

It is assumed that the system is stable when the AGC is able to compensate the difference between generation dispatch and load by changing their active power outputs, otherwise, it requires further investigation with dynamic security analysis, i.e., voltage and frequency stability evaluation. A detailed and elaborative cascading model for a single case may greatly extend the computational time by increasing the complexity of the algorithm because our study is a prospective research with supportive evidence from the evaluations of massive enumerative combinations. The risk index proposed in [25] presumes that each combination has the same weights, which is 1.0. In our study, the risk index is modified by multiplying the weighting factors based on the Eq. 3.12 and obtained weighting vector, as follows:

$$R_m = \begin{cases} 1 \cdot w_{i,m}, & \text{if } k = 1 \\ \frac{N_m \cdot w_m}{N_{b-s} \cdot w_{b-s}} = \frac{\Sigma w_{i,m}}{\Sigma_{i=b+1}^{s} w_i}, & \text{if } k > 1 \end{cases} \tag{3.13}$$

where R_m is the risk index of substation m. N_m is the number of combination in the list $\mathbf{S}$ that contains the specific substation m; w_m is the weighting factor of combination that includes substation m. N_{b-s} and w_{b-s} denote the number of the combinations with the size larger than 1 and the corresponding weighting factors, where b and s are the number of the combinations with size of 1 and the length of the list, respectively. $w_{i,m}$ is the weighting factor of combination containing substation m with the order i in the $\boldsymbol{w}$; k is the size of each combination.

3.4 Cyber-Induced Risk Modeling for Microprocessor Based Relays in Substations

3.4.1 Risk Modeling of Relay Outages

The combinations of the substation criticality have been investigated in the recent years on "bottleneck list" in [25] and [30], which essentially assess the risk level for each substation outage by identifying the cases that are critically-weakened conditions

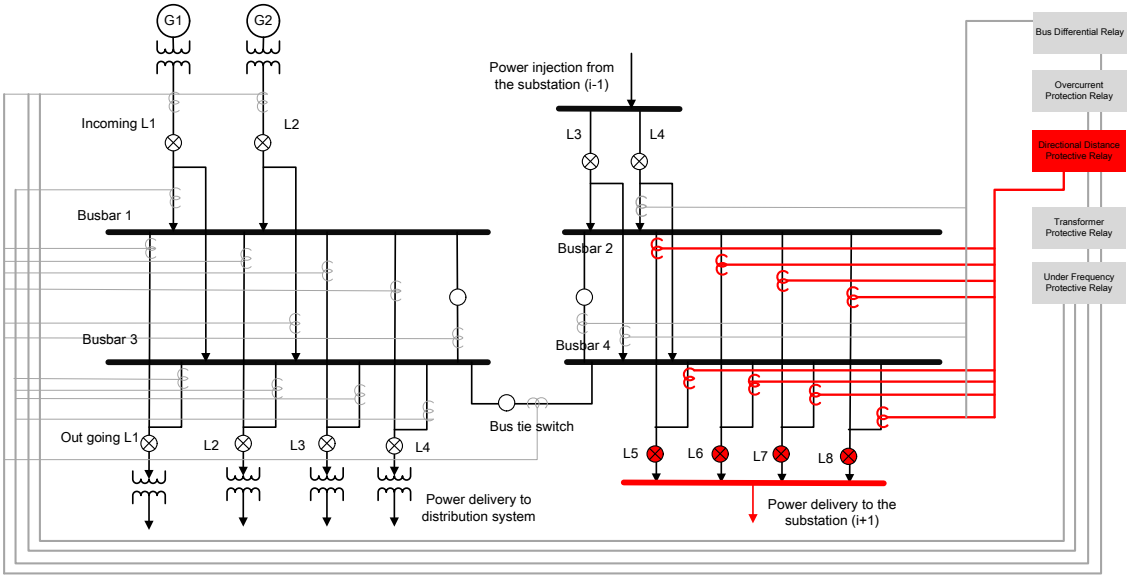

Figure 3.6: Schematic diagram of protective IEDs and the control perimeters within a substation

based on presumed attack scenarios. With the consistent representation of terminology in the definition of "critical" cases, the section extends the modeling of relay outages that can be risky to manipulated that may initiate system-wide instability.

Fig. 3.6 depicts the details of the connectivity relationship between the protective IEDs and their corresponding electrically controlling components in the substation i. Suppose that the substation i has been compromised, the attackers would be able to manipulate single or multiple protective relays. Different relay would generate different outage when it has been compromised. As depicted in Fig. 3.6, if the directional distance relay has been compromised, attackers can manipulate a disruptive switching command to electrically disconnect substation $i+1$, thus other relays may misoperate causing the transmission line $(i, i+1)$ to be de-energized. Similarly, the implications

may occur on other relays within a substation or other regional substations so as the resulting impacts to the power grid operation. In the steady-state analysis, the hypothetical outages of compromised protective relay is treated as the modifications on the relay is equivalent as the electrical modifications on the load demand, power injection, and topology of the power system. For example, the outages of bus differential relay would disconnect all the electrical components from the system, including transmission lines, transformer, lumped loads and generators.

To quantify this problem, the variable $\mathcal{C}_{i,k}$ is introduced to denote the set of the electrical components, including all the lines, transformers, generator units, and loads, which are electronically controlled by the protective IED k, at the substation i. To enumerate all the possible successful cyber intrusions in the substation i, it generates $\sum_{k\in K} 2^{|\mathcal{C}_{i,k}|}$ different consequences, K is the total number of the IEDs in the substation i. In our formulation, we'll assume the attacker would maximize the impacts by disconnecting as many electrical components as possible. Under this assumption, $\mathcal{C}'_{i,k}$ is the most "severe" set that is understudied in the proposed formulation, where $\mathcal{C}'_{i,k} \subset \mathcal{C}_{i,k}$. Derived from the previous studies on the hypothetical substation outages [25], it is observed that the assessment of the digital protective relays is a much more complex problem, which includes a larger number of combinations:

$$\begin{aligned}\mathbb{S} &= \Big(\sum_{k\in K_1} 2^{|\mathcal{C}_{1,k}|}\Big)\cdot\Big(\sum_{k\in K_2} 2^{|\mathcal{C}_{2,k}|}\Big)\cdots\Big(\sum_{k\in K_S} 2^{|\mathcal{C}_{S,k}|}\Big) \\ &= \prod_{i\in S}\Big(\sum_{k\in K_i} 2^{|\mathcal{C}_{i,k}|}\Big)\end{aligned} \tag{3.14}$$

Table 3.1
Results of standard deviation of IEEE test systems

Test systems	$\sigma \leq 1\%$	$1\% < \sigma \leq 5\%$	$5\% < \sigma \leq 10\%$	Total #.
IEEE 30-bus	1	49	34	106
IEEE 39-bus	4	61	47	131
IEEE 57-bus	7	74	71	245
IEEE 118-bus	24	238	121	439
IEEE 300-bus	43	411	354	959

where S is the total number of the substations in the system and K_i is the total number of the IEDs in the substation i. The constant 2 indicates the open or closed status for each scenario of associated IEDs and substations, which implies $2^{|\mathcal{C}_{i,k}|}$ scenarios if IED k is compromised. In our formulation, the most "severe" set $\mathcal{C}'_{i,k}$ is considered for each IED k, which would create K_i different scenarios in total within single substation i. Thus, the Eq. 3.14 can be modified as:

$$\mathbb{S} = 2^{K_1} \cdot 2^{K_2} \cdots 2^{K_S} = \prod_{i \epsilon S} 2^{K_i} = 2^{\Sigma K_i} \tag{3.15}$$

where 2^{K_i} represents the total number of outages of IEDs in substaion i. It is observed that $\mathbb{S}$ is determined by the configurations of IEDs in each substation or the total number IEDs in the system.

The right side of the Eq. 3.15 is the sum of the S-select-k formulation, which is expressed as the designated outages of two or more components/substations and would produce different outcomes with or without considering outages of IEDs. For instance, the S-select-3 problem on the substation outages would enumerate $C_3^{30} = 4,060$ cases

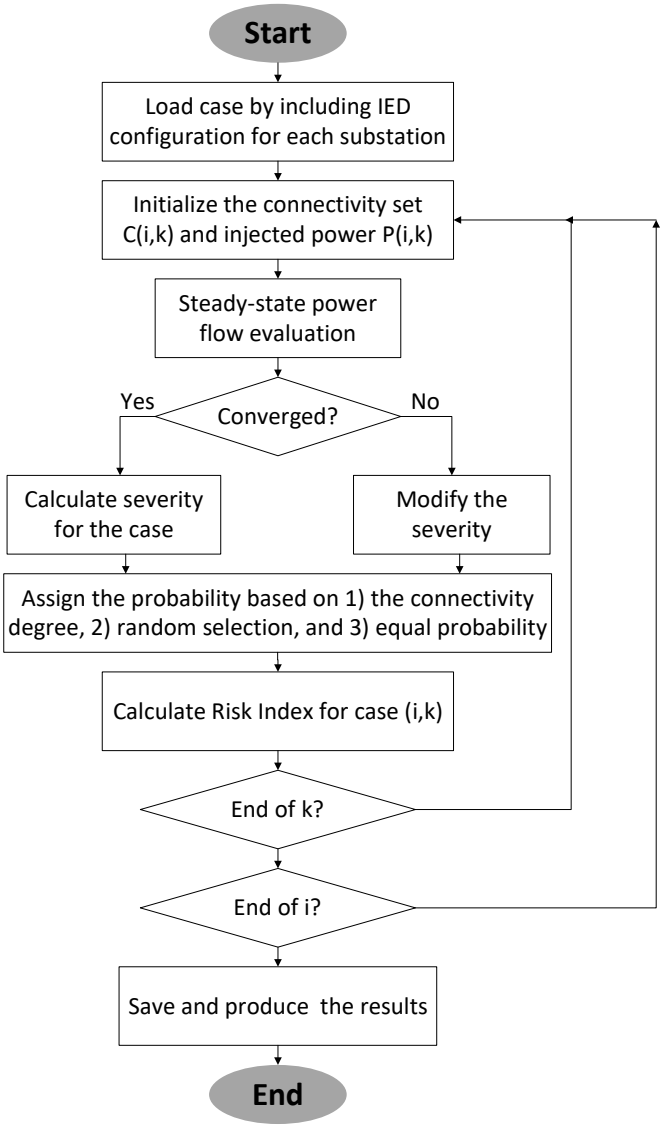

Figure 3.7: Algorithmic enumeration of relay outages

in IEEE 30-bus system. However, from the Table 3.4, it is observed that there are 106 IEDs are evaluated, which would generate $192,920$ scenarios consequently. It's predictable that the number of combinations would be greatly increased when studying larger cases. In this paper, we emphasize on detailing such hypothesized outages

to the device level (the digital relays) to determine the relay outages. Different relay types may result in a consequentially different effect on the system when it's compromised.

3.4.2 Cyber-Induced Impact Assessment

3.4.2.1 Probabilities and combinations

A standard evaluation model for quantifying the risk of the disturbances or the outages is represented by the product of the event probability and its severity [135]:

$$\mathbf{R}_{i,k} = \mathbf{Pr}_{i,k} \cdot \mathbf{Sr}_{i,k} \tag{3.16}$$

where $\mathbf{R}_{i,k}$ is the risk index of the protective IED k at substation i, $\mathbf{Pr}_{i,k}$ denotes the probability of event when the cyber intruder successfully hacks in the substation i and manipulate the protective IED k, consequently, $\mathbf{Sr}_{i,k}$ is the severity of the outages, which, in this paper, is represented using the most "severe" set $\mathcal{C}'_{i,k}$. To simulate probability of the intruding attempts, this paper assigns the probabilities based on

the size of the set $\mathcal{C}'_{i,k}$. The Eq. 3.16 is elaborated as follows:

$$\mathbf{R}_{i,k} = \begin{cases} \frac{|\mathcal{C}'_{i,k}|}{\sum_{k\in K}|\mathcal{C}'_{i,k}|} \cdot \frac{\sum_{i\in S}\sum_{k\in K}|\mathcal{P}_{i,k}|}{\sum_{k\in K}|\mathcal{P}_{i,k}|}, & \text{If diverged} \\ \frac{|\mathcal{C}'_{i,k}|}{\sum_{k\in K}|\mathcal{C}'_{i,k}|} \cdot \frac{|\mathcal{P}_{i,k}|}{\sum_{k\in K}|\mathcal{P}_{i,k}|}, & \text{Otherwise} \end{cases} \tag{3.17}$$

where $\mathbf{Pr}_{i,k} = |\mathcal{C}'_{i,k}| / \sum_{k\in K}|\mathcal{C}'_{i,k}|$ is the probability of the successful intruding attempts towards the protective relay k in the substation i. In the study, it is assumed that an attacker does not acquire the knowledge of the power system and does not have a complete information of the entire power grid. They would enumerate all trials based on the connectivity degrees of the relays that connect more electrical components. These can be represented by $\mathcal{C}'_{i,k}$. The probability is then calculated by measuring the proportion of the size of the "severe" set $|\mathcal{C}'_{i,k}|$ to the sum of the "severe" sets for all the protective relays.

In the Eq. 3.17, the variable $\mathcal{P}_{i,k}$ denotes the total injected power to the substation node i, which are electronically controlled by the relay k. When the intruder successfully compromises the control panel and has the access to the IED k, all the power that is connected to this IED is considered as potential risks. To quantify the outage severity, the power flow evaluation is applied to verify the solutions of the study in which the outcome can be either converged or diverged. For this reason, two different indices are proposed.

In the first scenario, if a solution agrees with a converged result, the severity of the

outage $\mathbf{Sr}_{i,k}$ is determined by calculating the quotient by dividing the injected power that connected to the protective IED k using the total injected power to the substation i, which is represented as $|\mathcal{P}_{i,k}|/\sum_{k\epsilon K}|\mathcal{P}_{i,k}|$. The quotient locates the threshold [0,1]. If the solution is diverged, which suggests that the system can be unstable. Under this scenario, the severity of such event is considered to be much more severe where a potential system-wide blackout would occur. $\mathbf{Sr}_{i,k} = \sum_{i\epsilon S}\sum_{k\epsilon K}|\mathcal{P}_{i,k}|/\sum_{k\epsilon K}|\mathcal{P}_{i,k}|$ is quantified as the severity of the outage. Note that the numerator is the total power injection for the system. The proposed metric assures a comparable larger index than the previous conditions.

3.4.2.2 Sensitivity analysis using standard deviation

To evaluate the performance of the proposed metric, the assigned probability $\mathbf{Pr}_{i,k}$ captures successful intrusion of a given cyber network using pseudo-random numbers. The results of the equal distribution of the probability are given in this problem, in order to initiate a comparison study. The pseudo-random number is calculated through:

$$\mathbf{P}_{i,k} = \frac{\mathbf{P}'_{i,k}}{\sum_{k\epsilon K}\text{rand}(1,K)} \tag{3.18}$$

where $\text{rand}(1,K)$ represents the function that generates an array of random numbers within the interval (0,1), which has length of K. $\mathbf{P}'_{i,k}$ is the k-th elements in the array. The sum of these random number $\mathbf{P}'_{i,k}$ will not necessarily give a 1.0, which

is not acceptable in probability distribution function. The scaling process is given by dividing each random number with the sum of all the random numbers, thus, the modified variable $\mathbf{P}_{i,k}$ is the k-th scaled random number which can be used as the probability assigned to the outage of the relay k in the substation i.

Accordingly, the standard deviation σ is given as the index to assess the performance of the proposed metric.

$$3\sigma_{i,k}^2 = (\mathbf{R}_{i,k}^C - \mathbf{R}_{i,k}^A)^2 + (\mathbf{R}_{i,k}^R - \mathbf{R}_{i,k}^A)^2 + (\mathbf{R}_{i,k}^E - \mathbf{R}_{i,k}^A)^2 \tag{3.19}$$

where $\mathbf{R}_{i,k}^C$ denotes the risk of protective IED k in the substation i using the probability which are derived from the connectivity set $\mathcal{C}'_{i,k}$. Similarly, $\mathbf{R}_{i,k}^R$ and $\mathbf{R}_{i,k}^E$ are the risk indices using probabilities of pseudo random value and equal distribution method, correspondingly. $\mathbf{R}_{i,k}^A$ is the average risk index. $\sigma_{i,k}$ is the standard deviation of protective IED k which is in substation i.

Fig. 3.7 describes the algorithm of the enumerative assessment for the protective relays. The proposed algorithm includes two loops, which include the iteration of power substations and the protective IEDs in each substation.

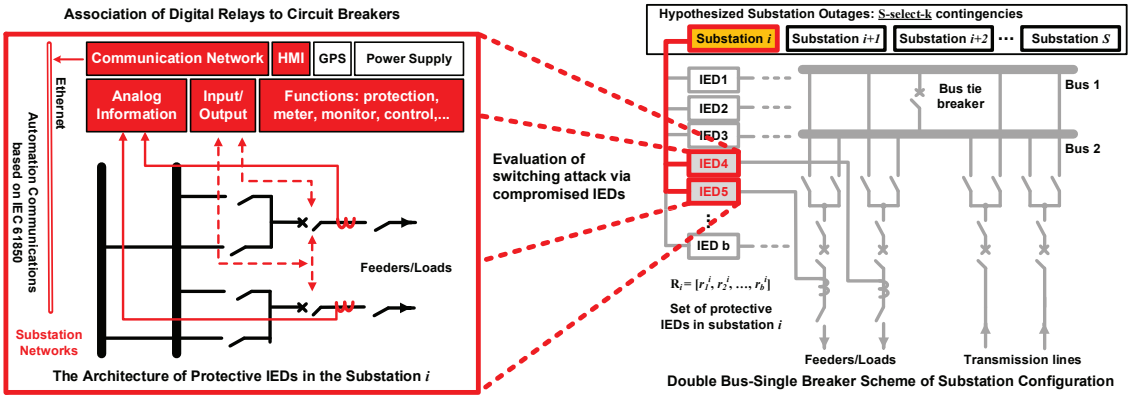

Figure 3.8: The architecture of protective IEDs and possible path enumeration within a substation network by hacking tools

3.5 Cascading Verification Initiated by the Switching Attacks through Compromised Relays

3.5.1 Vulnerabilities of Digital IED Architecture

The information communication technology has been widely deployed on the power system. Digital relays are crucial to power system protection, control, monitoring, and metering function. According to the IEC 61850 standards[136, 137, 138], IEDs are deployed with a robust platform on a local area network (LAN) within a substation based on Ethernet communication. The convenient remote connections allows protection engineers to visualize the connections and relationships between the control functions and the physical components through the human machine interface (HMI). With the support of IEC 61850 standards, the protection engineer is able to

customize the function settings of the relay to meet the specific requirement on the digital relay input and output variables.

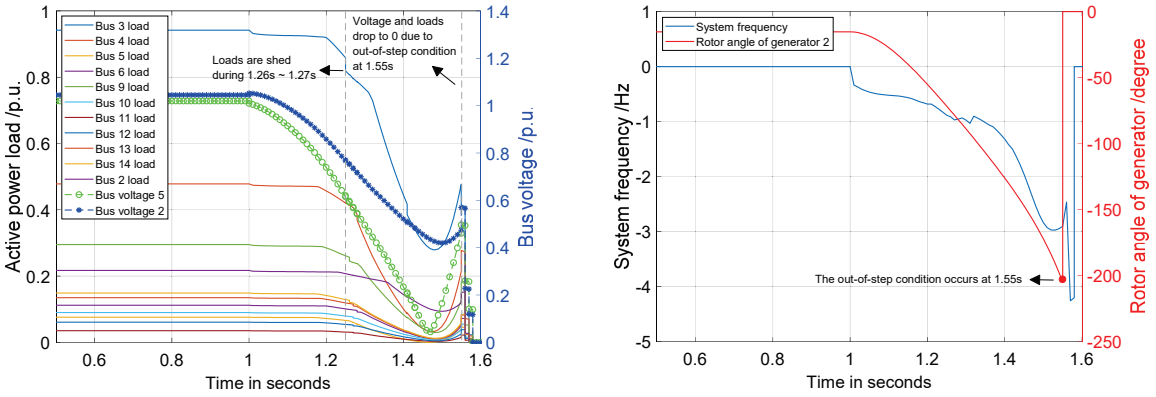

Figure 3.9: The simulation results of switching attack on the distance protection relays on the bus 2 in the IEEE 14-bus system

However, an IP-based protective relay may contain vulnerabilities that can be covertly manipulated by attackers. The 2015 Ukraine attack, for example, exploited remote access to IP-based substation equipment to disconnect busses and then erase the hard drives of that equipment. While the attack was not reported to affect protective relays, it does demonstrate the vulnerabilities of substation equipment to cyber attacks [11]. More recently, the US Department of Homeland Security issued an alert indicating that Russian threat actors were targeting American electric facilities with remote access attacks [139], and an alert indicating that safety equipment at industrial sites had been targeted by a sophisticated remote control attack as well [140]. Available hacking tools, e.g., Shodan, Nmap and Wireshark, can help attackers enumerate all the IP-based devices in an interconnected communication network. These software tools identify nearby devices if they are alive [141, 142, 143]. The vulnerabilities

of remote connectivity to protective relays are summarized in the [144], which are categorized as software security vulnerabilities, network security vulnerabilities, such as denial-of-service (DoS) attacks, system vulnerabilities, and other miscellaneous malware. For example, Fig. 3.8 introduces a possible intrusion scenario that the starts from IED 4 to IED 5 that primarily protects transmission lines and feeders. The S-select-k potential substation outage contingencies are covered in the Fig. 3.8 and have been investigated in previous work [25, 45]. The protective relay outages would be extended as a more complicated combinatorial problem as more relays with diverse functions are deployed on the substations. As shown in the Fig. 3.8, the hypothetical outages initialized by a breaker-switching attack via compromised protective relay b in the substation i is defined as an R-select-k contingency.

3.5.2 Disruptive Switching Attack via Local Digital Relays

Once the attacker successfully compromises the protective equipment, the attacker would be able to maliciously manipulate the circuit breakers, remotely changing the relay settings, which may cause (1) misoperation in the healthy condition or (2) malfunction in a fault condition. The impact of cyberattack on the protective relay is nontrivial and could lead to cascading failure of the system.

Suppose that the IEEE 14-bus system is in a steady-state condition, and the distance

relays on the bus 2 has been compromised, which lead the transmission lines 1-2 and 2-5 to electronically disconnect from the system at 1.0s and 1.2s. Figure 3.9 details the dynamic responses of load, bus voltage, frequency, and the rotor angle difference. It is observed that the initial contingency leads to the decrease of the system frequency, which accordingly result in the loads shed at 1.26s. Over 90% of the loads in the systems decrease rapidly in the following 0.5s. The generators are eventually disconnected at the time of 1.55s because of the out-of-step phenomenon, which may cause the entire system blackout. The results are provided by a time-domain simulation tool named CPAT [145]. Although some protection models such as fault clearing protection models are missing, the major protections which are initiated by voltage change and frequency change are implemented so that the system collapse caused by large frequency and voltage deviations are properly represented in the dynamic model. The malfunction caused by cyberattack would be more severe, compared to the traditional causes. For example, if the relay settings of the underfrequency protection on the loads are maliciously tampered by the attacker, such as intentionally lowering the operating frequency band, such protection would not open the circuit breaker correctly and fail to shed the loads. This would cause more significant frequency drop and the second and the third level of underfrequncy protections are likely to operate, which would eventually increase the size of the brownout, and, in the worst case, i.e. if all generators are disconnected, might lead to a blackout.

3.5.3 Screening the Diverged Cases of Power Flow

The extended enumerations of cyber-based substation outages are established [25, 45], which define the hypothesized substation outages as an S-select-k contingency. As presented previously, the number of the complete combinations of substations is $\sum_{k=1}^{|S|} \mathbf{C}_k^{|S|}$, where S is the substation set.

As shown in the Fig. 3.8, this proposed study extends the previous work to presume switching attack via compromised relays associated with the breakers, i.e. R-select-k contingency. Let $\tilde{\mathbf{R}}$ denotes the set of protective relay in the system, where:

$$\tilde{\mathbf{R}} = \mathbf{R}_1 \cup \mathbf{R}_2 \cdots \cup \mathbf{R}_i \cup \cdots \cup \mathbf{R}_{|S|} \tag{3.20}$$

$\mathbf{R}_i$ is the set of the relays of the substation i, such as:

$$\mathbf{R}_i = [r_1^i, r_2^i, \cdots, r_b^i, \cdots, r_{B^i}^i] \tag{3.21}$$

where r_b^i denotes the b-th protective relay on the substation i. B^i denotes the cardinality of the relay set $\mathbf{R}_i$ of the substation i. Thus, the total number of the relay combination enumerations $\mathbb{S}_R$ is:

$$\mathbb{S}_R = \sum_{k=1}^{|\tilde{\mathbf{R}}|} \mathbf{C}_k^{|\tilde{\mathbf{R}}|} = 2^{|\tilde{\mathbf{R}}|} - 1 = 2^{\Sigma_1^{|S|} B^i} - 1 \gg \mathbb{S}_S = 2^{|S|} - 1 \tag{3.22}$$

$\mathbb{S}_S$ and $\mathbb{S}_R$ denote the total number of enumerations of S-select-k and R-select-k contingencies, respectively. It is obvious that the total number of combination enumerations is greatly increased when the protective relays outages are considered. For example, assume that in a small 10-bus system, 3 protective relays are deployed on each bus. $\mathbb{S}_R$ is 2^{20} times larger than $\mathbb{S}_S$. The evaluation size would be further increased if the coordination behaviours between the protective relays are considered, since the sequential order of the relay operations would significantly increase the complexity of the problem. Note that the relay coordination and the backup protection schemes are not the scope of this study.

3.5.4 Static and Dynamic Validation

3.5.4.1 Modeling of Protective Relaying Outages

The complexity of the enumerations on the protective relaying outages have been introduced in previous sections. Generally, the protective coverage of the multiple relays would be overlapped and it is common to deploy two or more protective relays on the same equipment. The relay deployment and applications of r_b^i can be found in the table 3.2, which details the basic relay fundamentals, applications and electrical components, extracted from the [146]. As shown in the Table 3.2, each substation may deploy numerous relays for single or multiple equipment, which would create an

Table 3.2
The Fundamentals of relay deployments and applications on the substation i

Protection Objectives	Protective systems and typical relays r_b^i (if available)	Electrical Components
Generator	Over/under-frequency relay	Generation unit
	Inverse time overcurrent relay	
	Over/under-voltage relay	
Power Transformer	Transformer percentage differential relay	Transformer
	Inverse time overcurrent relay	
	Overload protection relay	
Transmission Lines	Distance Protection: Three-zone phase fault relay	Transmission lines
Feeders and Loads	Distance Protection: Three-zone phase fault relay	Lumped loads
Bus-bar	Differential protection	Generators Loads Feeders Lines Transformers

extremely large set of relays. It is observed that on the one hand, multiple relays are protecting the same equipment which may cause the same impact to the system; on the other hand, the impact level can also be different varying from the relay to relay. For example, compared with bus differential relay which connects multiple electrical components such as generators, feeders, and transmission lines, the distance protection relay obtains a lower level of impact to the system. This paper introduces a ranking method on each substation to sort and collect the first N relays that acquire higher impacts. It is assumed that these N relays would cover most of the outage scenarios within the substation. By uniting N relays for each substation, to differentiate from $\tilde{\mathbf{R}}$, the relay set $\hat{\mathbf{R}}$ is introduced.

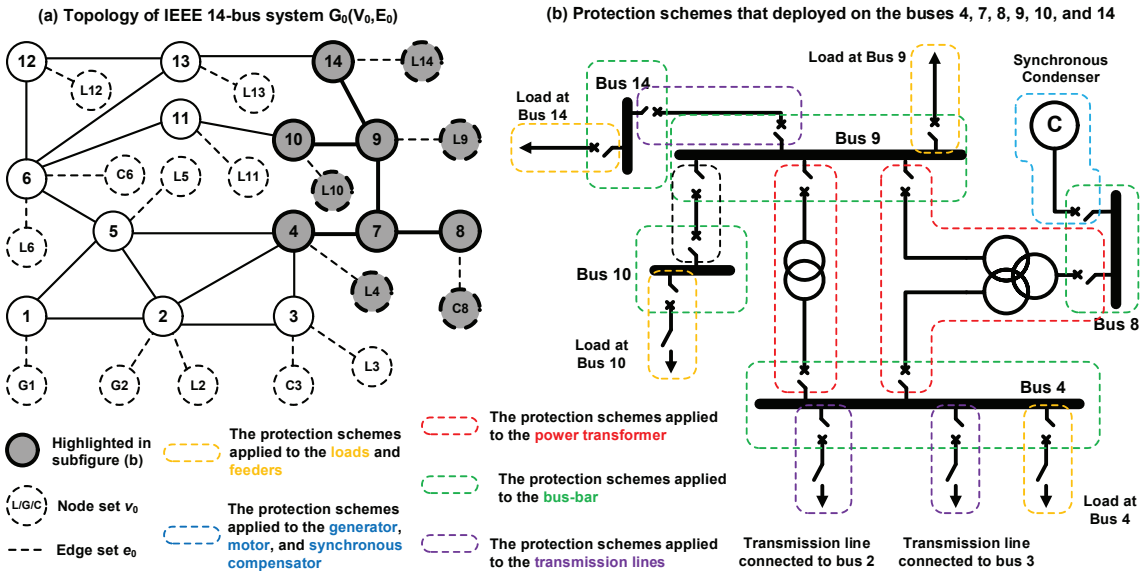

Figure 3.10: The modified topology of the original graph G_0 and the fundamentals of protections deployment in the IEEE 14-bus system

This work applies graph terminologies to perform the algorithm of evaluations on $\hat{\mathbf{R}}$-k contingencies. Let $G(V, E)$ represents the graph topology of the power system, where V and E denote the set of bus nodes and the set of edge. However, the original topology may not be able to represent the deployments of the generators and loads, therefore the set of generator and load nodes v_0 and the corresponding incident set of edges e_0 are incorporated. Thus, the graph $G_0(V_0, E_0)$, where $V_0 = V \cup v_0$ and $E_0 = E \cup e_0$, is introduced to evaluate the protective relaying outages, as depicted in the Fig. 3.10. Figure 3.10 also illustrates the correlation of the various protection schemes and the corresponding electrical components of the buses 4, 7, 8, 9, 10, and 14. The dashed circles with different colors are representing the different electrical components and its corresponding protection zones and relays. The initial event of

compromised relay outages $K(V_K, E_K)$ can be presented in the following equation:

$$\underbrace{G_0(V_0, E_0)}_{\text{(a) initial system } G_0} \xrightarrow[E'(G')=E_0(G_0)\backslash E_K]{V'(G')=V_0(G_0)\backslash V_K} \underbrace{G'(V', E')}_{\text{(b) } \hat{\mathbf{R}}\text{-k contingency}} \xrightarrow[\text{overloading}]{\text{Potential}}$$

$$\xrightarrow[\text{overloading outages}]{E''(G'')=E'(G')\backslash E_L} \underbrace{G''(V', E'')}_{\text{(c) overloading case}} \xrightarrow[\text{validation}]{\text{power flow}} \mathbf{PF}_{failed} \tag{3.23}$$

Equation 4.4 represents the modeling process for protective relay outages, where status (a) denotes the graph topology of the system before the initial event K, (b) denotes the topology after event K with $\hat{\mathbf{R}}$-k relay contingency applied, (c) denotes the topology with overloading implications. It is noticed that any initial event can be represented by the event K with V_K and E_K, once the topology G_0 is produced. E_L denotes the set of the overloading transmission lines, based on the same settings of thresholds in [45]. $\mathbf{PF}(\cdot) \in [0, 1]$ indicates either a converged or diverged outcome, respectively. $\mathbf{PF}_{failed}$ saves the diverged scenarios.

3.5.4.2 Static and Dynamic Verification

Deriving the concepts from the reverse pyramid model (RPM) in [25, 45], this chapter applies an extended enumeration algorithm for identifying the critical relay, which is given in the Fig. 3.11. It is worth noting that the an overload model is also incorporated in the steady-state method to diversify the RPM model. The criteria for tripping the overloading lines are using the model in the [45]. In the static analysis,

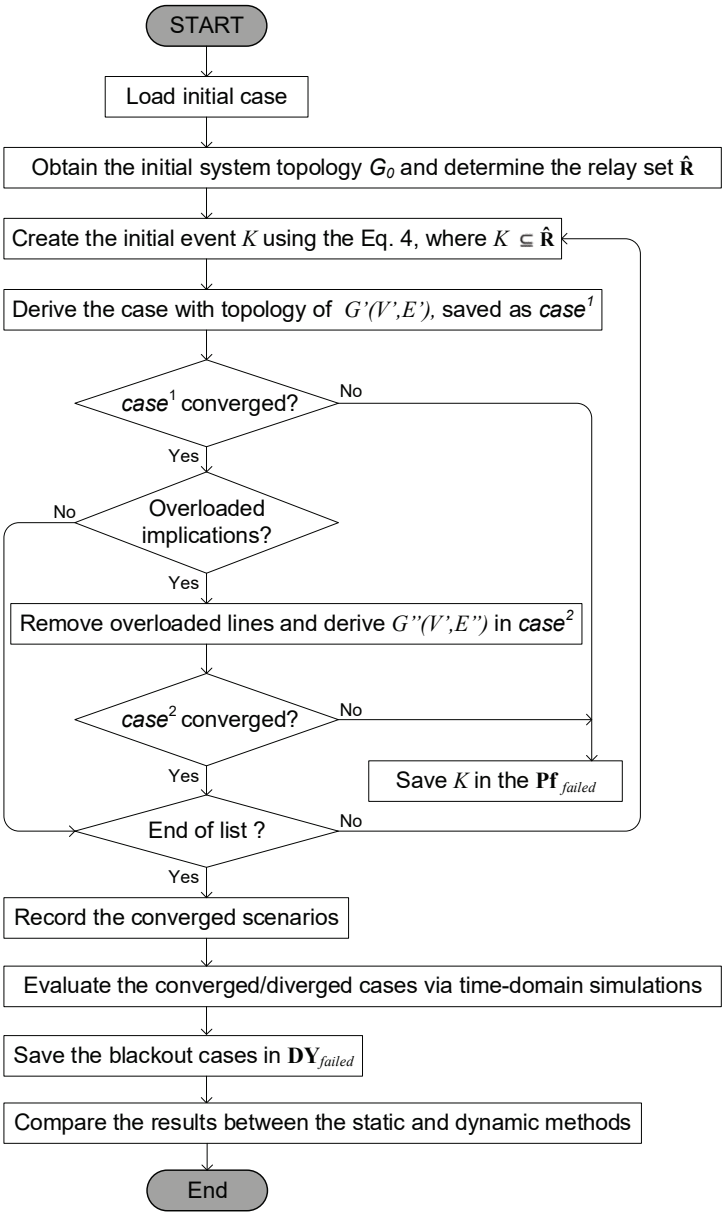

Figure 3.11: Extended enumerations on the identification of critical protective relays within static and dynamic methods

the italic fonts of $case^1$ and $case^2$ denote the system data after the initial event K and the data with overloading implications, respectively. The dynamic time-domain simulation is included in the model to evaluate the consistency performance between the converged combinations from the static simulation and the dynamic simulation. The

loss of load for each scenario is collected to determine the size of the blackout of the each event K and the blackout cases are saved in the $\mathbf{DY}_{failed}$. Based on the results of "worst cases" in the $\mathbf{PF}_{failed}$ and $\mathbf{DY}_{failed}$, the ratio of the verification between the methods can be calculated. Other related electrical quantities, i.e. deviations of frequency and voltage, are also recorded in the final results to further investigate the behaviors of the test system. The risk-based index is also incorporated to evaluate the impact level of each combination of digital relays, which quantifies the impact level of each relay r_b^i [25, 45].

3.6 Simulation Study

The simulation study involves multiple IEEE test cases with 14, 30, 39, 57, 118, and 300-bus systems [147]. A wide range of test systems is used to ensure the consistency of generalization from the study how the cascading outages would affect the outcome of total combinations, based on the expended enumeration algorithm, as well as if the size of a power system relatively may be vulnerability to a small number of hypothesized substations outages.

3.6.1 Test Case Setups and Computational Environment

This section begins with the illustration of IEEE case setup as well as the configuration of the computational platform are set up for the massive enumeration. It is then followed by the simulation results in performance comparisons in terms of size, combinatorial complexity in the earlier level of ks and speed up the improvement with high-performance computing platform. In the section, we assumed modified the risk index metric by $\tilde{R} = .5R$ [25], which indicates the uncertainty between the worst case and benign situation associated with each substation outage. Most IEEE test cases are arranged with a practical substation arrangement with the associated buses for each voltage level, which is implemented with an extra vector to relate bus information in the base case with substation association.

The test case is validated with an implemented algorithm that contrasts the proposed methods in comparison with single and parallel computing modes. The simulations with implications of linearized evaluation are built in the local laptop with specifications of Intel Core i7-5500u in 2.4GHz, with 2 cores, 4 threads, and 8 GB memory installed. In the parallel computing mode, 8 independent worker nodes are aligned. The setup of high-performance computing cluster is built with Rocks Cluster Distribution 6.1.1 in CentOS 6.3, containing 1 front end, 2 login nodes, 3×48 TB RAID60 network-attached storage (NAS) nodes with 33TB usable space, 92 CPU computing

nodes in which each node has 16 CPU cores (Intel Sandy Bridge E5-2670 2.60 GHz) and 64 GB RAM. The simulations in parallel mode are set up with 12 worker nodes. The power flow parameters are set with Newton-Raphson as a default solver for up to 10 iterations. Most IEEE test cases are arranged with a practical substation arrangement with the associated buses for each voltage level, which is implemented with an extra vector to relate bus information in the base case with substation association, e.g., in the IEEE 118-bus system, bus node 25 and 26 are physically connected through a transformation, with an extra generation unit implemented on the node 26. The node 25 and 26 are aligned together as an individual substation, which is denoted as substation 24.

3.6.2 Substation Outages with Overloading Implications

3.6.2.1 Risk Index Comparison

Fig. 3.12 provides several pairs of comparison results of risk index under the condition with and without overloading outages based on IEEE 14-bus, 30-bus, and 39-bus systems. Under the observation of single substation outage on IEEE 39-bus system, the single outage on individual substation 11, 14, 19, 22, and 23 results in power flow diverged, resulting in the highest risk index value of 1.0. This scenario considers with cascading effect denoted by case 1 in the figures. Under the condition without

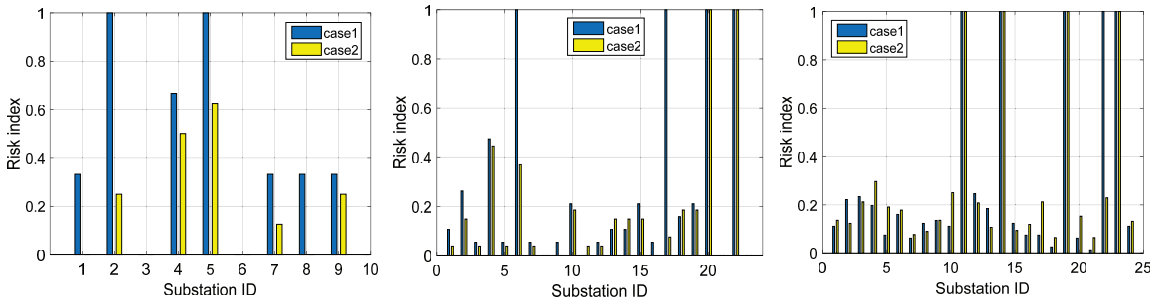

Figure 3.12: Risk index of IEEE systems with 14, 30, 39 nodes from left to right with case 1 to include overloading effect and case 2 without.

cascading failure as case 2, the worst cases for individual substation outages are 11, 14, 19, 23. In IEEE 30-bus system, individual substation outage 6, 17, 20, and 22 are observed with the highest impact under case 1. Only two worst cases are present in case 2. On the smallest size system among the three systems, realizing that either individual substation 2 or 5 results in nonconvergent power flow solution in IEEE 14-bus system acquire under case 1; however, no worst case is present at the level of k = 1 under case 2. It can be concluded that the highest impact of both cases is related as follows:

$$\mathbf{PF}_{failed}(\text{case 2}) \subseteq \mathbf{PF}_{failed}(\text{case 1}) \tag{3.24}$$

where case 1 represents that the simulation is with overloading effect and case 2 without.

3.6.2.2 Identification of S' with Overloading Implications

Table 3.3 lists the statistical details of the enumeration for each level under different IEEE test cases. "# Total Comb." column lists the total number of combinations without elimination at k level. The "# Reduction χ" column shows the number of combinations that has been reduced. "# New" records the number of cases that need to be evaluated in the level k. Column $\mathbf{PF}_{failed} = 1$ indicates the total number of nonconvergent combinations that occurs at each level. The disjoint of each level nonconvergent scenarios can be generalized as follows:

$$\mathbf{SS}_{failed}(k) \bigcup \mathbf{SS}_{failed}(k+1) \cdots \bigcup \mathbf{SS}_{failed}(S'). \tag{3.25}$$

Table 3.3 details the simulation results of the extended enumeration algorithm with the implementation of the overcurrent protection scheme. These are the sets for each level that are exclusive of all to be used for identifying pivotal substations for the investment of cyber infrastructure protection in planning. The simulation results for the 3 IEEE test cases show that the inclusion of cascading effect can increase the number of nonconvergent combinations at the earlier stage of k, which tremendously reduces the combinations at higher k level. Not only this can be massive combinations, a smaller number of combinations would also help to identify critical substations that have nonconvergent solutions.

Table 3.3
Summary of the results of IEEE test systems with implementation of overcurrent protection scheme

Cases #	k	# Total Comb. s_k	# Reduction χ	# New $s_{new,k}$	$\mathbf{PF}_{failed}$ = 1
14-bus	1	10	-	10	3
	2	45	24	21	1
30-bus	1	24	-	24	8
	2	276	156	120	5
	3	2,024	1,593	493	15
	4	10,626	9,354	1,272	17
	5	42,504	40,315	2,189	39
	6	134,596	132,172	2,424	59
39-bus	1	27	-	27	11
	2	351	231	120	30
57-bus	1	43	-	43	18
	2	903	603	300	7
	3	12,341	10,197	2,144	10
	4	123,410	112,594	10,816	21
	5	962,598	922,402	40,196	39
118-bus	1	109	-	109	42
	2	5,886	3,675	2,211	44
	3	209,934	164,673	45,261	347
	4	5,563,251	4,893,480	669,771	3,717
300-bus	1	176	-	176	112
	2	15,400	13,384	2,016	82
	3	893,200	856,221	36,979	274
	4	38,630,900	38,137,765	493,135	2,099
	5	1,328,902,960	1,328,307,418	595,542	111,552

3.6.2.3 Decreasing Ratio ψ

Decreasing ratio is presented in Eq. 3.2, which evaluates the decreasing rate under the extended enumerative evaluation of each testing cases. In Table 3.3, it is noticed that the depth S' for the IEEE 14-, 30-, 39-, 57-, 118-, and 300-bus system are 2, 6, 2, 5, 4,

and 5, respectively. The decreasing ration ψ for the testing systems is calculated as follows: $\psi_{14-bus}(1-2)$ are 100% and 55.56%; $\psi_{30-bus}(1-6)$ are 100%, 43.48%, 21.29%, 11.97%, 5.15%, and 1.80%; $\psi_{39-bus}(1-2)$ are 100% and 34.29%; $\psi_{57-bus}(1-5)$ are 100%, 33.22%, 17.37%, 8.76%, and 4.18%; $\psi_{118-bus}(1-4)$ are 100%, 37.56%, 21.56%, and 12.04%; $\psi_{300-bus}(1-5)$ are 100%, 13.09%, 4.14%, 1.28%, and 0.04%.

The high decreasing rate in larger cases implies that the larger cases include more critical substations, which supply more active power with larger generation and might serve as a 'cut node' that separates the system into several isolated subgrids and agrees with '1' in $\mathbf{PF}_{failed}$ evaluation if they are removed from power system.

3.6.2.4 Nonconvergence and Islanding

This is a two-stage verification with a hypothesized outage of one or more substations as well as its resulting cascade based on the switching attacks. This study is to determine if islanding may occur upon hypothesized outages. Under the observation on the base case of IEEE 57-bus system in Table 3.3, less than 5% combinations require power flow verification. The resultant 95 cases out of 53 499 cases cannot converge with a load flow solution. In contrary on IEEE 118-bus system, 12.413% cases are required power flow verification and 4 150 out of 717 352 cases cannot converge. In IEEE 300-bus cases, over 99.8% cases are filtered out based on the proposed algorithm. There are 1 127 848 cases remaining, which include 114 119

nonconvergent cases. The ratio between $\mathbf{PF}_{failed}$ = 1 and "# New $s_{new,k}$" reflects the effectiveness of identifying worst-case scenarios, which is 12.90%, 2.19%, 27.89%, 0.18%, 0.58%, and 10.11% for all IEEE test systems. The detailed combination solutions and the corresponding ratio ψ are illustrated in Fig. 3.16. The left y-axis value is given as the computation time(s). Figs. 3.13, 3.14, and 3.15 depict the risk index of hypothesized substations at level k = 1 for the cases of IEEE 57-bus, 118-bus, and 300-bus systems, respectively. Compared with the most cases mentioned above, these larger cases are all evaluated with consideration of cascading consequence.

Figs. 3.14 and 3.15 also reflect potential islanding risks. As shown in Fig. 3.14, 54.76% substations out of the combinations at the first level (k=1) has the "worse case" scenarios. The absence of 45.24% substations can implicate islanding instability, i.e., tripping outages that result in excluding transmission lines 8-9, 12-117, 68-116, 71-73, 85-86, and 110-111 out of the system could disconnect bus 9, 10, 117, 116, 73, 86, 87 and 111 from the main grid. At the first level of IEEE 300-bus case, as shown in Fig. 3.15, 60.71% substations are concluded with the highest impacts, bars colored in blue with 39.29% cases can be at risk of potential islanding implication.

3.6.2.5 Computing Performance Analysis

Fig. 3.16 illustrates the results of computing performance of the proposed algorithm with implementation of parallel computing modes. Most cases with less than 30

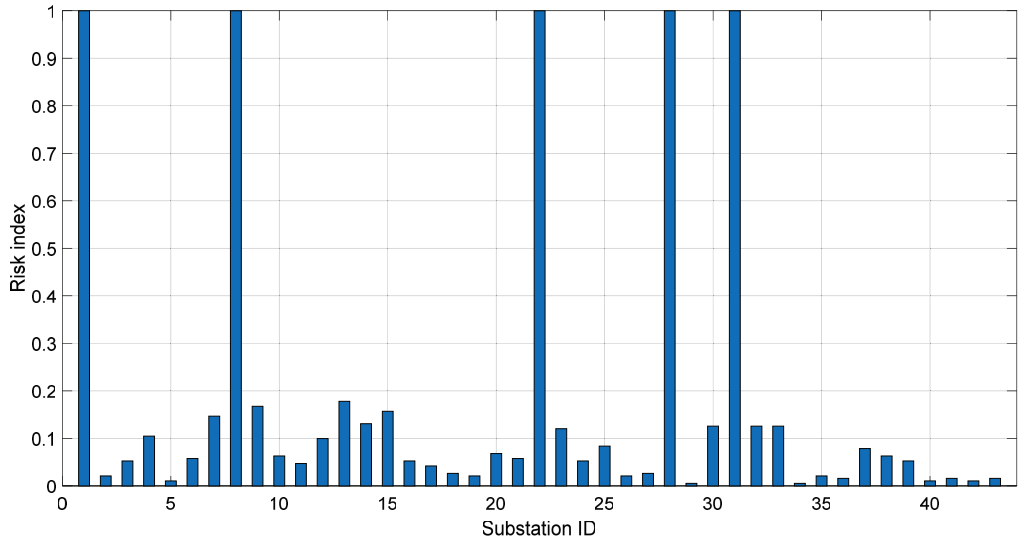

Figure 3.13: Risk index of IEEE 57-bus system

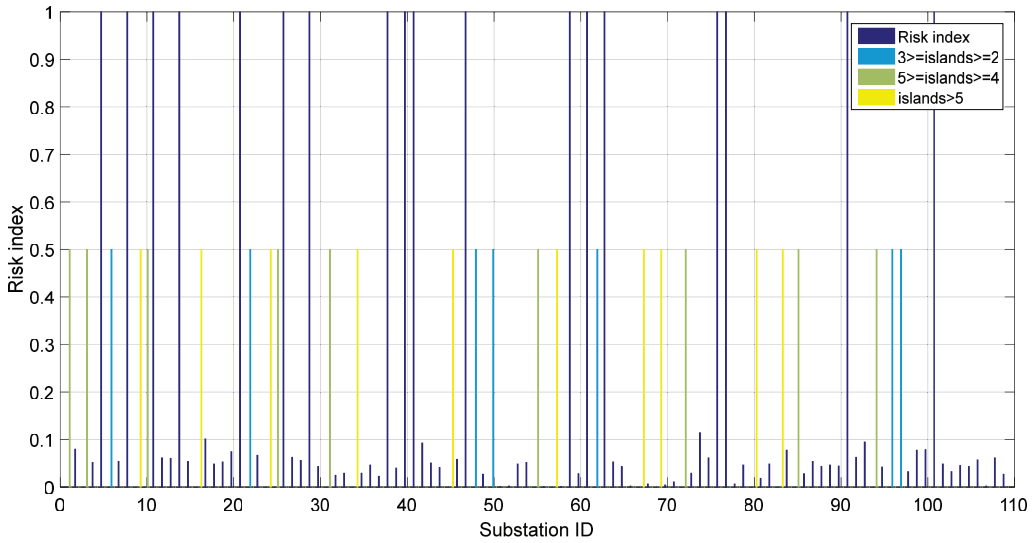

Figure 3.14: Risk index of IEEE 118-bus system

nodes do not make an obvious difference in computation time. It is observed that the computation time is related to the number of the "new" cases during each level k. Additionally, the subtle difference in parallel and series is observed in IEEE 14-bus system. There are two major aspects that may influence this that are based on: (1) the more local workers are assigned, and (2) size of the test cases. The initialization may

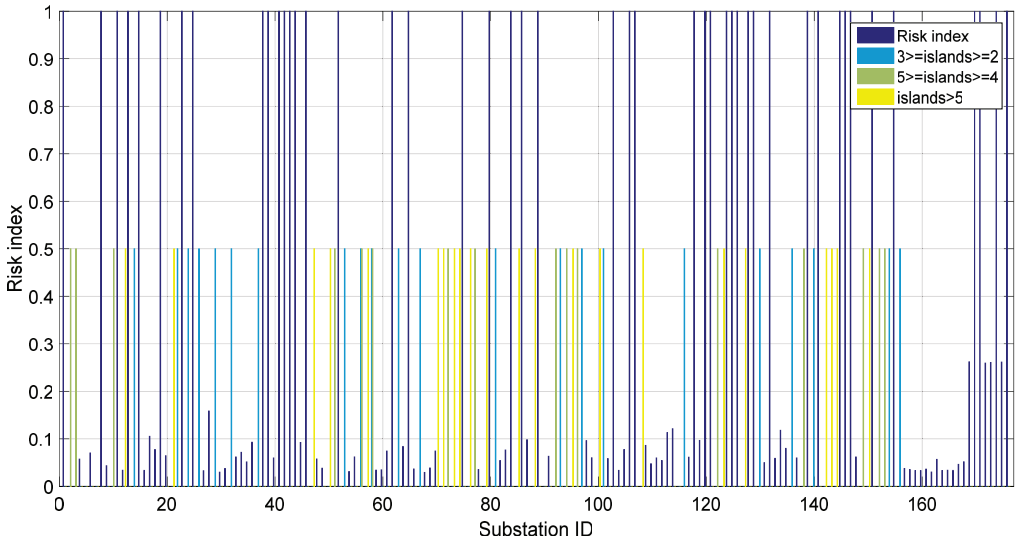

Figure 3.15: Risk index of IEEE 300-bus system

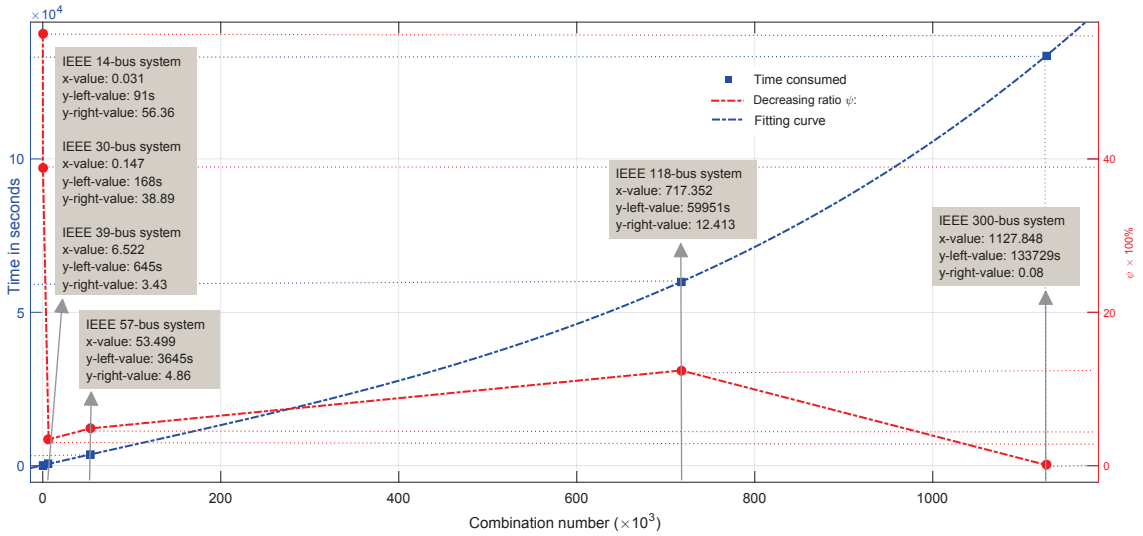

Figure 3.16: Extrapolation of computation time for larger power systems using parallel computing platform

dominate the time elapsed for smaller test cases in parallel mode. The typical time required for initialization can range from 40 to 50 seconds. The variation of estimated time can be random as it all depends upon the state of computing clusters and its availability. In the smaller test cases, there may require hundreds, if not thousands, of

iterations. This implies that the high-performance platform may not be fully utilized. However, in the case of a larger system such as IEEE test systems with 118 or 300 nodes, the computation time in parallelizing the independent combinatorial cases demonstrates a speedup, which requires much lesser than in serial mode. The larger cases demonstrate the effectiveness of utilizing the parallel computing platform.

It is presumed that the computation time elapsed is directly proportional to the number of committed processors in high-performance platform. The allocation of processors is 3 for IEEE 14- and 30- bus systems and 4 processors assigned for the remaining four IEEE test cases, i.e., the systems with 39, 57, 118, and 300 nodes.

By default, the high-performance environment is set to be in multi-processor mode. In consideration of computing resource utilization, the exact number of processors to be assigned is defined by the users. Memory is one critical peripheral of computer system that can affect computing efficiency. In the setting on spatial utilization, the maximum memory used for the IEEE14-bus system is utilized with 3.907GB in series mode and it is 47.155GB for parallelizing. The maximum memory utilization for IEEE 30-bus system is 4.036GB, and 47.402GB, respectively. The IEEE 39-bus system has a slight difference in both modes, i.e., 3.9391 GB in serial mode and 47.376 GB in parallel mode. Finally, for IEEE 118-bus system, there is not a significant bumpup of computing resources with 4.128GB in serial and 49.012GB in parallel. An empirical equation is tentatively approximated to

be Max. $\text{Memory}_{\text{Parallel}} \approx$ Max. $\text{Memory}_{\text{Series}} \times \#$ workers. The proposed estimation equation would be applied to qualitatively extrapolate the possible memory used for larger systems.

A detailed time-consuming performance of the algorithm is provided in Fig. 3.16, which shows an exponentially increasing characteristic with respect to system size using proposed enumerative method. The proposed algorithm extends the testing cases and determines the depth S' by enumerating all the possible solutions and combinations, which may differ the operating time for the various testing systems. The proposed algorithm focuses on the planning study which formulates a quantitative metric to evaluate the risk level for the substations, which may not be necessary to be implemented in real-time assess modules. Additionally, for a larger system, the required computation time could take up weeks that is time-consuming and may not be applicable in online environment.

In Fig. 3.16, it shows a fitting curve of enumerative performance in parallel computing mode with the increase of the combination solution pool for each IEEE testing systems. The proposed algorithm demonstrates the required computation time based on memory utilization and each CPU in the computing nodes at the time. The fitting function of elapsed time $f(x)$, where x denotes the number of evaluated combinations. The parallel computing time can be estimated using $f(x) = (5.47 \times 10^{-5})x^3 + (-1.54 \times 10^{-2})x^2 + (66.314)x - 150.64$ with 95% confidence

bounds and 88.561 of norm of residual. It can be observed that the performance is correlated with system size and the combination pool for each case; however, we noted that the decreasing ratio ψ changes from 56.36% in IEEE 14-bus system to 0.08% in 300-bus system. This ratio ψ can help researcher/operator to quantitatively estimate the testing combination space for a larger system and the extrapolation function will provide a computation estimation in time. The elapsed time of the 300-bus system in serial time is 37.15 hours in which the deviation is 0.55%. The proposed fitting function with parameters can be applied to estimate the required time. This can help planning engineers to expect the time variation based on the size and computing modes, although different topologies with the same size may make a difference. This shows a time reduction of enumeration that is close to 90%. With the estimation function, for 1000 substation system can be extrapolated approximately 30 days.

In summary, this enumerative study introduces a systematic method to quantify cyber-induced contingencies with hypothesized substation outages and incurred overloads. The proposed algorithm is validated through a steady-state evaluation using 6 IEEE test systems (with 14, 30, 39, 57, 118, and 300 nodes). The evaluation is proceeded to ensure the coverage of all critical "worst-case" substations combinations are identified at each level k and the subsets of nonconvergent substations combinations are excluded for $k+1$ level to avoid explosion of combinations. The validation of its application has been greatly extended by incorporating steady-state load flow evaluation and the consideration of islanding formations after presumption of hypothesized

substation attacks. This research also studies with a simplified model of potential cascading by introducing cascaded overloads after the initial cyberattack events. A further possibility of incorporation of cyber-based evaluation of hypothesized outages with dynamic-security analysis shall be investigated for the future work. A comparable analysis towards the simulation performance in between serial and parallel computing modes has been established based on a platform of the superior computing cluster.

3.6.3 Risk Index Modification with Islanding Implications

This chapter investigates the islanding implications based on the results of previous section using IEEE 30-, 39-, 57-, 118-, and 300-bus system. In details, the IEEE 30-bus system is installed 6 generators with 335 MW of total active generation capacity and 189.2 MW of active load. IEEE 39-bus system case contains 7367 MW of total active generation capacity and 6254.2 MW of active load with 10 generators. IEEE 57-bus system is installed with 7 generators with 1975.9 MW of total active capacity and 1250.8 MW of load demand. We presume that the generation adjustment is proceeding within one minute after the initial contingency is applied with the ramping rate as 8% MW/min. The study has simulated 4,130, 1,238, and 6,690 combinations for IEEE 30-, 39-, and 57-bus systems, respectively, based on the proposed enumerative algorithm. The critical lists for IEEE systems are given in table 3.4, table 3.5,

and Fig. 3.17.

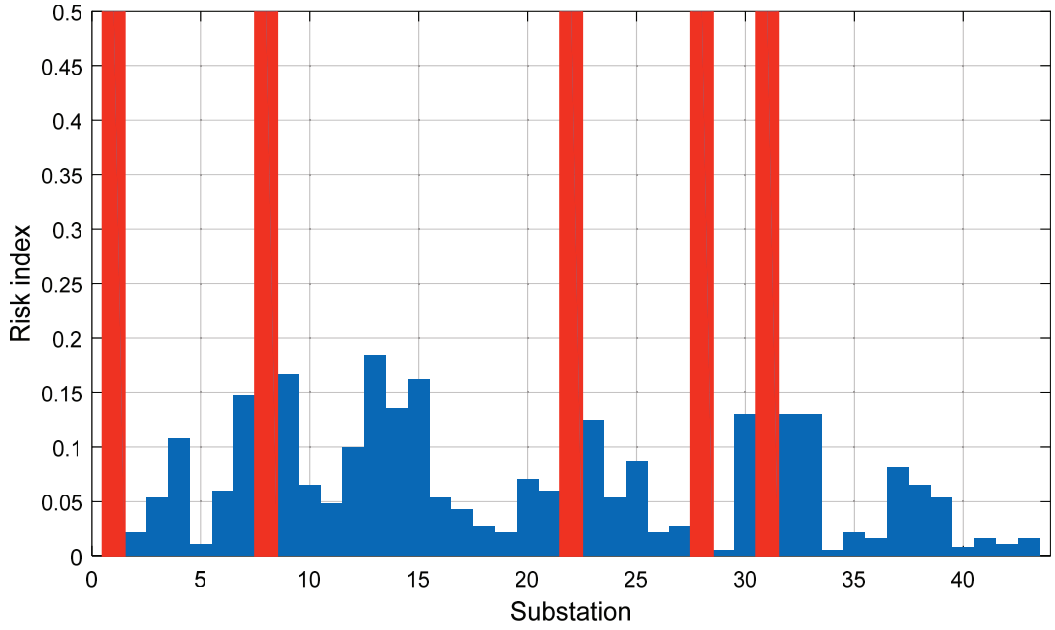

Figure 3.17: Modified risk index of IEEE-57 bus system with islanding implications

Fig. 3.18 displays the number of islands after the evaluation of proposed method based on IEEE 30- and 39-bus cases. The length of the worst-combination list in the testing of IEEE 30-bus system is 23, including 4 combinations with the size of 1, 19 combinations with size of 2. There are 21.74% combinations proved to lead the power grid to split into 2 or more isolated subsystems. In the test of IEEE 39-bus system, the number of combinations in the list is 86, including 5 combinations with the size of 1, 34 combinations with the size of 2, and 47 combinations with the size of 3. Over 54.65% combinations are identified with indications of isolated sub-grids. In the simulation of IEEE 57-bus system, which is drawn in Fig. 3.19, the system contains the 191 combinations in the list. The number of combinations with the size

of 1, 2, and 3 is 5, 95, and 101, respectively. Combinations with 13 worst cases are verified with the islanding scenarios. The modified risk index is drawn in Fig. 3.17, the bar graph colored in red highlights the value of high risk index. Substations 1, 8, 22, 28, and 31 in the IEEE 57-bus system are verified to acquire a high risk index.

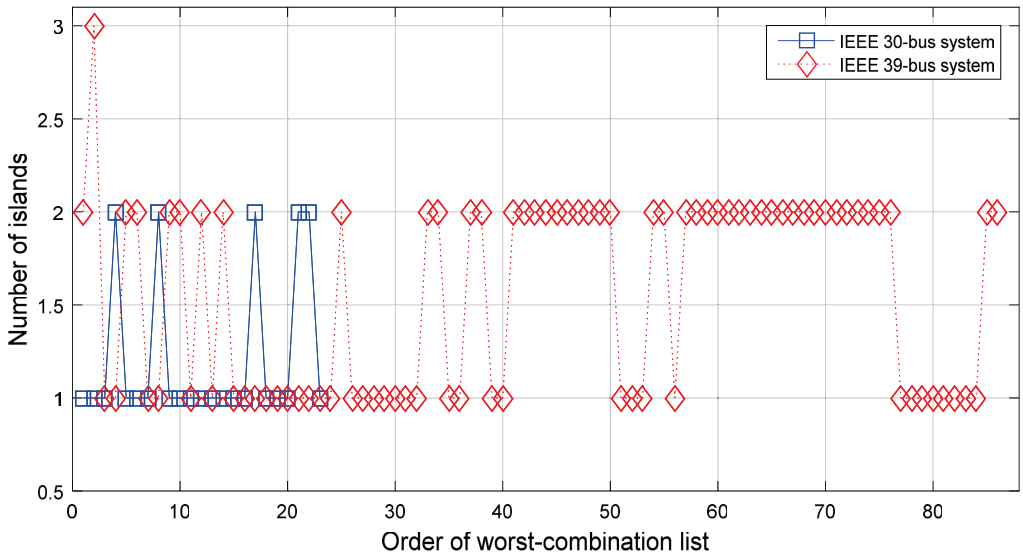

Figure 3.18: The number of islands in IEEE 30- and 39-bus systems in accordance with the order of worst-combination list

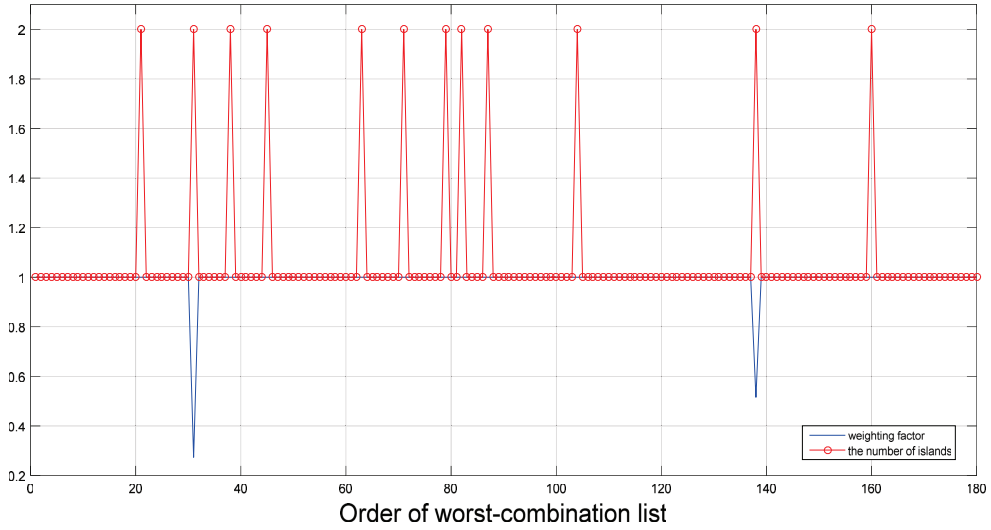

Figure 3.19: The weighting vector and the number of islands in IEEE 57-bus system

Tables 3.4 and 3.5 are the results of comparison between the risk index for cases with and without islanding using IEEE 30- and 39- bus system, respectively. The fourth column in each table records the difference between the value of risk index with or without islanding implications. The colored rows annotate the substations whose risk indexes are modified. The rows in blue, yellow, and green denote the difference that falls within 40%, 40-50%, and over 50%, respectively. It can be observed that the corresponding substations (4, 13, 14, 19, 22) have been corrected, and 4 out 5 substations changed within 40% and the risk index of substation 22 declines by 84.71%. When applying the initial outage of substation 22, the system is islanded into 2 subsystems. Subsystem 1 contains the active load of 162.3 MW and 13 MW for subsystem 2; however, no generation unit is assigned for subsystem 2, which directly leads the subsystem 2 into blackouts. After adjusting the generation-load imbalance of 13.9 MW, the subsystem 1 reaches a stable status of load shedding with the amount of 13.9 MW and a total loss of 15.4 MW.

Table 3.5 details two critical lists of IEEE 39-bus system with the comparison between the cases with and without islanding implications. In the table, it is concluded that the risk indexes of 59.26% substations have been modified with proposed method for assessing the risk of isolated subsystems. 12 substations have been modified with around 40% of dropping and risk indexes for these 4 substations (4, 12, 21, and 23) have been decreased with over 55% rate. When testing an initial contingency of hypothesized outage of the substation 23, the system is split into 2 subsystems.

Table 3.4
Comparison of risk index with and without islanding on IEEE 30-bus system

Substation Order #	Risk index in case with islanding	Risk index in case without islanding	Differece in percent.
1	0.1053	0.1053	0.00%
2	0.2632	0.2632	0.00%
3	0.0526	0.0526	0.00%
4	0.3901	0.4737	17.65%
5	0.0526	0.0526	0.00%
6	1.0000	1.0000	0.00%
7	0.0526	0.0526	0.00%
8	0	0	N/A
9	0.0526	0.0526	0.00%
10	0.2105	0.2105	0.00%
11	0	0	0.00%
12	0.0526	0.0526	0.00%
13	0.0653	0.1053	39.70%
14	0.0653	0.1053	39.70%
15	0.2105	0.2105	0.00%
16	0.0526	0.0526	0.00%
17	1.0000	1.0000	0.00%
18	0.1579	0.1579	0.00%
19	0.1269	0.2105	39.71%
20	1.0000	1.0000	0.00%
21	0	0	N/A
22	0.1529	1.0000	84.71%
23	0	0	N/A
24	0	0	N/A

Subsystems 1 and 2 involve 5625.7 MW and 489.5 MW of active load respectively, and both subsystems 1 and 2 have been reached a new separate stable point.

For another example, when applying the initial hypothesized outage of substation 14, which is align with bus node 16, the system is divided into 3 parts by removing the fault branches 15-16, 16-17, 16-19, 16-21, and 16-24. Subsystem 1 is containing 28

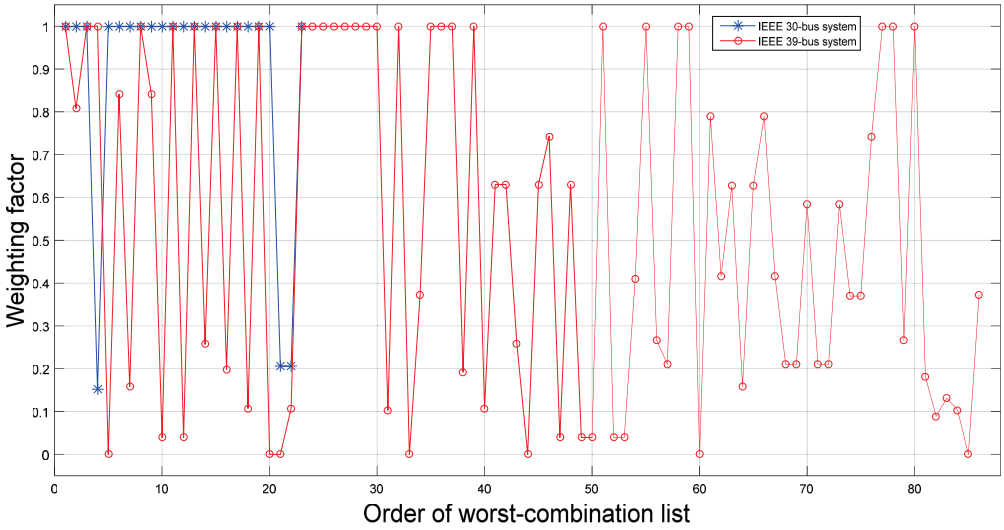

Figure 3.20: The weighting factor of IEEE 30- and 39-bus system in accordance with the order of worst-combination list

bus nodes which involves 6 generators with injection of 3947.9 MW of active power; Subsystem 2 is constituted by the nodal set [21, 22, 23, 24, 35, 36] and 2 generators are assembled on the node 35 and 36 with 1210 MW generation capacity; Subsystem 3 is composed of the bus set [19, 20, 33, 34] and installed 2 generators equipped with 1140 MW of power supply. Under the verification of the proposed assessing method, only subsystem 2 is validated to be able to reach a new stable point by ramping down 379.9 MW of generation power.

It is noted that the index value of substation criticality has dropped from the highest level (non-convergent solution for the power flow evaluation, $R_m = 1$) to the acceptable level ($R_m = 0$). When applying a hypothesized outage on substation 23 on IEEE 39-bus system, the substation is presumably disconnected, resulting in branches 25-26, 26-27, 26-28, and 26-29 are electrically disconnected. The system is split into 2

Table 3.5
Comparison of risk index with and without islanding on IEEE 39-bus system

Substation Order #	Risk index in case with islanding	Risk index in case without islanding	Differece in percent.
1	0.0708	0.1111	36.27%
2	0.1400	0.2222	36.99%
3	0.1385	0.2346	40.96%
4	0.0858	0.1975	56.56%
5	0.0741	0.0741	0.00%
6	0.1605	0.1605	0.00%
7	0.0617	0.0617	0.00%
8	0.0852	0.1235	31.01%
9	0.0772	0.1358	43.15%
10	0.1111	0.1111	0.00%
11	1.0000	1.0000	0.00%
12	0.1100	0.2469	55.45%
13	0.1071	0.1852	42.17%
14	0.8079	1.0000	19.21%
15	0.0749	0.1235	39.35%
16	0.0467	0.0741	36.98%
17	0.0741	0.0741	0.00%
18	0.01479	0.0247	40.49%
19	1.0000	1.0000	0%
20	0.0617	0.0617	0.00%
21	0.0024	0.0123	80.49%
22	1.0000	1.0000	0
23	0	1.0000	100.00%
24	0.0491	0.0111	55.81%
25	0.0247	0.0247	0.00%
26	0.0741	0.0741	0.00%
27	0.0969	0.1358	28.65%

subsystems: subsystem 1 consists of 9 generating units up to a total of 5467.9 MW, where subsystem 2 has a total generation of 830 MW. With these generating units in those two islands, they are able to reach a stable condition by ramping up the output of 157.9 MW in subsystem 1 but requires to shed the load with the amount

Profile Summary

Generated 13-Feb-2017 15:49:31 using performance time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
riskmodify118	1	48.953 s	0.821 s	
mpoption	1953	39.400 s	8.700 s	
rundcpf	976	18.999 s	0.067 s	
mpoption>mpoption_default	2930	17.155 s	13.197 s	
mpoption>mpoption_optional_fields	1953	10.405 s	8.093 s	
nested_struct_copy	69338	5.992 s	5.661 s	
runpf	977	2.810 s	0.441 s	
submodify118	976	2.204 s	1.404 s	
Subtest118	973	2.059 s	1.170 s	
have_fcn	75199	1.762 s	1.599 s	
unique	20331	1.265 s	0.718 s	
find_islands	973	1.254 s	0.148 s	
connected_components	976	1.097 s	1.097 s	
union	5857	0.905 s	0.202 s	
ext2int	977	0.860 s	0.534 s	
int2ext	977	0.795 s	0.254 s	
union>unionR2012a	5857	0.703 s	0.204 s	
unique>uniqueR2012a	20331	0.547 s	0.547 s	
mpoption_info_fmincon	6836	0.510 s	0.247 s	
i2e_field	977	0.431 s	0.055 s	
i2e_data	1954	0.376 s	0.115 s	
get_reorder	6113	0.355 s	0.355 s	
mpoption_info_intlinprog	6836	0.345 s	0.193 s	
mpoption_info_quadprog	6836	0.345 s	0.194 s	
deal	78126	0.342 s	0.342 s	
mpoption_info_linprog	6836	0.338 s	0.194 s	
e2i_field	977	0.311 s	0.039 s	
mpoption_info_clp	6836	0.307 s	0.119 s	

Figure 3.21: The time-consuming performance of algorithm for IEEE-118 bus system

Profile Summary

Generated 13-Feb-2017 14:17:37 using performance time.

Function Name	Calls	**Total Time**	Self Time*	Total Time Plot (dark band = self time)
riskmodify300	1	7316.722 s	0.584 s	
parallel_function	1	7315.532 s	0.112 s	
parallel_function>distributed_execution	1	7315.193 s	0.088 s	
...>remoteparfor.getCompleteIntervals	11	7315.021 s	5.119 s	
java.util.concurrent.LinkedBlockingQueue (Java method)	7276	7304.555 s	7304.555 s	
remoteparfor>remoteparfor.displayOutput	7276	5.207 s	2.323 s	
remoteparfor>iDisplayStringArray	7277	1.594 s	1.594 s	
...ox.distcomp.pmode.DrainableOutputImpl (Java method)	7277	0.924 s	0.924 s	
...x.distcomp.pmode.ParforControllerImpl (Java method)	7316	0.384 s	0.384 s	
mpoption	1	0.321 s	0.021 s	
runpf	1	0.282 s	0.128 s	
mpoption>mpoption_default	2	0.279 s	0.038 s	
have_fcn	47	0.195 s	0.038 s	
parallel_function>iMakeRemoteParfor	1	0.189 s	0.002 s	
remoteparfor>remoteparfor.remoteparfor	1	0.186 s	0.100 s	
ver	4	0.145 s	0.002 s	
ver>locGetSingleToolboxInfo	4	0.143 s	0.023 s	
mpoption_info_fmincon	4	0.118 s	0.001 s	
...hworks.toolbox.distcomp.pmode.Session (Java method)	7281	0.092 s	0.092 s	
serialize	36	0.078 s	0.017 s	
deserialize	34	0.047 s	0.028 s	
int2ext	1	0.039 s	0.019 s	
ext2int	1	0.037 s	0.023 s	
remoteparfor>remoteparfor.addInterval	27	0.035 s	0.005 s	
cell.intersect	4	0.034 s	0.005 s	
nested_struct_copy	42	0.032 s	0.031 s	
cell.strcat	8	0.031 s	0.029 s	
mpoption_info_clp	4	0.030 s	0.020 s	

Figure 3.22: The time-consuming performance of algorithm for IEEE-300 bus system

of 340 MW in subsystem 2. Thus, the weighting factor for hypothesized outages on substation 23 should be assigned a zero value.

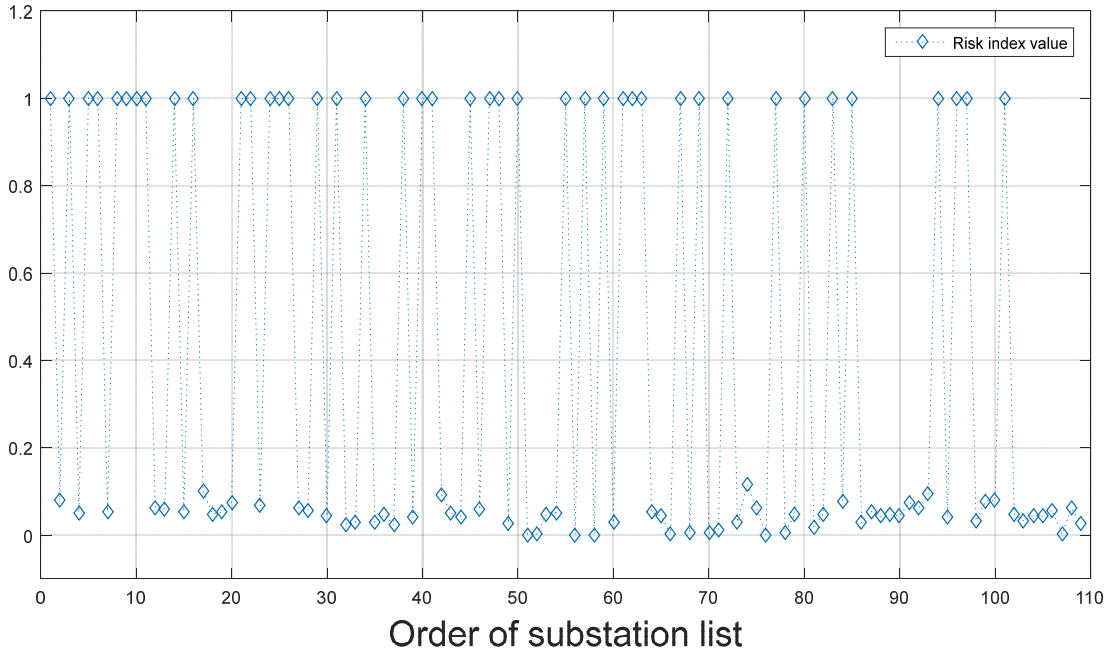

Figure 3.23: Modified risk index of IEEE-118 bus system with islanding implications

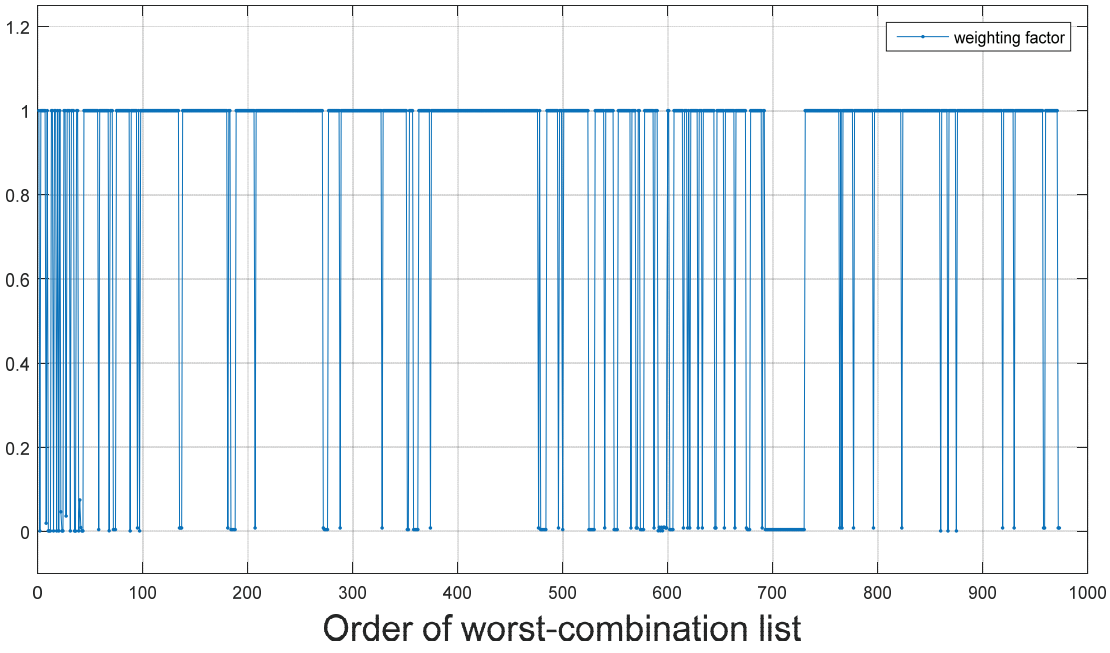

Figure 3.24: Weighting factor of IEEE-118 bus system

Fig. 3.20 depicts two weighting vectors for IEEE 30- and 39- bus cases. In the IEEE 30-bus system, it is the subtle amount we notice that only a few substations (5 out of 24) require adjustment of risk values based on the islanding conditions. The sum of the weighting factor in the system is 20.56 with the small fraction of 10.6% decrease compared with the case without islanding implications; in the IEEE 39-bus system, over half of risk indexes of substations (16 out of 27) are modified with proposed evaluation method. The Σw_i is 46.24 with over 46.22% amount of weighting factors are decreased compared with the case without implication of islanding issue. For example, in the Table 3.5, the risk index of substation 12 is 0.2469 in the case without islanding implications and there are totally 20 combinations with equal weighting factor 1 because any one of combinations will cause the whole system into a system-size blackout. When applying the proposed metric, 10 out of these 20 combinations could cause the power grid split into several subsystems, which may cause the weighting factor less than 1 once the subsystem is verified to be able to reach a new stable point when the rebalance is completed through generation adjustment or load shedding.

Fig. 3.24 represents the simulation results of the weighting factors in the IEEE-118 bus case. The total active generation capacity installed in IEEE-118 bus system is 9966.2 MW and the load in the system is 4242 MW. 54 generation units are assigned in the test case with 17 active generation injection nodes and 34 reactive compensation nodes. According to the Table 3.3, the total number of the worst-case scenarios in the extended enumeration method in each level is 973 with 44 cases, 93

cases, and 836 cases in the level k = 1, 2, and 3 respectively. In the level k = 1, 44 single-substation outages are detected in the extended enumeration evaluation with overloading implications, whose risk index is 1.0, however, the weighting factors for over 45.4% single-substation cases are less than 0.1. For example, when removing substation 76, which associates with bus node 85, the system is split into 2 subsystems. Small subsystem contains bus node (86,87) and larger subsystem contains other bus nodes except bus node 85. 4 MW active power loss is detected in the separation. Additionally, when the substation 91, which associates with bus node 100, is removed from the system because of the hypothesized outages, the line 92-100, 94-100, 98-100, 99-100, 100-101, 100-103, 100-104, and 100-106 are electrically disconnected from the system. An island containing substation (103, 104, 105, 106, 107, 108, 109, 110, 111, 112) has been formed with 76 MW of active power generation installed. The weighting factor of substation 91 outages reduces from the 1.0, which represents the necessary blackouts of the system if substation 91 compromised, to the 0.0744 within safety lower level because the islands-stability evaluations validate that the one of the subsystems will be able to reach to a new stable status through regulating the active generation outputs. The modified risk index is given in Fig. 3.23. The computing time for enumerating all the 973 cases is 48.95 seconds in the serial model with 1 computing core, 1 worker, and 1209 MB memory usage.

The details of time performance of the algorithm for IEEE 118-bus system is given in Fig. 3.21, which is provided by MATLAB (R2015b, version: 8.6.0.267246), in a

descending order with total computational time. "riskmodify118" is the main function that is called once and enumerates all the worst-case substation list derived from the previous results. "mpoption" is a control function that determines the status of the systems, which is provided by MATPOWER, incorporating with "submodify118" and "Subtest118" , which remove the hypothesized substations and update the topological status of testing cases by modifying the bus, generation, and branch sets.

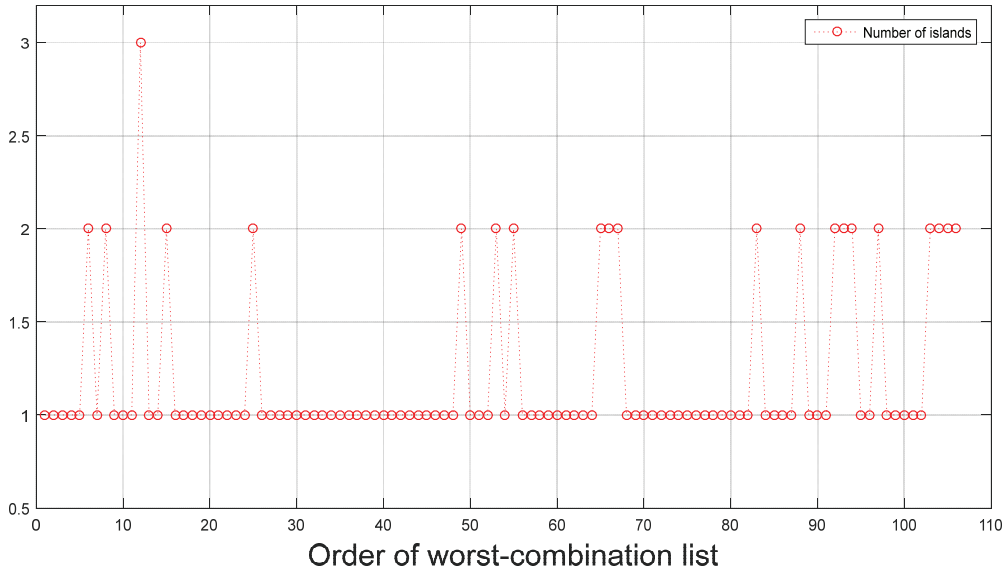

Figure 3.25: The number of islands in worst-case list of IEEE-300 bus system

IEEE 300-bus system includes 176 electrical substations with 23935.4 MW of power generation and 7983 MVAr of reactive power. 69 generators are installed in the system. Fig. 3.25 lists the number of islands in the worst-case substation list of IEEE 300-bus system for the level $k = 1$, which contains 106 cases. According to the Table 3.3, there are 348,367 worst-case combinations need to be tested through the proposed method. For example, when applying the substation outages on the substation of 11,

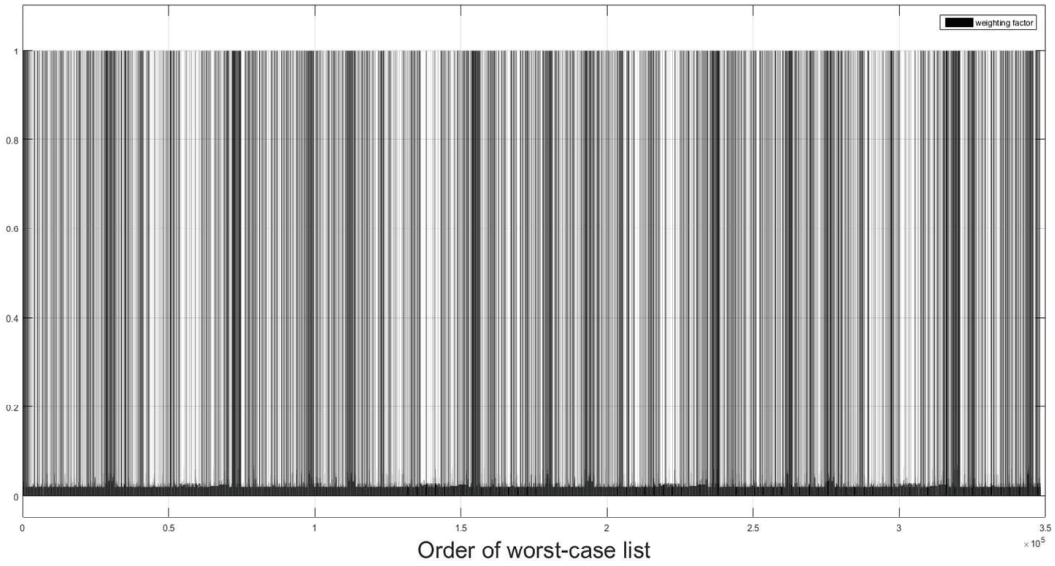

Figure 3.26: Weighting factor of IEEE 300-bus system

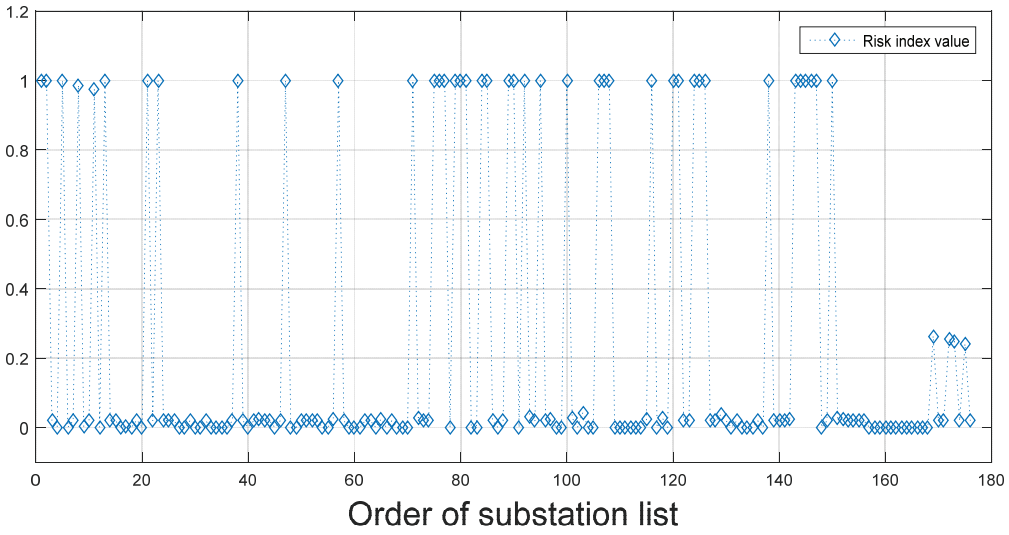

Figure 3.27: Modified risk index of IEEE 300-bus system with islanding implications

which associates the bus nodes(20, 21), branches 13-20, 20-27, 20-23, 21-12, 21-19, and 21-24 are electrically disconnected from the power system, which directly forms a small islands containing bus nodes(22, 23, 24, 25, 26, 27, 320,7023, 319, 7024) with generation capacity of 595 MW installed.

Fig. 3.26 details the weighting factor of IEEE 300-bus system with the ramping rate of 250 MW/minute. As described in the Table 3.3, 348,367 cases are enumerated in this simulation. All the value recorded in the figure are limited in the [0,1] based on the definition of 3.12. 197,397 worst-case combinations are modified and 43.34% cases appear high-risk value (1.0) after the evaluation. The modified risk index are given in the Fig. 3.27, 23.30% substations display the high-index risks of potential system-size blackouts if they were complete compromised. For example, substation 1 associates 6 bus nodes (1, 7001, 2, 7002, 3, 7003) and 5 power transformers and 3 generation units with the capacity of 2300 MW, which is tested to be able to cause the instability to the system through power flow evaluation with implications of islanding and overloading. We can conclude that the substation 1 serves as a pivotal substation that may need a larger investment and implementation of the high-priority protection scheme. Fig. 3.22 details the programming performance with descending order of time-costing. The parallel computing toolbox is implemented in the main script which uses all 2 computing cores and 4 threads within 8 worker nodes. The total computing time is 7,316 seconds which saves 78.66% time compared with serial computing mode, which costs 14 hours.

3.6.4 Probability-based Results of Hypothesized Relay Outages

This study is validated using IEEE test systems. IEEE 30-bus system contains 6 generation units and 20 loads, which generate 191.6 MW power to the system and consume 189.2 MW power respectively. IEEE 39-bus system contains 9 generation nodes and 21 loads are connected to the system. 12 power transformers are connected to the system. It is observed that 6297.9 MW power is injected into the system and 6254.2 MW power is dispatched to the loads. IEEE 57-bus system is installed with 17 transformers and 7 generation units, which supply 1278.7 MW to the grid. The fixed 42 loads consume 1250.8 MW power in total. IEEE 118-bus system contains 54 generation units, 99 fixed loads, and 9 power transformers. The total power injection to the grid is 4374.9 MW and the total load consumption is 4242 MW power. 69 generators are installed in the IEEE 300-bus system with 23935.4 MW power supply and 201 loads totally consume 23525.8 MW of power. For each IEEE test case, it is initialized with five default protective relays in each substation, which are directional overcurrent relay, bus differential relay, directional distance relay, under frequency relay, and transformer relay. For different bus type and configuration, the set of protective relays will diversify. It is noticed that the in the Eq. 3.17, the diverged solution would give a comparably higher value than the converged solution, in this

section, in order to explicitly identify the "worst" cases, all the risk indices of diverged solutions are modified to 1.0.

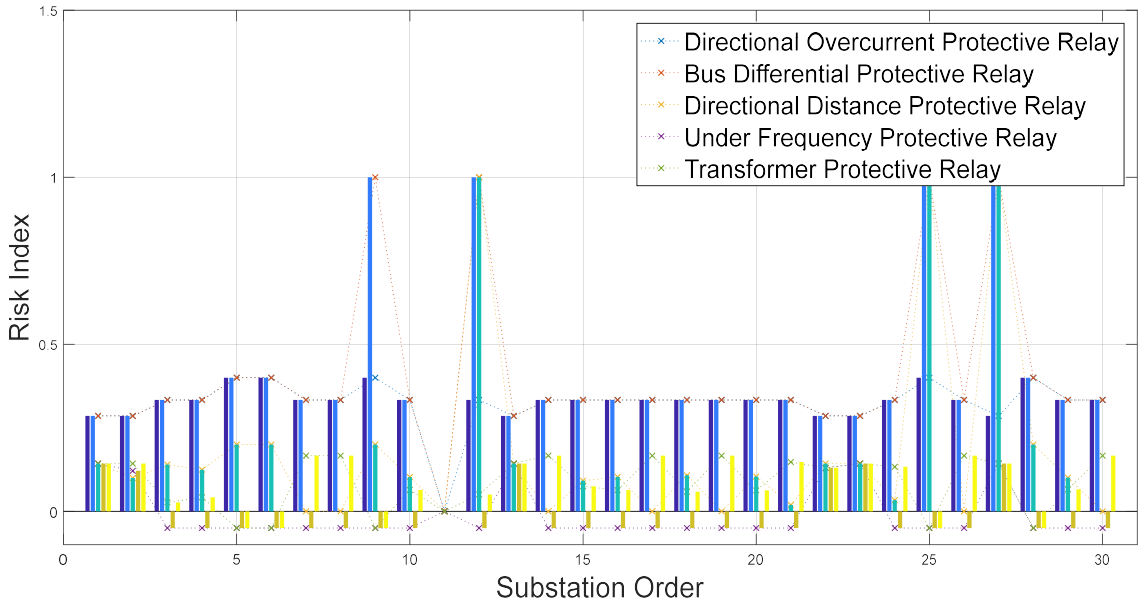

Figure 3.28: Risk index of protective relays in IEEE 30-bus system

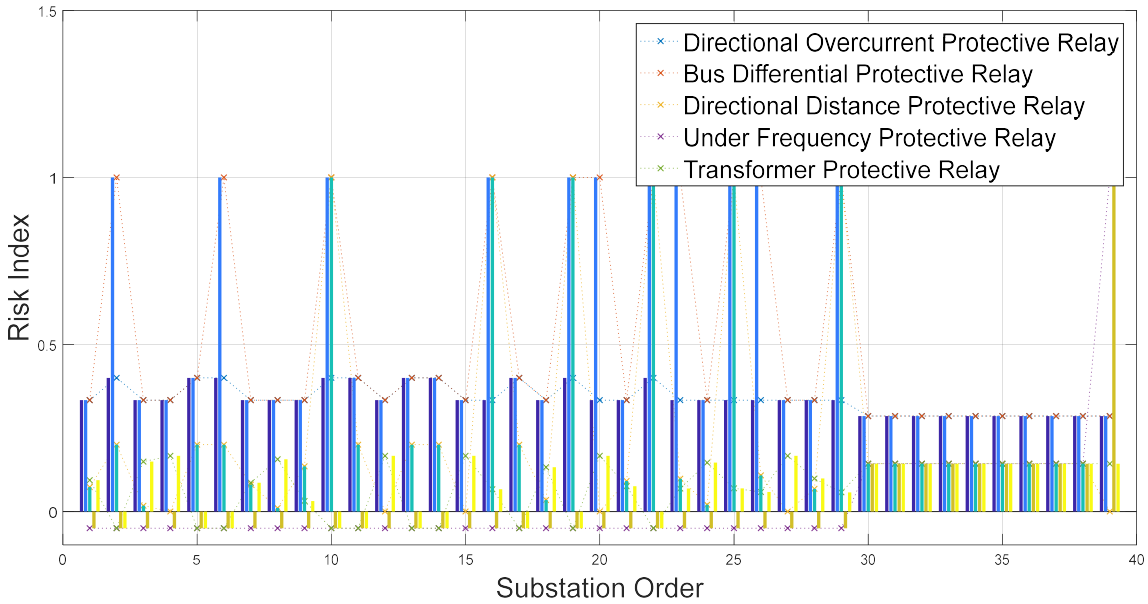

Figure 3.29: Risk index of protective relays in IEEE 39-bus system

Figs. 3.28–3.32 display the results of propsed risk index for different relays in IEEE

30-, 39-, 57-, 118-, and 300-bus systems, respectively. From these figures, the negative markers represent "not available" for such relay. For example, it is assumed in this study that the under frequency relays are equipped with the substations with generators. For those substations which are not classified as generation bus or load bus, the transformer relays are not equipped. In this respect, the negative risk value is given to differentiate the relay configurations between each substations. In the Fig. 3.28, the bus 11 is not modeled with any relay as the solutions of steady-state analysis reveal that the power flows from/to the bus 11 is 0 MW, which, based on the definition in the Eq. 3.17, would assign 0 as the risk index for each relay. However, the potential risks of relay outages in this substation may still exist. The cascading studies and transient analysis can be included to improve the existing model for future enhancement.

From the figures, it is observed that risk index for most relays are within [0.35, 0.50]. The critical IEDs are marked out with risk index of 1.0. For example, in IEEE 30-bus system, the overcurrent relay in the substation 9, bus differential and distance relays in the substation 12, 25, and 27, are identified as "worst" relays which would cause the system-wide instability in the steady-state analysis. In IEEE 39-bus system, it is observed that 18 out of 195 relays are identified as the critical relays, 11 out of which are bus differential relay. In IEEE 57-bus system, it can be observed that 9 out of 285 relays are evaluated as critical relays with 1.0 risk index, 5 of them are bus differential relays and 4 of them are distance relays. In IEEE 118-bus system,

16 out 590 relays are found to be critical and half of them are bus differential relays. Similarly, in the IEEE 300-bus system, 125 relays are identified as critical. 28% of the relays are directional distance relays, 59% of them are bus differential relays.

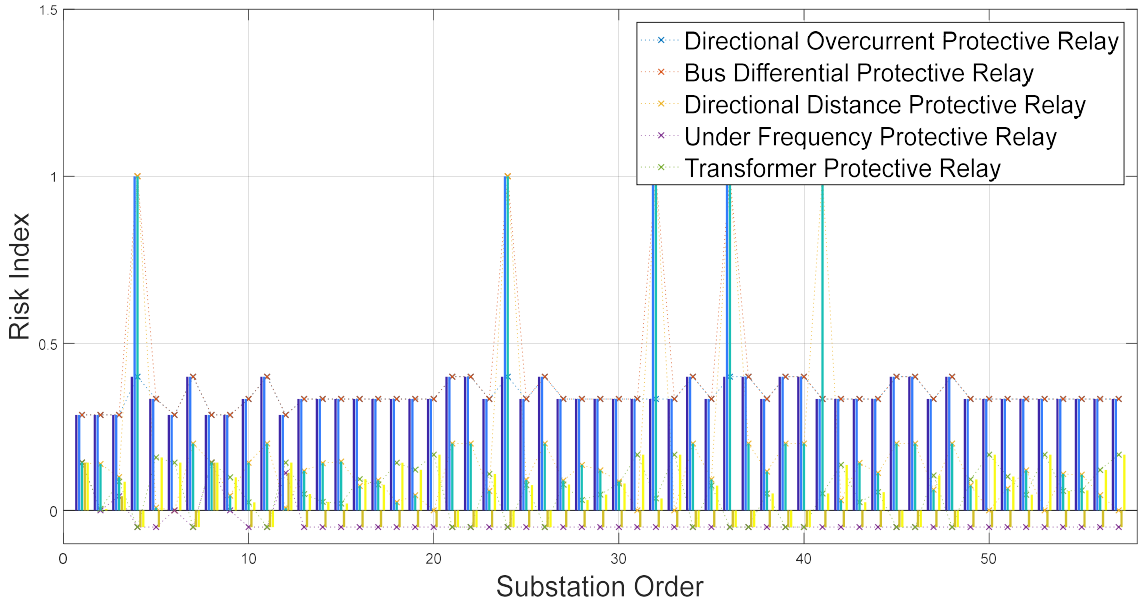

Figure 3.30: Risk index of protective relays in IEEE 57-bus system

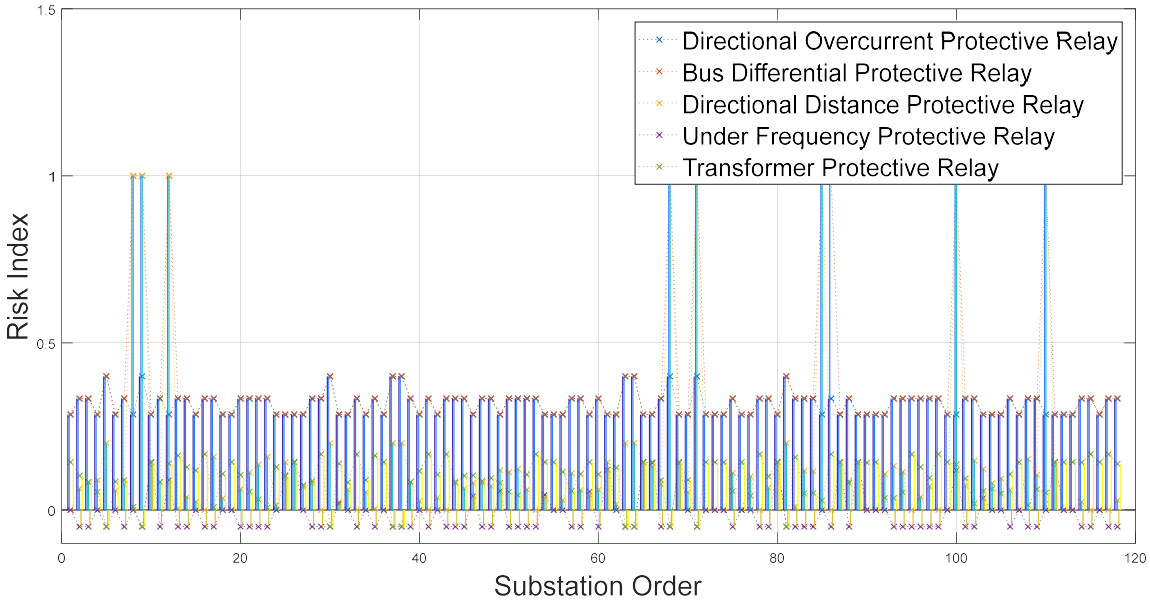

Figure 3.31: Risk index of protective relays in IEEE 118-bus system

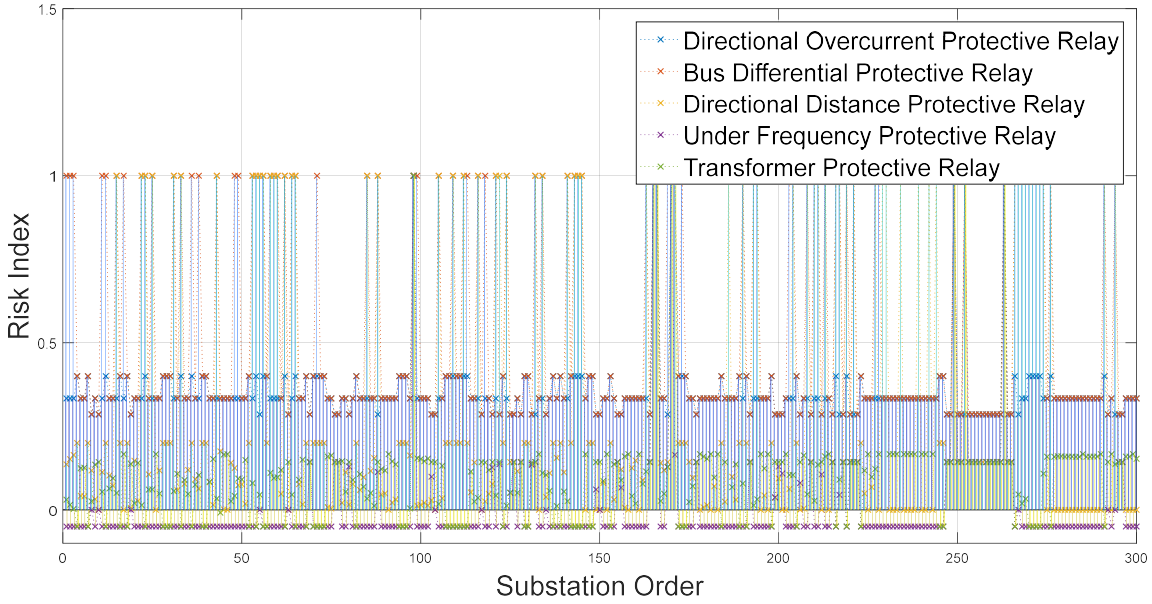

Figure 3.32: Risk index of protective relays in IEEE 300-bus system

Generally, the distance relays in large-sized system are ranked as critical outage whereas the impacts of a relatively smaller system may not have similar impacts. For example, substation 186 is connected with a load demand of -21 MW, which would provide 21 MW to the grid. Once the distance relay has been compromised, the outgoing lines of the substation would be disconnected, in which case, all the branches (93-186, 185-186) adjacent to that bus would be consequently disconnected. Thus, the substation 186 is islanded and the unbalance between the generation and load demand cannot be absorbed in the steady-state power flow analysis. From the observation of this simulation study, the larger cases with a larger lumped load per location (substation) can also result in a higher risk level of distance relays.

By integrating the results found risk index evaluations, it is concluded that the bus differential relay acquires the highest risk index compared with other relays because

1) bus differential relay is the most commonly deployed relay in the substation and 2) it would electrically disconnect all the switches from the system if it has been compromised, which would change the system configuration and remove the substation from the initial setup in the test system. To improve the risk metric of the bus differential relays, the potential cascading failure is needed to be further studied. Additionally, the impacts of directional distance relay are higher than the directional overcurrent relay due to the physical relations and relays where the disconnects affect abrupt change of the operating states. Compared with distance relay, overcurrent relay is assumed installed on the incoming lines from generators and local loads. When it has been compromised, the power injections and load demand would largely be disconnected from the system. However, the compromised distance relay would change the topology of the initial grid and consequently, cause substation islanded from the system, which is unstable in the study of steady-state evaluation.

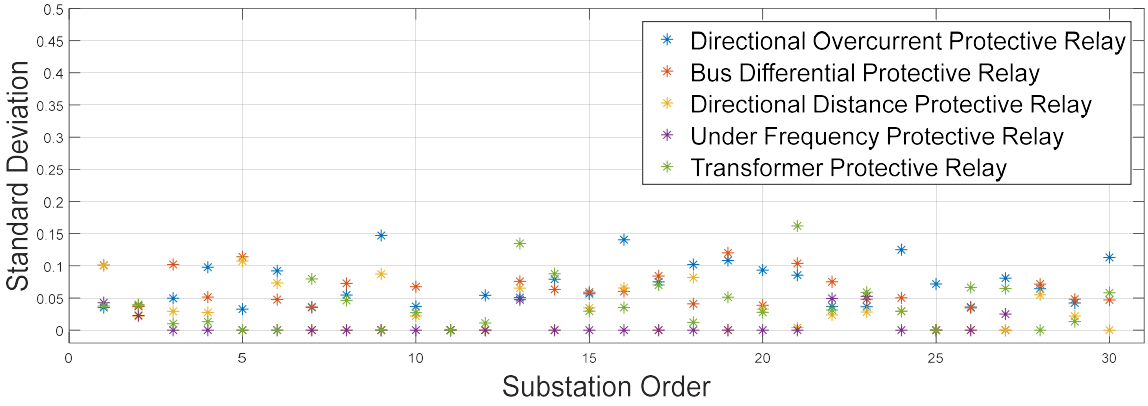

Figure 3.33: Standard deviation σ for IEEE 30-bus test system

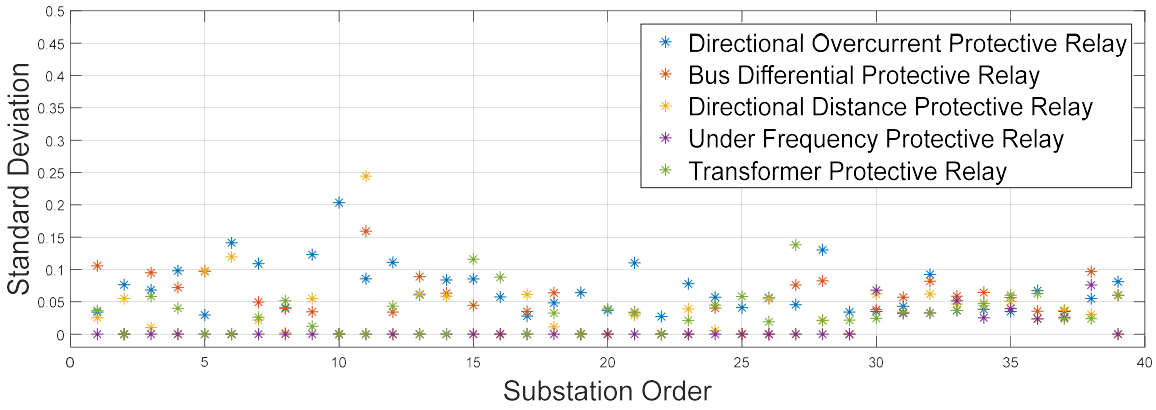

Figure 3.34: Standard deviation σ for IEEE 39-bus test system

3.6.4.1 Sensitivity analysis of proposed metric

In order to compare the performance using different probability distribution, the Eq. 3.19 introduces the standard deviation to evaluate the sensitivity of the proposed metric. Table 3.4 in section II summarizes the detailed results of standard deviations for each IEEE test cases. The σ is denoted by the standard deviation and the middle three columns record the number of relays whose σ are in the thresholds of (0, 0.01], (0.01, 0.05], and (0.05, 0.1], respectively. The 'Total #' denotes the number of protective IEDs that are evaluated through the proposed method for each test system. Each substation might have different protective IED configuration. When starting the standard deviation evaluation, the relays that are recorded in negative risk index in the previous sections should be eliminated. For example, in the IEEE 30-bus system, under frequency relay is not available in the substation 3 but is equipped in the substation 2.

Figs. 3.33–3.37 show the standard deviations for different relays using different probability distributions in the IEEE test systems. Generally, it is recorded that 79%, 85%, 62%, 87%, and 84% of relays acquire the standard deviation within 0.1 for IEEE 30-, 39-, 57-, 118-, 300-bus system, respectively.

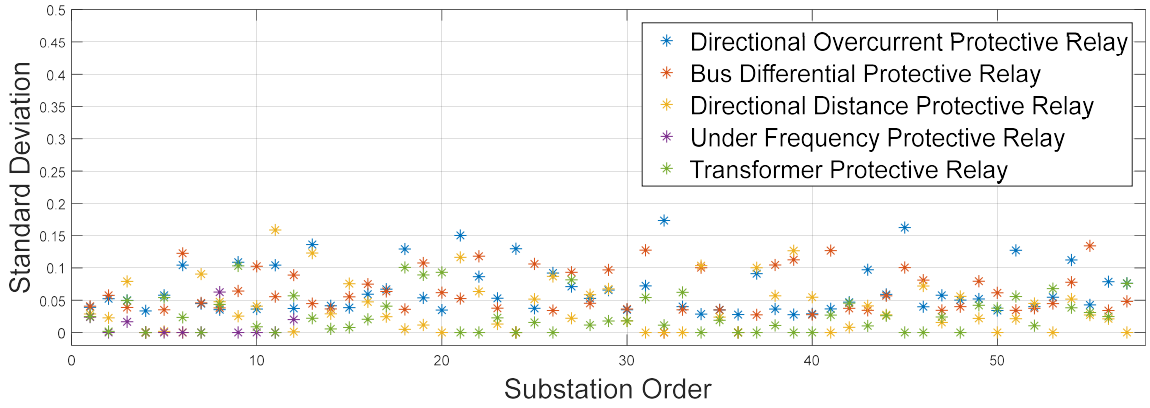

Figure 3.35: Standard deviation σ for IEEE 57-bus test system

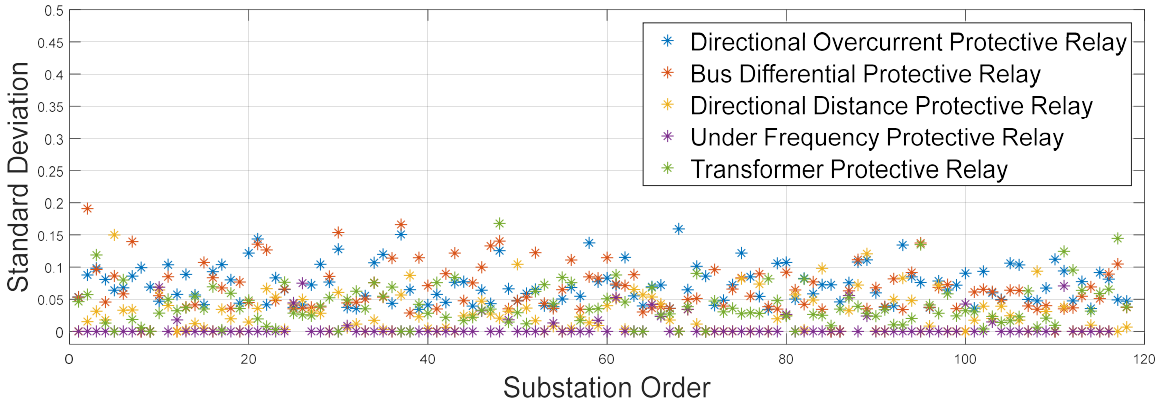

Figure 3.36: Standard deviation σ for IEEE 118-bus test system

As summarized in Table 3.4, it is observed that the σ of 80% of relays are located in the interval (0, 0.1], which equals to the variance in the interval (0, 0.01]. Additionally, it is realized that the σ for most scenarios are located in the section $3\% \leq \sigma \leq 8\%$, which is the middle part of the in the interval (0, 0.1]. To specify the distribution, Fig.

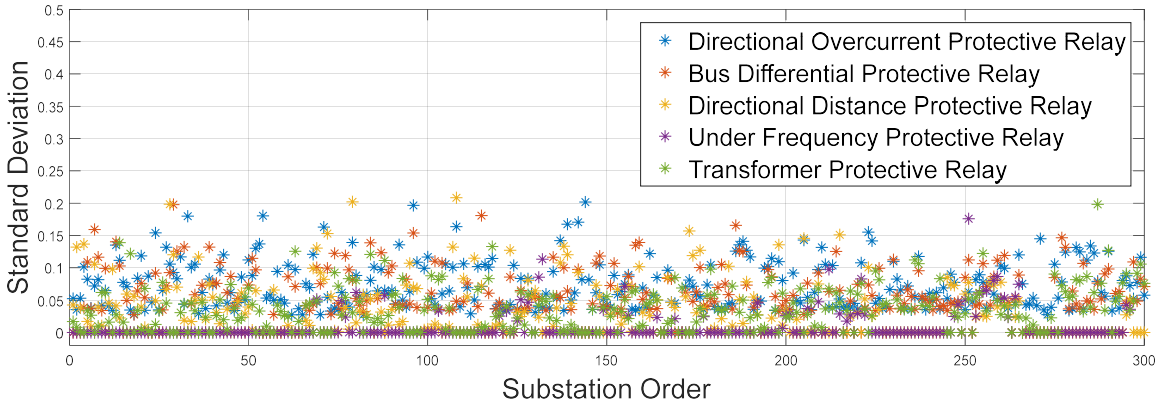

Figure 3.37: Standard deviation σ for IEEE 300-bus test system

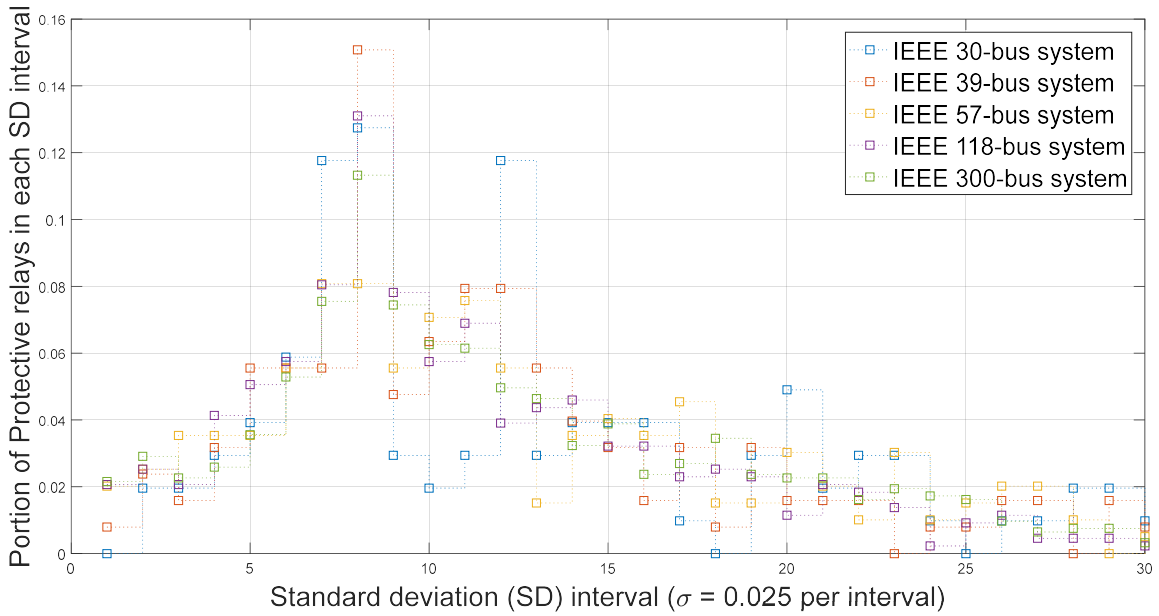

Figure 3.38: Statistical summary of the protective relays distribution according to standard deviation interval

3.38 details the numerical results the relay distributions according to the standard deviation interval, notice that each big interval would represent 0.025 incremental of the standard deviation as the x-axis variable. The portion of the relays in the corresponding standard deviation interval is given as the y-axis variable. For example, combining these five test systems, approximate 25 % of relays would locate in the first

interval $\sigma \leq 2.5\%$ and 30% of relays are found in the interval $2.5\% \leq \sigma \leq 5\%$. According to the distribution sample points in the fig. 3.38, it is statistically observed that such distribution can be fitted using a Normal distribution or Poisson distribution with the mean approximately equals to 8 units, which suggests that σ equals to 0.04. The fitting function would be determined to calculate the confidence interval for the standard deviation. Additionally, it is revealed that the σ of critical relays are much less than other relays. Because the Eq. 3.17 suggests that the higher the severity of the event, the lesser the risk index would be that is affected by the probability distribution. In this respect, the critical protective relays recorded in the risk index figures can be considered as reliable in the sense of steady-state analysis.

3.6.5 Static and Dynamic Verification of Through Compromised Protective Relays

3.6.5.1 Computational Environment and Test Case Setup

This simulation study evaluates IEEE 14-, 30-, 57-, and 118-bus systems using steady-state analysis. MATLAB R2018a (9.4.0.813654) is used as the simulation tool for steady-state analysis with supported by the high-performance computing cluster, *Superior*, which contains 92 compute nodes and each node is deployed with 16 CPU

cores in Intel Xeon E5-2670 at 2.60GHz and set with 64 GB RAM. The test cases are validated with an implemented parallel computing mode, which occupies 8 computing cores with 12 workers assigned and takes up 50GB of RAM. The time-domain dynamic study is implemented in the simulation tool CPAT [145] with the platform of Cygwin for providing Unix-based environment. For each hypothesized scenario, the total simulation time is set as 10 seconds and the time settings of the outages caused by hypothetical switching attacks are assigned at the moment of t=1.0s. The thresholds of protective relays are set referring to the operating guides [148].

This simulation study would investigate the $\hat{\mathbf{R}}$-k contingency with N set to 3, which includes top three digital relays with highest impacts on the system based on the fundamentals and applications in the Table 3.2. For each substation, the bus differential relay is assumed to be able to cause the most severe outage and ranked as level 1; generator protection relay is ranked to level 2; rank 3 includes the feeder protection relay; the distance protection relay is ranked to level 4. The double-circuit model is employed on each transmission line. Compromising single distance protection relay is assumed to increase the impedance of the transmission line, instead of removing the branch from the system.

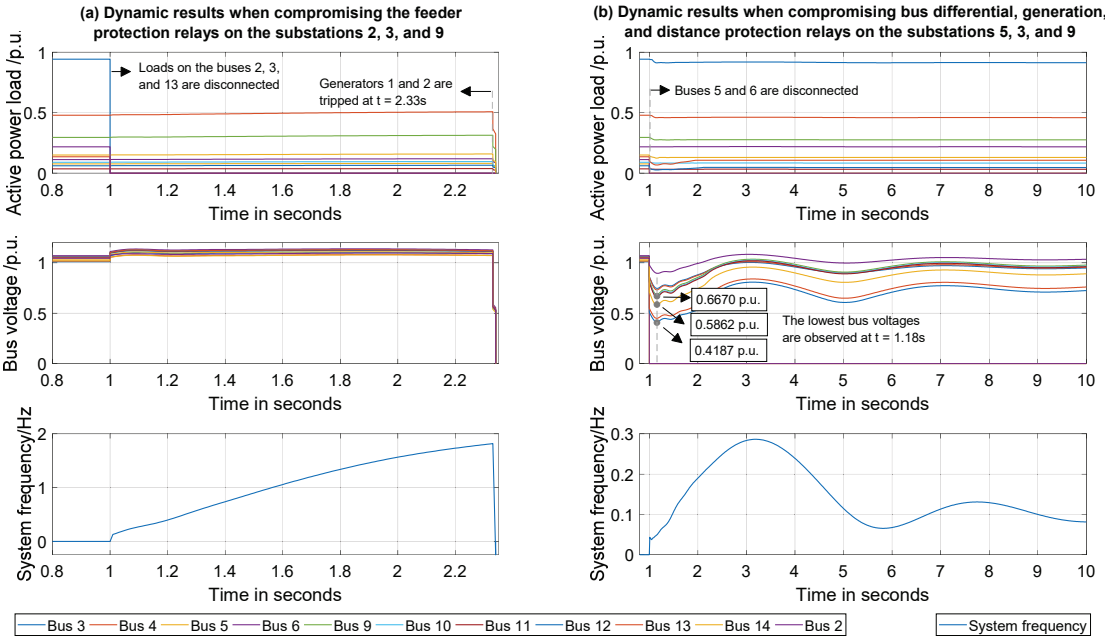

Figure 3.39: Dynamic simulation results of loads, bus voltages, and the system frequency

3.6.5.2 Steady-State and Dynamic Simulation Verification Study

The verification study on the outages caused by switching attacks between the steady-state and dynamic simulation results have been investigated via the IEEE 14-bus system. The Table 3.6 records the evaluation results in both static and dynamic simulations.

Table 3.6
Steady-state and dynamic evaluation verification using IEEE 14-bus system

Steady-State Analysis	Total #.	Dynamic Analysis	Total #.
Converged cases	3,412	Stable cases $\mathbf{DY}_{failed}$	3,141 271
$\mathbf{PF}_{failed}$	1,113	Stable cases $\mathbf{DY}_{failed}$	175 938

The steady-state analysis and the dynamic analysis do not always show the same conclusion in terms of the loss of electricity. The steady-state analysis is more likely to show optimistic results compared to the dynamic analysis especially when the significant imbalance between generations and loads occurs in the case of $\hat{\mathbf{R}}$-k contingencies. On the other hand, this analysis is more likely to show pessimistic results especially when the significant voltage drop such as the low bus voltage below 0.6 p.u. occurs in the case of $\hat{\mathbf{R}}$-k contingencies. Such discrepancies come from the following limitations of the static approach: 1) Dynamic constraints and constraints for dynamic change are skipped, 2) Self-regulated controls and protections are skipped. Because the voltage change and frequency change can happen at the same time, the steady-state analysis can show both optimistic and pessimistic aspects compared to the dynamic analysis depending on which aforementioned two factors are more correlated.

For example, Fig. 3.39a depicts the behaviors of the active loads, bus voltages, and the system frequency of a $\hat{\mathbf{R}}$-3 contingency, where the feeder protection relays on the buses 2, 3, and 13 have been compromised. It is observed that over 49% of the active power has been disconnected at $t = 1.0$s when the system frequency starts to increase. The generators 1 and 2 are disconnected from the system by the overfrequency relays at t=2.33s, which would result in the whole system collapse. It is noted that the steady-state analysis treated as the converged case because the loss of generation is promptly compensated by another generator, which is impractical for the real network. Additionally, Fig. 3.39b shows the same quantities where the

bus differential relay, generation protection relay, and distance protection relays on the substations 5, 3, and 9 are compromised. The extremely low bus voltages have been observed following the contingency and self-regulation of loads, i.e. partial disconnection of loads contributes to recover the voltage. It is noted that the steady-state analysis treat it as the diverged case because such dynamic behavior of the load (reduction) cannot be represented.

As described in Table 3.6, 4,525 cases are evaluated in both steady-state and dynamic analysis. $\mathbf{PF}_{failed}$ and $\mathbf{DY}_{failed}$ record the nonconverged and blackout cases in static and dynamic methods correspondingly. It is noticed that the original result counts 4,236 cases as the converged scenarios; however, the static evaluation incorporates the basic power flow evaluation which hypothesizes that the generator nodes can be adjusted to absorb imbalance between the generator outputs and the system loads. If the limit of the generator capacity is fixed in the simulation, more cases would be counted as diverged case. Thus, the number would be modified to 3,412 and 3,141 out of 3412 cases are validated as the stable cases. It is counted that 938 out of 1,113 cases are verified as the blackout cases through the dynamic analysis. Generally, the ratio of the match between the static and dynamic results is $(3141 + 938)/(3412 + 1113) = 90.14\%$. Specifically, it is counted that the sum of the stable cases is $3141 + 175 = 3316$. The steady-state analysis identifies 3,141 out of 3,316 cases, which gives the coverage ratio of 94.72%. Based on these results, it is reasonable to conclude that the steady-state analysis would be considered as acceptable in the following sections.

Compared with steady-state analysis, the dynamic analysis would include more dynamic details and would cost more time. The average computing speed for dynamic simulation is around 10 cases per minute and the total computing time for completing 4,525 cases costs several hours with over tens of gigabytes of numerical data produced. It is reasonable to conclude that the steady-state evaluation would be a feasible method to conduct a prescreening study in terms of the verification ratio and the efficient storage.

3.6.5.3 Static Study on the Prescreening of the Protective Relaying Outages

This section conducts the prescreening process by investigating the impacts based on enumeration of hypothetical switching attacks via presumably compromised relay outages based on the static evaluations. The comparison study between the results with and without overloading implications are summarized in the Table 3.7.

As summarized in the Table 3.7, IEEE 30-, 57-, and 118-bus cases evaluate 72, 129, and 327 protective relays, which, respectively, generate 62,268, 357,899, and 5,827,903 cases in total. It is observed that with the overload implications, the number of evaluated cases are reduced as the level k increases. For example, in the IEEE 30-bus system, the number of evaluated cases without overloading settings is 55,755 and

Table 3.7
The steady-state evaluations of identification of critical protective relays

IEEE 30-bus system			
No overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	72	2
$k = 2$	141	2,415	23
$k = 3$	6,372	53,268	40
With overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	72	5
$k = 2$	345	2,211	37
$k = 3$	13,990	45,650	95
IEEE 57-bus system			
No overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	129	3
$k = 2$	381	7,875	98
$k = 3$	35,522	313,982	612
With overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	129	20
$k = 2$	2,370	5,886	51
$k = 3$	144,769	204,735	475
118-bus system			
No overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	327	10
$k = 2$	3,215	50,086	88
$k = 3$	35,522	5,738,753	268
With overloading	Reduced cases	Evaluated cases	Critical #.
$k = 1$	-	327	38
$k = 2$	11,685	41,616	61
$k = 3$	1,810,096	3,964,179	839

it drops to 47,993 with the overload implication, which reduces 12.46% of combinations in total. For 57- and 118-bus systems, the reduced rate is 31.08% and 30.59%, respectively.

Specifically, in the IEEE 57-bus system, it is observed that if the bus differential relay on the substation 22 has been compromised, the simulation would agree with a

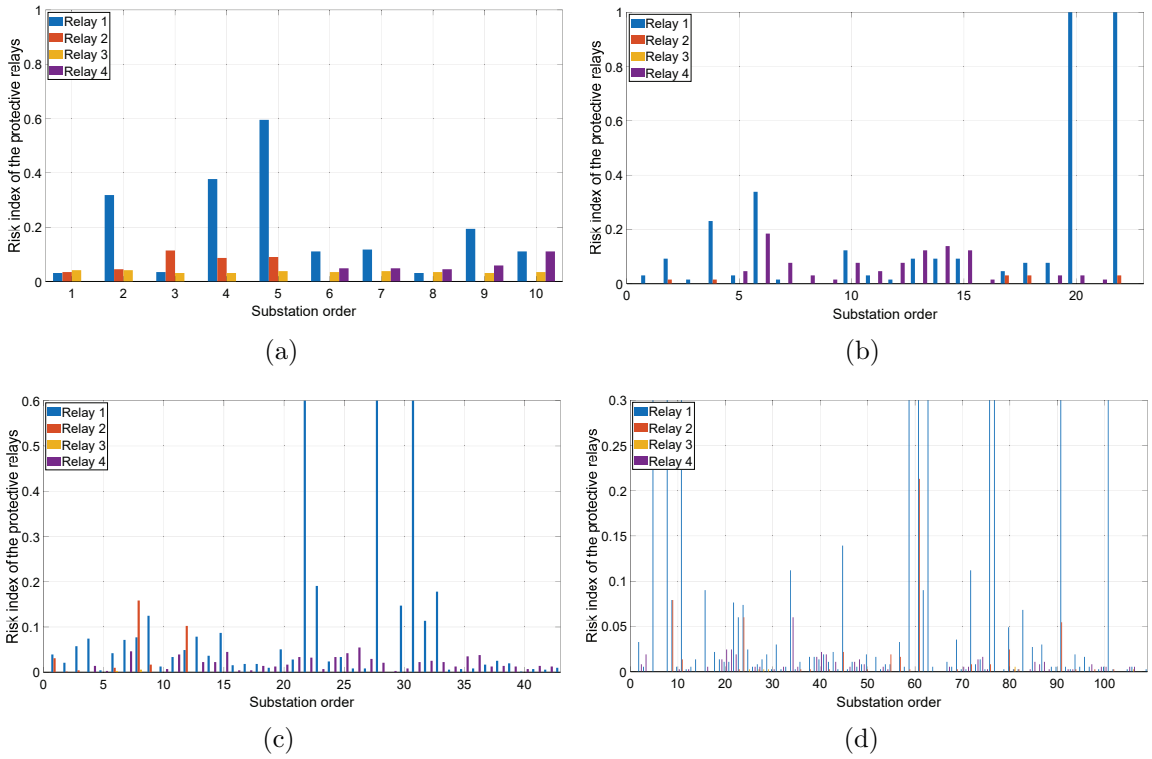

Figure 3.40: Risk index of the protective relays in the IEEE test systems with 14, 30, 57, and 118 bus nodes: (a) IEEE 14-bus system; (b) IEEE 30-bus system; (c) IEEE 57-bus system; and, (d) IEEE 118-bus system.

diverged solution. Similarly, $\hat{\mathbf{R}}$-2 contingency evaluation also reveals that when the bus differential relays on the substation 1 and the generator protection relay on the substation 3 are compromised simultaneously, the system would not be stable in the static analysis.

In a larger system, i.e., IEEE 118-bus system, the $\hat{\mathbf{R}}$-1 contingency suggests that when the bus differential relay on the substation 8 has been compromised, which disconnects 28 MW of load and transmission line 8-5 and line 8-9, the system would not be stable. The $\hat{\mathbf{R}}$-2 contingency analysis reveals another worst case that the when

the bus differential relay on the bus 37 and the generator protection relay on the bus 10 are compromised, 450 MW of power and the transmission lines 35-37, 37-38, 37-39, and 37-40 are disconnected from the system. Similarly, the $\hat{\mathbf{R}}$-3 contingency records another worst case that when the generator protection relays on the bus 10, 12, and 69 are compromised, the system would lose 1051.4 MW of power source and the system would not be stable.

To quantify the impact level of the protective relays at each substation using the results of critical protective relays, Figs. 3.40(a), 3.40(b), 3.40(c), and 3.40(d) depict the risk index for IEEE 14-, 30-, 57-, and 118-bus systems. It is worth noting that the risk index is derived from the results without overloading implication. 4 different relay ranks are included in each figure to classify the critical relays. The legends of relay 1, 2, 3, and 4 denote the relay with the first, second, third, and forth rank, which denotes the bus differential, generator protection, feeder protection, and distance protection relay, respectively. The bus differential, generator, and feeder protection relays are selected as the first three relays that would lead to the most severe outages. It is also noticed that the generator protection relays may not be necessarily deployed because the some substations might not be connected with generation units, then the alternative distance relay is included in the evaluation.

In the IEEE 14-bus system, as depicted in the Fig. 3.40(a), it is observed that the bus differential relay on the substation 5 acquires the highest risk index with

0.5952. The highest risk index of the generation protection relay and distance relay is 0.1142 and 0.1107. Compared with the risk index level of bus differential and generator protection relay, the feeder protection relay is lower than 0.05. Though the distance relay would produce a relatively lower index, it is unwise to underestimate its impact. For example, when the bus differential relay on the substation 5 has been compromised, which would disconnect 18.8 MW of load and the multiple transmission lines, including line 1-5, 2-5, 4-5, 5-6, 6-11, 6-12, and 6-13, the simulation would agree with a converged solution. But when combining the contingency that compromising the single distance relay on the buses 14, which would increase the impedance of the lines 13-14 and 9-14, the power flow calculation fails to converge.

In the IEEE 30-bus system, as depicted in the Fig. 3.40(b), 2 critical bus differential relays are identified in the $\hat{\mathbf{R}}$-1 contingency analysis, which are on the substations 20 and 22. The second critical bus differential relay, which is on the substation 6, acquires the value of 0.3358. The generator protection relay acquires the highest index of 0.0308 on the substations 17, 18, and 22. The distance protection relay acquires the highest index of 0.1846 on the substation 6. It is also noticed that no critical feeder protection relay is detected in the system. In the IEEE 57-bus system, as shown in the Fig. 3.40(c), it is observed that bus differential relays on the substation 22, 28, and 31 are identified as critical relays, which acquire the risk index of 1.0. Other differential relays acquire comparably lower risk which are less than 0.2. The generation protection relay on the substation 8 acquires the highest index of 0.1585

in the second rank. Both distance and feeder protection relays demonstrate relatively low risk indices in the results. Similarly, in the IEEE 118-bus system, as displayed in the Fig. 3.40(d), the differential relays on the substations 5, 8, 11, 59, 61, 63, 76, 77, and 101 are identified as critical in the $\hat{\mathbf{R}}$-1 contingency analysis. It is noticed that the vertical coordinate has been re-scaled to 0.3 to increase the readability of the figure. The generator protection relay on the substation 61 acquires the highest risk index of 0.2131. Compared with the differential and generator protection relays, it is found that most of the feeder and distance protection relays obtain lower impact level. In the prescreening process, it is also observed that the risk index not only include the impact level of the critical digital relays but also incorporates the potential vulnerability of the substation. For example, both the differential and generator protection relays on the substation 61 obtain relatively higher indices than other substations, it is reasonable to conduct a detailed investigation on the security of the protection parameter of the substation.

Chapter 4

Cyber Risk Management: Insurance Premium for Power Grids

4.1 Introduction

This chapter proposes a framework for grid insurance against disruptive switching attacks, which is assumed to be determined by two major aspects: (1) the probability of successful intrusion into the substation(s) which will presumably result in disruptive switching attack from the compromised substation(s) and (2) the discrete distribution

of claim size of each potential attack scenario [64, 65, 66]. The vulnerability and the steady-state probability of potential electronic intrusion to each power substation have been studied in the papers [67, 68], which are derived from the firewall and password models using Markov chain. The steady-state probability [67] is assumed to be effective to generate the discrete distribution of the hypothesized scenario. The proposed claim size of power utilities is assumed to be equal to the estimated economic loss that is directly related to substation outages. To address the impact of the hypothesized cyberattacks, following assumptions are included in the proposed framework:

† The risk index studies [1, 25, 30, 45], using the extended combination method and reverse pyramid model (RPM), generate the risk-based "bottleneck list." The "critical" combinations would lead to the potential instability of the power system in steady-state analysis [45].

† the surveys on the operational loss [149, 150, 151] and the electricity prices [152, 153] are included in the paper to conduct a comparative study of the economic loss of the hypothesized power outages. It is assumed that the operational loss discussed in the paper only covers the direct loss that has been studied in [149, 150, 151].

† The studies on the mean time to restore power (MTTRP) [154, 155, 156] of the hypothesized power system outages are also performed, which estimate the

expected restoring time of a system after a presumed cyberattack.

In general, the insurance claim has the specific verbatim emphasizing on cyber-physical switching attacks that are directly initiated by the control systems from substations or control centers. Any other security threats that do not immediately cause operational impacts [157, 158] are not included in this premium model.

4.2 Probability distribution based on Cyber-Reliability Assessment Model

4.2.1 Probability Mass Distribution of the Hypothesized Scenario

The vulnerability of the control networks has been evaluated by modeling intrusions and consequences of a cyberattack on control networks [67, 68]. The embedded connectivity of the firewall and password models can be formulated using a cyber-net diagram. Such connectivity generates a transition probability matrix $\mathbf{M}$ that satisfies:

$$\begin{aligned} \tilde{\pi} \cdot \mathbf{M} &= \tilde{\pi} \\ \sum \tilde{\pi} &= 1 \end{aligned} \tag{4.1}$$

where $\tilde{\pi}$ denotes the steady-state probability of state in the embedded transition matrix of the Markov chain $\mathbf{M}$. The steady-state probability π can be calculated by weighting each element in $\tilde{\pi}$ with its costed sojourn time of the corresponding markings [67]:

$$\pi(\cdot) = \begin{cases} \frac{\bar{\tau}_s(M_s)}{\bar{\tau}_c(M_j)} & M_s \in T \\ 0 & M_j \in V \end{cases} \tag{4.2}$$

where T and V are the marking sets for immediate and timed transitions [67], respectively. The mean time that a process transits from state M_s to M_j are given as $\bar{\tau}_s$. The time spent in the state M_j is denoted as $\bar{\tau}_c$. s and j denote the different positions in the Markov chain $\mathbf{M}$. The steady-state probability derived from Eqs. 4.1 and 4.2 is employed in this framework. Such probability not only embeds vulnerability of the protective models, i.e., the firewall and password models, but also incorporates the topology of protective networks contained in the substation.

Assume that the system contains S substations. Let $\mathbf{T}$ be the collection of all non-empty subsets of $\mathbf{S} = \{1, 2, \cdots, S\}$. This definition lets the set $\mathbf{T}$ consist of all k-combinations of $\mathbf{S}$ with $k = 1, \cdots, S$. Let the t-th element of $\mathbf{T}$ be $\mathbf{t} \subseteq \mathbf{S}$. The probability of the t-th substation combination $\tilde{p}_x$ is defined as:

$$\tilde{p_x}(t) = \left(\prod_{i \in \mathbf{t}} \pi(i)\right)\left(\prod_{j \in \mathbf{S}, j \notin \mathbf{t}} \Big(1 - \pi(j)\Big)\right) \tag{4.3}$$

where i and j in the Eq. 4.3 denote the indices of substations and the subscript x

denotes the claim size of the t-th substation combination.

It is worth noting that we exclude the empty set in $\mathbf{T}$, which corresponds to the case without insurance claims. For this reason, the cardinality $|\mathbf{T}|$ of set $\mathbf{T}$ is equal to $2^S - 1$, and the sum of the probability $\tilde{p}_x$ calculated in Eq. 4.3 may not necessarily be equal to 1. As a consequence, the probability mass function of the discrete substation combination can be normalized that will be summed up to 1.0:

$$p_x(t) = \frac{\tilde{p}_x(t)}{\sum_t^{|\mathbf{T}|} \tilde{p}_x(t)} \tag{4.4}$$

Eq. 4.4 formulates the basic discrete probability distribution of hypothesized substation outages. $p_x(t)$ is the function of t in which it cannot be directly applied to the premium calculations because the different substation outages could claim the same size of economic loss. The following section would further illustrate the formulation of the claim size and the necessary modifications to Eq. 4.4.

4.2.2 The Claim Size of the Hypothesized Substation Outages

Determining the claim size due to the hypothesized substation outage is important for insurance companies to implement their insurance policy because of the direct effect

on their own business strategy. In the following formulation, the data is obtained from the previous cyber-based contingency analysis in the steady-state studies [1, 25, 30, 45] and the claim size x is assumed to be equal to the direct loss due to the hypothesized power outages, which is determined by three variables: (1) the power loss **PL** (MW) due to the substation outages in steady-state evaluation [1, 25, 30, 45], (2) the expected mean time to restore power **H** (hour) from the abnormal status to normal steady-state conditions [154, 155, 156], and (3) the direct costs γ (\$/MWh) during the power outages [149, 150, 151]. Thus, the claim size x (\$) for the t-th substation combination is defined as:

$$x_t = \mathbf{PL}_t \cdot \mathbf{H}_t \cdot \gamma \tag{4.5}$$

Fig. 3.3 depicts the flowchart of an enumerative algorithm for calculating the claim size based on Eq. 4.5. The "critical" lists C is generated using the extended enumeration model in [45]. The "critical" combination of substation(s) recorded in C may cause the system steady-state instability, which is considered as the blackout situation in this formulation. The critical list C is applied here to identify the size of blackouts of the substations combination set $\mathbf{t} \in \mathbf{T}$. The MTTRP simulation is conducted based on the concept of generic restoration milestones (GRMs) [154]. The italic form of $MTTRP$ represents the vector that records the restoration time of each

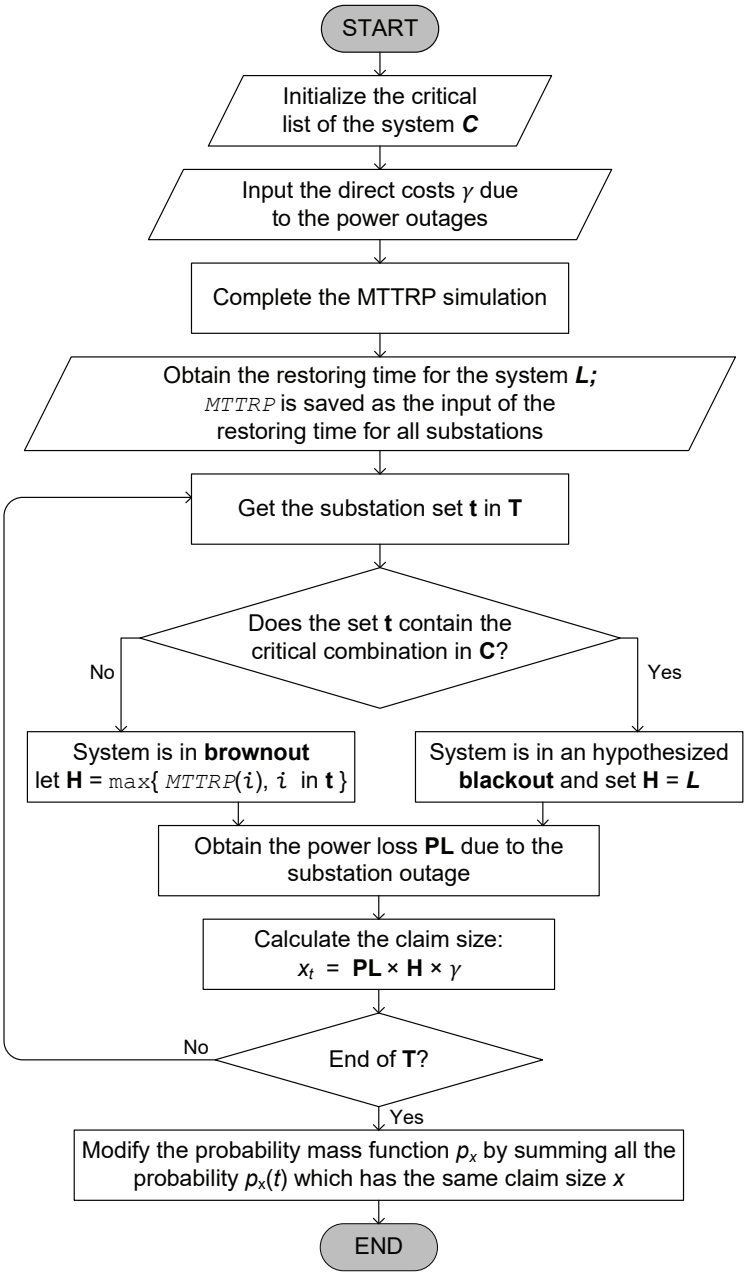

Figure 4.1: Algorithm for enumerative calculations of the claim size x

substation and $\mathbf{L}$ is the total restoration time initiated from the blackstart (BS). It is observed that, after all the claim sizes in $\mathbf{T}$ have been identified, the different combination sets $\mathbf{t_1}$ and $\mathbf{t_2}$ may have the different $p_x(t_1)$ and $p_x(t_2)$ but share the same

claim size x_i. In order to create the probability mass function of the claim size x, which the cyber insurance company focuses on, the probability distribution function determined in the formula 4.4 needs to be modified by aggregating all $p_x(t_i)$ that have the same claim size:

$$p(x) = \sum_{t}^{|\mathbf{T}|} p_x(t) \tag{4.6}$$

Eq. 4.6 formulates the PMF of the diverse claim sizes x and the variable t has been canceled out. Compared with Eq. 4.4, Eq. 4.6 is more clear and convenient to be applied in the ruin probability calculations to determine the insurance premium.

4.3 Determination of Cyber Insurance Premium using Ruin Probability Theory

4.3.1 Ruin Probability Calculation

Ruin probabilities has been widely implemented since the beginning of last century and has demonstrated its effectiveness in evaluating the long-run viability of insurance portfolios [64, 65, 66]. The primary purpose of using Ruin is to estimate the probability that the total claims exceed the sum of the initial risk reserve of a utility and the total premium received in a given time interval. To avoid the ruin of a

company to the greatest extent, the total premium should be able to bound the ruin probability in a significantly small level [65].

The ruin probability $\psi(u)$ for the initial risk reserve u is fundamentally defined in [64] as :

$$\psi(u) = Pr\{M > u\} = 1 - F_M(u) \tag{4.7}$$

where M is defined as the maximal aggregate loss and $M = L_1+L_2+L_3+\cdots+L_N$. $Pr\{A\}$ denotes the probability that the event A happens, and $F_X(x) = Pr\{X \leq x\}$ represents the cumulative density function (CDF) of X. It is assumed that the number of claims N follows a geometric distribution satisfying

$$Pr\{N = n\} = (1-q)q^n, \quad n = 0, 1, 2, \cdots \tag{4.8}$$

where $0 < q < 1$. Each random variable L_n represents claimed loss. Assume that for any fixed N, the amounts of the successive claims, denoted as $L_1, \cdots, L_N$, are positive, independent and identically distributed (i.i.d.) with a common CDF $F_L(x)$ with mean μ. L_n is assumed to be i.i.d. with the probability density function of given as:

$$f_L(x) = \frac{1 - F_L(x)}{\mu}, \quad x > 0. \tag{4.9}$$

As a result, the CDF of the random sum M is derived as

$$F_M(u) = \sum_{n=0}^{\infty} Pr\left\{\sum_{k=1}^{n+1} L_k \leq u\right\} Pr\{N = n\} \tag{4.10}$$

Eq. 4.10 is known as the distribution function of the compound geometric distribution. If we assume that M is defined on non-negative integers, the recursive formula for the CDF of M is shown as [64]:

$$F_M(u) = \frac{\theta}{1+\theta-f_L(0)} + \frac{1}{1+\theta-f_L(0)} \sum_{y=1}^{x} f_L(y) F_M(u-y) \tag{4.11}$$

In order to use the recursive formula in Eq. 4.11, $f_L(x)$ need to be discretized. The discrete distribution $\{f_x : x = 0, 1, 2, ...\}$ is utilized to replace the continuous distribution $f_L(x)$ at points $0, h, 2h\cdots$ by matching a certain number of moments. As a consequence, within each incremental interval, a certain number of local and global moments of f_x and $f_L(x)$ are equal. The number of moments which are required for replacement is usually the same as the number of intervals. Combining Eqs. 4.7 and 4.11, the probability of ruin can be derived:

$$\psi(u) = \frac{1-\mathbf{F}_u}{1+\theta-f_0} - \frac{1}{1+\theta-f_0} \cdot \sum_{y=1}^{x} f_y \cdot \psi(u-y) \tag{4.12}$$

where $\mathbf{F}_u = f_0 + f_1 + \cdots + f_u$ and $\theta \in (0, 1)$ is a user-defined variable, which needs to be adjusted by an insurance company. Eq. 4.12 is employed in the whole framework

presented in the paper for the probability of ruin.

It is observed that the claim size x is discrete and may not be necessarily starting from 0. Assume the system contains the claim size x that satisfies $x \in [a, b]$, where a and b are the lower and upper bounds of the claim size, respectively. Consider it is a two-moment problem, the following linear system is verified:

$$\begin{bmatrix} 1 & 1 & 1 \\ a & a+h & b \\ a & (a+h)^2 & b^2 \end{bmatrix} \cdot \begin{bmatrix} f_a \\ f_{a+h} \\ f_b \end{bmatrix} = \begin{bmatrix} \int_a^b f_L(x)dx \\ \int_a^b x f_L(x)dx \\ \int_a^b x^2 f_L(x)dx \end{bmatrix} \tag{4.13}$$

The right-hand-side values of Eq. 4.13 are called the r-th moment with the form of $\int_a^b x^r f_L(x)dx$ and h denotes the general increment of each moment. These values can be derived from Eq. 4.9. Combining Eqs. 4.9, 4.12 and 4.13, the ruin probability can be solved with the predetermined parameter θ.

4.3.2 Premium Calculation Using Ruin Probability Theory

Based on the details of ruin probability calculation clarified in previous section, the tentative premium amount, **I**, is defined:

$$\mathbf{I} = (1 + \theta_f)\lambda\mu \tag{4.14}$$

where θ_f is the feasible θ that can be identified in the ruin probability calculation. λ denotes the expected number of claims of the process and can be obtained by using Eq. 4.3. Compared with the traditional insurance policy, the frequency of claims for the cyber insurance on the power system outage may be much less because of its low occurrence in the historical data. μ is the mean of the successive claims that can be derived through Eqs. 4.4 and 4.9. Additionally, θ_f may not be unique if the insurance company provides an acceptable range of ruin probabilities, which would affect the range of θ and the feasible premium amount. In chapter 4.4, we provide a list of the feasible ruin probabilities with different choices of θ's and different settings of initial reserve u.

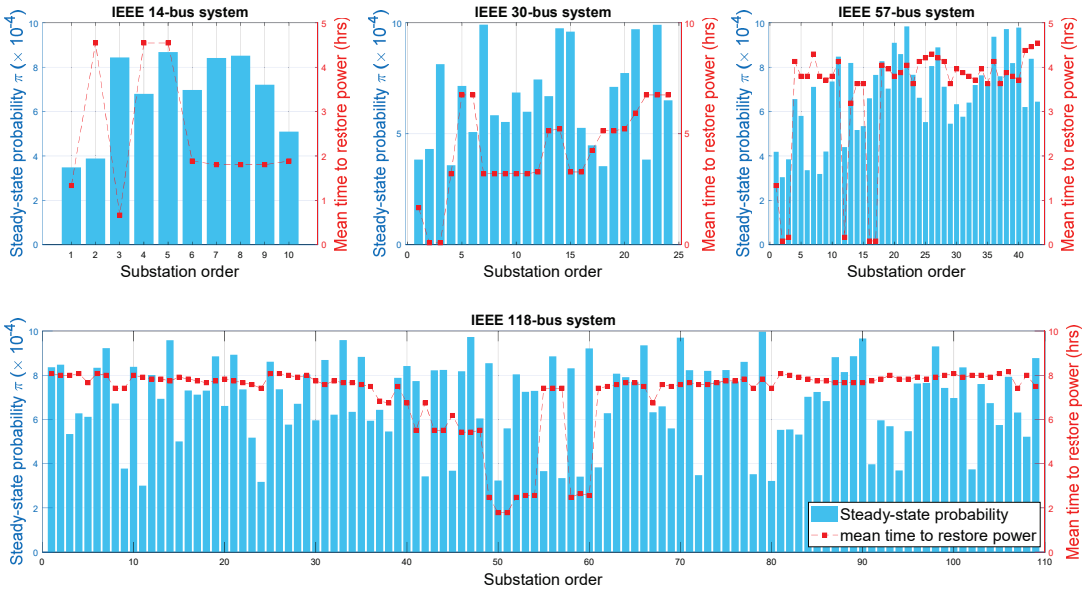

Figure 4.2: The summary of steady-state probability and the expected mean time to restore power for IEEE test cases

4.4 Numerical Illustration

4.4.1 Test Case setup: Steady-state Probability, MTTRP, and Claim Size

4.4.1.1 Steady-state probability

The case setup of the steady-state probability is derived from the intrusion probabilities of "Model 1" and "Model 3" from "outside" attack in [67], denoted as π_1 and π_3, respectively. Notice that $\pi_1 \in \Pi_1$ and $\pi_3 \in \Pi_3$, where Π_1 and Π_3 are two probability

pools for different models. In order to improve the feasibility of the model, the authors assume that the substations with generation units installed are deployed with more secure protective parameters, which would lead to a lower intrusion probability. Fig. 4.2 gives the detailed settings of the steady-state probability for each system, highlighted in light blue and based on the left-side axis. It is observed that in the IEEE 14-bus system (10 substations), substations 1 and 2 are equipped with generators which are in lower probabilities of being compromised, i.e., $\pi(1) = 0.00034856$ and $\pi(2) = 0.00038848$. In the IEEE 30-bus system (24 substations), substations 1, 2, 4, 17, 18 and 22 are connected with generation unit, which would be assigned with lower probabilities. Similarly, substations 1, 2, 3, 6, 8, 9 and 12 in the IEEE 57-bus system are with lower probabilities of successful intrusion.

4.4.1.2 Critical list of hypothesized substation outages

The critical list C is derived using the extended RPM model [45], which enumerates all the hypothesized substation combinations, and the "worst" combinations are identified. In the 14-bus system, 3 "critical" substations are identified, which are substation 2, 4 and 5. 8 substations are found to be critical in the 30-bus system, which are substation 2, 4, 5, 6, 10, 17, 20 and 22. Similarly, in the 57- and the 118-bus system, 18 and 42 "critical" substations are found, which may lead the system to potential instability in terms of steady-state analysis. Based on the critical list, the complete

combination list **T** would be determined to identify the hypothesized power outages. It is noticed that even though the critical lists could generate numerous combinations as much as possible; however, in the proposed premium calculation study, the depth k is determined as k = 3. It is observed that the steady-state probabilities of the combinations at the 4th or higher order would be less than 10^{-12} and is considered as the small probability event which would not be included in this study.

4.4.1.3 Simulation results of expected mean time to restore power

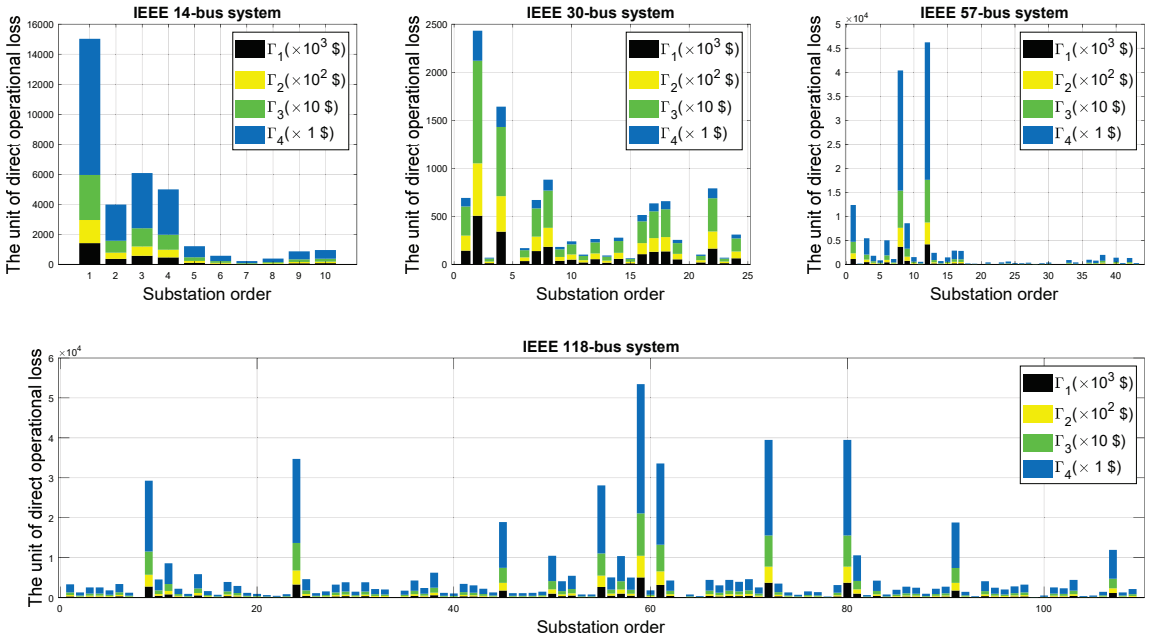

Figure 4.3: The direct operational loss due to power outages with different systems and diverse γ settings

The simulations of expected mean time to restore power (MTTRP) for different systems are derived based on the GRM models [154]. In the IEEE 14-bus system, the

bus 2 is selected as BS node. For other generation substation, i.e., substation 1, the setting of the time to crank the generator is 80 minutes. The lumped load at substation 1 is selected as the critical load. For both 30- and 57-bus systems, node 1 is selected as the BS nodes and node 7 is selected as the BS node in the 118-bus system. The time to crank generator is selected within [80,120] minutes. The "pick up" time of transformers and transmission lines are applied with the default settings of 5 minutes. MTTRP simulations demonstrate that it takes 3, 6, 3 and 8 steps to restore 14-, 30-, 57-, and 118-bus systems respectively, which cost 118, 404, 373, and 414 minutes in total. In the Fig. 4.2, the expected restoration time **H** of each system is marked in red.

In this simulation, the direct operational costs γ ($/MWh) caused by the hypothesized substation outage are extracted from four different studies: 1) the studies on value of loss load (VOLL) [150, 151]; 2) the surveys on the estimated direct costs in the previous power outage [149]; 3) the statistical studies of the average retail electricity price [152]; and 4) the basic local marginal price (LMP) from the optimal power flow (OPF) solution [147]. Based on the results of the contingency analysis C and the MTTRP simulations, the operational loss of the each substation outage, denoted as Γ_{1-4}, for these four cases with different settings of costs γ_{1-4}, are given in Fig. 4.3. To improve the readability of the figure, the authors re-scale the unit for each case and specify the amount of the dollars per unit in legends.

4.4.2 Numerical Results of Ruin Probability and Premium Amount

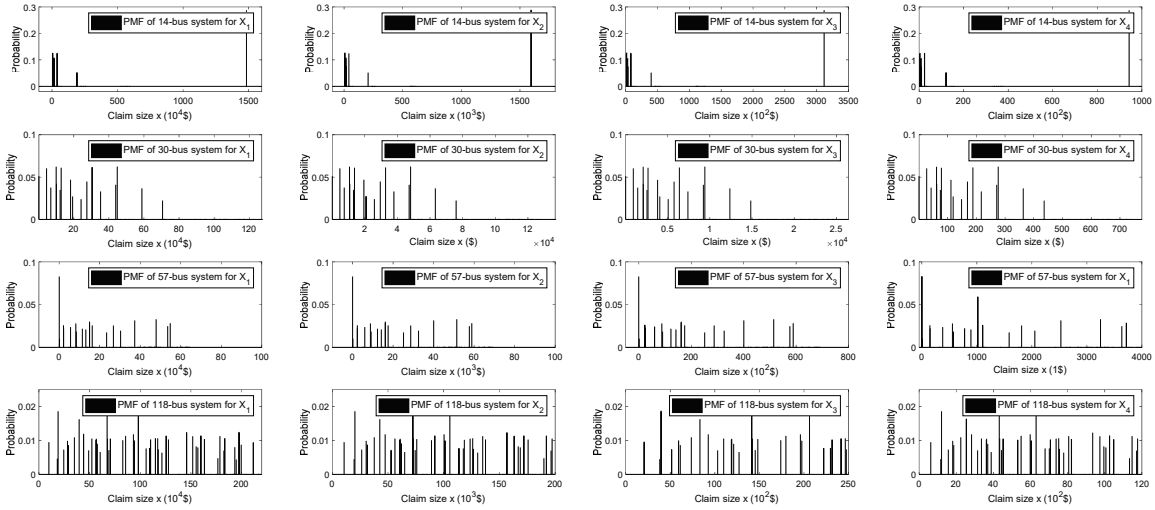

Figure 4.4: The PMF of test cases with diverse settings of γ

Figure. 4.2 presents the distribution function of steady-state probability of substation intrusions and the expected MTTRP for each substation under hypothesized cyberattack. Combining Eqs. 4.9, 4.12 and 4.14 with the diverse settings of direct operational loss, i.e., Γ_{1-4}, as displayed in Fig. 4.3, this section would provide the numerical results of ruin probability and the corresponding premiums.

According to Eqs. 4.4, 4.5 and 4.6, the distributions of PMF for all test cases are given in Fig. 4.4. It is worth noting that cases 1, 2, 3 and 4 denote the test cases with diverse settings of direct operational loss with the corresponding Γ_{1-4}.

In the IEEE 14-bus system, the sample size of the discrete variable L is 29. For

different settings of γ, $X_{1,2,3,4}$ are within the thresholds of [\$38,743, \$14,834,302], [\$4,164, \$1,594,566], [\$813, \$311,665] and [\$246, \$94,224], respectively. It is noticed that the diverse settings of γ would not change the bound of the PMF, $p(x)$, which is [0.000026246, 0.2875]. In Fig. 4.4, the first 100 samples are displayed for the PMF's of the 30-, 57- and 118-bus systems. The sample size of discrete variable X in the 30-bus system is 572, where $X_{1,2,3,4}$ would locate in the intervals [\$1,227, \$15,682,970], [\$131, \$1,685,791], [\$930, \$329,495] and [\$27, \$9,677], respectively. The upper and lower bounds of the PMF are 0.1028 and 4.4912×10^{-9}, respectively. In the 57-bus system, the sample size of variable X is 1,861. The feasible intervals of discrete variables $X_{1,2,3,4}$ are [\$21,490, \$64,279,598], [\$2,310, \$6,909,534], [\$452, \$1,350,500] and [\$146, \$435,919], respectively. The bounds of the PMF for this system is [1.5139×10^{-9}, 0.09925]. Similarly, as for the 118-bus system, there are 3,463 different samples and the corresponding discrete variables $X_{1,2,3,4}$ are in the intervals [\$98,171, \$431,905,449], [\$10,553, \$46,426,319], [\$2,063, \$9,074,235] and [\$630, \$2,770,175], respectively. The upper and lower bounds of the PMF for this system are 0.05104 and 8.6668×10^{-8}, respectively. It is observed that thresholds of the PMF gradually decrease with the increasing sample sizes, constrained to $\sum p(x) = 1$.

By combining Eqs. 4.9, 4.12 and 4.13 with the PMF depicted in Fig. 4.4, the results of ruin probability and the corresponding feasible premium amounts are summarized in Table 4.1. In the table, θ is selected from 0 to 1 with the increment of 0.2. The initial reserve u are selected among 0, 10 and 100, which, refer to Eq. 4.12, would

determine the recursive level for calculating the ruin probability ψ. It is observed that, when u is 0, Eq. 4.12 could be written as $\psi(0) = (1-f_0)/(1+\theta-f_0)$, which only involves the first iteration. In the row of "System constants," parameter λ denotes the frequency of the claim that have been formulated through Eq. 4.3, which is 0.0067, 0.0157, 0.0289, and 0.0724 in the 14-, 30-, 57-, and 118-bus systems, respectively. It is observed that in Eq. 4.12, variable h denotes the general increment for each global moment, here the authors consider the formulation of the proposed problem as a two-moment process which would optimally cover the whole interval of the claim size. It indicates that each interval would cover half of the claim size. To distinguish the general increment h, h' is introduced as the proportion of the coverage.

From Table 4.1, among all the test systems, $\psi(0)$ is always larger than 0.4. It might be "too risky" and may not be an acceptable probability. Additionally, it is found that the ruin probability $\psi(u)$ in each case would be decreasing with θ increased, which coincides with Eq. 4.12. Consider $\psi(0)'$ with a larger θ' and $\psi(0)''$ with a smaller θ'', it can be calculated that for the first ruin probability, it holds: $\psi(0)' < \psi(0)''$. Since the $\psi(u)$ is calculated recursively based on the first item $\psi(0)$, then the probability of $\psi(u)'$ with a larger θ would be eventually smaller than $\psi(u)''$. Therefore, $\psi(u)$ is a decreasing function as θ increases. For this reason, the authors are able to give a reasonable guess of certain ruin probability even without a predetermined value of θ. Take the calculation results of IEEE 30-bus system as an example, even though the ruin probability $\psi(10)$ under the condition of θ = 0.9 is not provided, it

is reasonable to conclude that the probability $\psi(10)$ would locate the interval [1.029 $\times 10^{-4}$, 1.094$\times 10^{-4}$], which are the lower and upper bounds of the probability detailed in the table when $\theta = 0.8$ and 1.0.

According to Eq. 4.14, Table 4.1 also provides the feasible premium amounts for each IEEE test system with different settings of γ, where θ_f is assumed to be 0.8. In a more general case, for example, if the insurance company would be able to accept the ruin probability that less than 5.0 $\times 10^{-4}$ for the 57-bus system, and if the initial reserve is 10 for the costs settings of γ_1, the feasible set of θ can be determined from the table as [0.6, 1.0]. Based on Eq. 4.14, the feasible premium interval [$\mathbf{I}^l$, $\mathbf{I}^u$] could be determined as [\$919,945, \$1,149,931], where $\mathbf{I}^l$ and $\mathbf{I}^u$ denote the lower and upper bound of the premium $\mathbf{I}$ accordingly. Similarly, in the 118-bus system with the initial reserve of 100, if the acceptable range of the ruin probability is less than 2.0$\times 10^{-4}$ and the operational costs are set as γ_2, the tentative range of the θ can be approximately identified to be [0.5, 1.0]. The feasible premium amount $\mathbf{I}$ is determined with the lower bound of \$ 1,622,810 and the upper bound of \$2,163,746.

Table 4.1 The results of ruin probability and feasible premium policy

14-bus system			30-bus system			57-bus system			118-bus system		
u	θ	Ruin Prob.	u	θ	Ruin Prob.	u	θ	Ruin Prob.	u	θ	Ruin Prob.
0	0.2	7.925×10^{-1}	0	0.2	7.775×10^{-1}	0	0.2	7.965×10^{-1}	0	0.2	8.802×10^{-1}
	0.4	6.563×10^{-1}		0.4	6.360×10^{-1}		0.4	6.618×10^{-1}		0.4	6.706×10^{-1}
	0.6	5.601×10^{-1}		0.6	5.381×10^{-1}		0.6	5.660×10^{-1}		0.6	5.758×10^{-1}
	0.8	4.885×10^{-1}		0.8	4.663×10^{-1}		0.8	4.945×10^{-1}		0.8	5.044×10^{-1}
	1.0	4.331×10^{-1}		1.0	4.114×10^{-1}		1.0	4.390×10^{-1}		1.0	4.488×10^{-1}
10	0.2	4.005×10^{-3}	10	0.2	1.879×10^{-2}	10	0.2	2.076×10^{-2}	10	0.2	3.023×10^{-4}
	0.4	3.469×10^{-3}		0.4	2.374×10^{-3}		0.4	2.868×10^{-3}		0.4	2.248×10^{-4}
	0.6	3.149×10^{-3}		0.6	4.783×10^{-4}		0.6	4.925×10^{-4}		0.6	1.906×10^{-4}
	0.8	2.887×10^{-3}		0.8	1.029×10^{-4}		0.8	9.674×10^{-5}		0.8	1.665×10^{-4}
	1.0	2.662×10^{-3}		1.0	1.094×10^{-4}		1.0	2.061×10^{-5}		1.0	1.571×10^{-4}
100	0.2	3.900×10^{-3}	100	0.2	1.688×10^{-4}	100	0.2	2.779×10^{-6}	100	0.2	2.294×10^{-4}
	0.4	3.469×10^{-3}		0.4	1.500×10^{-4}		0.4	1.806×10^{-6}		0.4	2.068×10^{-4}
	0.6	3.165×10^{-3}		0.6	1.350×10^{-4}		0.6	1.597×10^{-6}		0.6	1.882×10^{-4}
	0.8	2.892×10^{-3}		0.8	1.227×10^{-4}		0.8	1.461×10^{-6}		0.8	1.727×10^{-4}
	1.0	2.662×10^{-3}		1.0	1.125×10^{-4}		1.0	1.347×10^{-6}		1.0	1.596×10^{-4}
Const.	λ	0.0067	Const.	λ	0.0157	Const.	λ	0.0289	Const.	λ	0.0724
	h'	50%		h'	50%		h'	50%		h'	50%
μ($)	1	4,467,000	μ($)	1	3,166,400	μ($)	1	19,895,000	μ($)	1	139,010,000
	2	$480,170		2	$340,360		2	2,138,600		2	14,943,000
	3	$93,851		3	$66,525		3	418,000		3	$2,920,600
	4	28,373		4	$1,954		4	$134,920		4	891,590
I($)	1	53,872	**I**($)	1	894,826	**I**($)	1	1,034,938	**I**($)	1	18,115,783
	2	5,791		2	9,619		2	11,250		2	1,947,372
	3	1,132		3	1,880		3	21,744		3	380,613
	4	342		4	55		4	7,019		4	11,6192

Chapter 5

Conclusion

Improving the cyber-situation awareness of the control centers throughout an interconnection can be challenging. Emerging, renewable energy sources increase the uncertainty of entire power networks, as well as local networks. This uncertainty raises the possibility of unexpected incidents in future networks. The cybersecurity of a power grid is also a topic of research that enables asset owners to anticipate cascading failure as well as identify interdependencies due to cyber-related initiating events. We are in an era where intelligent cyberattackers are emerging with the cross-domain knowledge to execute an attack plan against power grids. In such attacks, attackers may not have enough or complete information about the grid to assure the success of their attack plan. Defenders can reduce risks to power infrastructure with improved security analytics in order to anticipate attacks with serious consequences,

and thus strategically deploy additional security protections to critical substations and components.

The dissertation starts to review the cyber-related contingency analysis and summarizes the steady-state and dynamic stability concerns of the contingency. The following chapters then introduce a cyber-risk assessment model, which includes the implementation of derived metrics on combinations of hypothesized outages with verification of steady-state and dynamic system simulations. The reduction of permutations and combinations of the hypothesized scenarios can be explored to determine its practicality and systemic bottleneck assessment in order to identify the pivotal components/substations of a power grid. The preliminary cyber insurance premium model has also been demonstrated in the dissertation, which reveals that understanding the impact of a cyberattack event is significant for developing a feasible cyber risk coverage solution.

5.1 Cyber-Risk Assessment Framework

This work extends the previous RPM model by incorporating enumerative combinations to quantify cyber-based contingencies with hypothesized substation outages and incurred overloads. The evaluation is proceeded to ensure the coverage of all critical "worst-case" substations combinations are identified at each level k and the subsets of

nonconvergent substations combinations are excluded for k-1 level to avoid the explosion of combinations, which is also defined as S-k contingency. The validation of its application has been greatly extended by incorporating steady-state load flow evaluation. The consideration of islanding formations after presumption of hypothesized substation attacks are also modeled in this study. A comparable analysis towards the simulation performance in between serial and parallel computing modes has been established based on a platform of the superior computing cluster. This research also provides two aspects to decompose combinatorial evaluation with a curve fitting function to estimate time with respect to the available computing resources as well as utilization of computing memory to speed up, which may prove the feasibility of future implementation and estimate the ballpark number of how much time it would take for a larger system.

In order to improve the feasibility of the cyber-risk assessment model, evaluating the impact of the critical protective relay(s) is required to be included, which is defined as R-k contingency. This research verifies the computational outcomes of disruptive switching attacks and combinations using the power flow and time-domain dynamic simulations. The consistency of the results between the dynamic and static studies has been exhibited in the study. It is observed that the time-domain simulation provides more details of the behaviors on the relays based on the initial event (hypothetical switching attack scenarios through digital relays). Compared with the dynamic simulation, the computation of power flow studies (steady-state analysis) takes less time

and computing resources. Hence, this reliably serves as a means to pre-screen larger combinations. The results also demonstrate promising outcomes and can be further explored for online applications to identify the critical protective relays.

The "routable" keyword in the latest NERC CIP compliance implies the limitation of firewalls. This proposed model would be a tremendous interest from a perspective of asset owners where they can identify pivotal substations/relays as suggested in this cyber-induced contingency analysis that might initiate cascading failure. They could then thwart electronic intrusion by deploying unidirectional gateway while not compromising data exchange between the substations and control center. This would eliminate the possibilities of cyberintrusion from outsides. This method can also help to prioritize their investment according to the substation criticality, based on the annual budget they could expense each year.

5.2 Cyber Insurance Premium Framework

The insurance would serve as an effective incentive to improve the cybersecurity parameters of the utilities' infrastructures or devices. The cyber insurance market for power grids remains in an emerging stage and it is yet to mature. Based on the previous risk-assessment model, the preliminary establishment of cyber insurance premium using IEEE test cases has demonstrated the promise of actuary and its correlation

to the potential problematic combinations of disruptive switching cyberattacks. The studies provide the simulation results of steady-state probability and its distribution function, the expected mean time to recover power (MTTRP) for each substation, and the diverse settings of estimated operation loss. All factors provided here are the necessary setups to calculate the ruin probability. The ruin probability is applied in the study to evaluate the management performance of the insurance company in the long-term operation. With the detailed and numerous cases provided in the studies, the insurance companies can formulate the feasible premium amounts based on their owner-defined conditions and their base cases.

5.3 Future Work

The future research on the cyber-assessement model will incorporate the current model into the online application of the power system operation, which would include two main functions: (1) online assess and update the cyber reliability of the system before an attack occurs and (2) restrict the level of physical impact after an attack occurs. Defenders may not be able to predict the attackers' behaviors or their strategies, which would induce coordinating attacks on multiple "weak points" and lead to cascading failures. Additionally, the independence study on the intrusion stability in the insurance model would also be investigated in the future work.

5.3.1 Online Cyber-Risk Assessment with Applications of Wide-area Protection Schemes

"More and more functions are moved from local and regional control centers toward the central or national control center [159]." This statement has clarified the major difference between the wide-area protection schemes and the traditional protection schemes. The proposed cyber-risk assessment model is implemented on the network of the wide-area protection scheme. Based on the real-time data, such as inputs of loads, bus voltages, and power sources, collected from the wide-area measurement system (WAMS) [159], the cyber-risk assessment model might perform exhaustively evaluations using both static and dynamic analyses. A reliability-related log file would be generated with potential critical infrastructures and high risky electrical devices included. With the given set of time intervals for sampling, operational logs are collected and analyzed, which can be used to evaluate the performance of the accuracy and consistency of the wide-area protection scheme based on statistical studies.

5.3.2 Cyber Impact Restriction Framework

The proposed online framework would introduce an improved algorithm of *k-medoids* clustering/partitioning method using (1) system indicators of electrical quantities collected from the WAMS and (2) the list of critical infrastructures from the risk assessment model. Once an attack occurs, compromised infrastructures or electrical equipment are selected as k center nodes. For each point, the proposed algorithm would resolve a set of optimization functions and generate a feasible parameter of outages that would minimize the impact of the attack. The wide-area protection scheme would then perform the "operation" algorithm and disconnect loads, generators, transmission lines, and transformers as needed to restrict the fault area.

5.3.3 Local Power Restoration with Incorporating Stability Constraints

It is possible that the results from the previous section may not necessarily be the optimal solution as the "operation" report may include the potential risky electrical components that have not been compromised and may not cause cascading failures. The local power restoration algorithm is implemented in the framework to examine the performance *k-medoids* clustering algorithm and pick up local loads/generators

and reclose circuit breakers to connect transmission lines back to the system with satisfying the constraints of power system transient/steady-state stability. Additionally, due to stability constraints, the reclosure procedure would further reduce the cyber impact level by recharging and synchronizing isolated islands.

5.3.4 Improvement on the Cyber Insurance Model with Independence Implications

The future study on the cyber insurance framework will investigate the independence research. The original PMF introduced in the Chapter 4 needs to be modified by incorporating: (1) the specific and realistic cyberattack paths through a single or multiple substations based on the network topology of the system; (2) the historical and statistical data observed from previous physical blackout/brownout scenarios, such as N-1, N-2, or N-k contingencies events, to formulate a verified potential dependent connections within certain contingencies events; and (3) the close-connected relationship among multiple control areas in a large power grid network in terms of cascading failures.

References

[1] C.-W. Ten, K. Yamashita, Z. Yang, A. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4405–4425, Sep. 2018.

[2] D. Veluz, "Stuxnet malware targets SCADA systems," Oct. 2010. [Online]. Available: http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

[3] E. Perez, "First on CNN: U.S. investigators find proof of cyberattack on Ukraine power grid," Feb. 3 2016. [Online]. Available: http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/

[4] Cable News Network (CNN), "Sources: Staged cyber attack reveals vulnerability in power grid," Sep. 26 2007. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

[5] S. Reilly, "USA Today records: Energy department struck by cyber attacks,"

Sep. 11 2015. [Online]. Available: http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/

[6] Idaho National Laboratory, "Mission support center analysis report: Cyber threat and vulnerability analysis of the u.s. electric sector," Aug. 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

[7] J. Berr, ""wannacry" ransomware attack losses could reach $4 billion," May 16 2017. [Online]. Available: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

[8] Industrial Control Systems Cyber Emergency Response Team (ICSCERT), "Cyber-attack against ukrainian critical infrastructure," Feb. 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[9] Electricity Information Sharing and Anlaysis Center (E-ISAC), "Analysis of the cyber attack on the ukrainian power grid," Mar. 18 2016. [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[10] K. Zetter, "Everything we know about ukraines power plant hack," Jan. 20 2016. [Online]. Available: http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[11] ICS-CERT Alert (IR-ALERT-H-16-056-01), "Cyber-attack against ukrainian critical infrastructure," Feb. 25 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[12] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), "Overview of cyber vulnerabilities." [Online]. Available: https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[13] Power system relaying and substations committees, "IEEE standard cybersecurity requirements for substsation automation, protection, and control systems," in *IEEE PES Std C37.240-2014*, IEEE-SA standards board, Dec. 2014, pp. 1–38.

[14] S. Bricker, T. Gonen, and L. Rubin, "Substation automation technologies and advantages," *IEEE Comput. Appl. Power*, vol. 14, no. 3, pp. 31–37, Jul. 2001.

[15] Office of the Press Secretary, The White House, "Executive order – commission on enhancing national cybersecurity," Feb. 9 2016. [Online]. Available: https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

[16] Federal Register, "Executive order 13636 – improving critical infrastructure cybersecurity," Feb. 19 2013. [Online]. Available: http://www.gsa.gov/portal/mediaId/176567/fileName/ATTCH_1_-_CyberEO\discretionary{-}{}{}FedReg.action

[17] National Institute of Standards and Technology (NIST), "Improving critical infrastructure cybersecurity executive order 13636: Preliminary cybersecurity framework," Jun. 2013. [Online]. Available: https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf

[18] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems – attacks, impacts, and defense: A survey," vol. 13, no. 2, pp. 411–423, Apr. 2017.

[19] NERC Board of Trustees, "Cyber attack task force: Final report," May 2012. [Online]. Available: http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf

[20] ——, "Reliability standards for the bulk electric systems of north america," Feb. 15 2018. [Online]. Available: http://www.nerc.com/pa/Stand/ReliabilityStandardsCompleteSet/RSCompleteSet.pdf

[21] R. Kuckro, "Simulated cyberattack takes down u.s. power grid," Nov. 15 2013. [Online]. Available: http://www.utilitydive.com/news/simulated-cyberattack-takes-down-us-power-grid/195153/

[22] M. Sahraei-Ardakani, X. Li, P. Balasubramanian, K. W. Hedman, and M. Abdi-Khorsand, "Real-time contingency analysis with transmission switching on real power system data," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2501–2502, May 2016.

[23] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669–683, Mar. 2016.

[24] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

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

[26] L. Pietre-Cambacedes, M. Tritschler, and G. N. Ericsson, "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs," *IEEE Trans. Power Del.*, vol. 26, no. 1, pp. 161–172, Jan. 2011.

[27] M. A. C. Camargo, A. J. Rivera, and R. R. Pea, "Impact assessment of substation contingencies in power systems," in *Transmission Distribution Conference and Exposition - Latin America (PES T D-LA), 2014 IEEE PES*, Medellin, Sep. 2014, pp. 1–6.

[28] S. H. Song, S. H. Lee, T. K. Oh, and J. Lee, "Risk-based contingency analysis for transmission and substation planning," in *Proc. IEEE Trans. Dist. Conf. Exposition: Asia and Pacific*, Seoul, Oct. 2009, pp. 1–4.

[29] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power

grid critical infrastructures," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790–1799, Dec. 2012.

[30] R. Bulbul, Y. Gong, C.-W. Ten, A. Ginter, and S. Mei, "Impact quantification of hypothesized attack scenarios on bus differential relays," in *Proc. IEEE Power Systems Computation Conference (PSCC)*, Wroclaw, Poland, Aug. 2014, pp. 1–7.

[31] Q. Chen and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 823–834, Nov. 2005.

[32] NERC, "Reliability concepts," Dec. 19 2007. [Online]. Available: http://www.nerc.com/files/concepts_v1.0.2.pdf

[33] H. Wardak, S. Zhioua, and A. Almulhem, "PLC access control: a security analysis," in *Proc. 2016 World Congress on Industrial Control Systems Security (WCICSS)*, London, UK, Dec. 2016, pp. 1–6.

[34] J. Hong, C.-C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *Innovative Smart Grid Technologies (ISGT), 2014 IEEE PES*, Feb. 2014, pp. 1–5.

[35] G. N. Ericsson, "Cyber security and power system communication – essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.

[36] M. Govindarasu, A. Hahn, and P. Sauer, *Cyber-Physical Systems Security for Smart Grid: Future Grid Initiative White Paper*, 1st ed. (Power Systems Engineering Research Center) PSERC, 2012.

[37] Critical Infrastructure Protection Committee (CIPC), "Cybersecurity – bes cyber system categorization," Oct. 26 2012. [Online]. Available: http://www.netsectech.com/wp-content/uploads/2013/05/Version-5-of-the-NERC-CIP-Cyber-Security-Standards.pdf

[38] Agence nationale de la sécurité des systèmes d'information (ANSSI), "Classification method and key measures," Jan. 2014. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

[39] ——, "Detailed measures," Jan. 2014. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf

[40] National Institute of Standards and Technology (NIST), "Cybersecurity framework workshop 2017 summary," Jul. 2017. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2017/07/21/cybersecurity_framework_workshop_2017_summary_20170721_1.pdf

[41] Federal Energy Regulatory Commission (FERC). (Jul. 19, 2018) Cyber security incident reporting reliability standards. 888 First Street, NE Washington,

DC. [Online]. Available: https://www.ferc.gov/whats-new/comm-meet/2018/071918/E-1.pdf

[42] Z. Yang and C.-W.Ten, "Cyber-induced risk modeling for microprocessor-based relays in substations," in *Proc. 2018 IEEE Conf. Innov. Smart Grid Technol.–Asia (ISGT–Asia)*, Singapore, May 2018, pp. 856–861.

[43] Vaiman, Bell, Chen, Chowdhury, Dobson, Hines, Papic, Miller, and Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, May 2012.

[44] J. J. Meeuwsen and W. L. Kling, "Substation reliability evaluation including switching actions with redundant components," *IEEE Trans. Power Del.*, vol. 12, no. 4, pp. 1472–1479, Oct. 1997.

[45] Z. Yang, C. W. Ten, and A. Ginter, "Extended enumeration of hypothesized substations outages incorporating overload implication," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6929–6938, Nov. 2018.

[46] Z. Yang and C.-W.Ten, "Assessment of hypothesized substation cyberattack using linearized power flow approach," in *Proc. 2017 IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Washington, DC, Apr. 2017, pp. 1–5.

[47] P. M. Anderson, *Power System Protection*, 1st ed. New York, USA: The Institute of Eelctrical and Electronics Engineers, INC.

[48] A. G. Phadke and J. S. Thorp, "Expose hidden failures to prevent cascading outages," *IEEE Comput. Appl. Power*, vol. 9, no. 3, pp. 20–23, Jul. 1996.

[49] W. S. Baer and A. Parkinson, "Cyberinsurance in it security management," *IEEE Security Privacy*, vol. 5, no. 3, pp. 50–56, May 2007.

[50] U.S. Department of Energy and the Critical Infrastructure Protection Program of George Mason University School of Law. (Jun. 21, 2005) Insurance and the nations electrical infrastructure: Mutual understanding and maturing relationships. George Mason University School of Law, Arlington, VA. [Online]. Available: https://cip.gmu.edu/wp-content/uploads/2016/06/CIPHS_Insurance-and-the-Nations-Electrical-Infrastructure_White-Paper.pdf

[51] European Network and Information Security Agency, "Incentives and barriers of the cyber insurance market in europe," Jun. 28 2012. [Online]. Available: http://www.biztositasiszemle.hu/files/201207/cyber_insurance_market.pdf

[52] U.S. Department of Homeland Security, "Cybersecurity insurance." [Online]. Available: https://www.dhs.gov/cybersecurity-insurance

[53] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating risk with cyberinsurance," *IEEE Security Privacy*, vol. 13, no. 6, pp. 38–43, Nov. 2015.

[54] M. Xu and L. Hua, "Cybersecurity insurance: Modeling and pricing," Mar. 2017. [Online]. Available: https://www.soa.org/Files/Research/Projects/cybersecurity-insurance-report.pdf

[55] R. Böhme and G. Kataria, "Models and measures for correlation in cyber-insurance," in *Workshop on the Economics of Information Security (WEIS)*, University of Cambridge, UK, Jun. 2006, pp. 1–26.

[56] R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Workshop on the Economics of Information Security (WEIS)*, Harvard University, USA, Jun. 2010, pp. 1–36.

[57] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive cyber-insurance and internet security," in *Economics of Information Security and Privacy*, T. Moore, D. Pym, and C. Ioannidis, Eds. Boston, MA: Springer US, 2010, pp. 229–247.

[58] G. Schwartz, N. Shetty, and J. Walrand, "Cyber-insurance: Missing market driven by user heterogeneity," in *Workshop on the Economics of Information Security (WEIS)*, Harvard University, USA, Jun. 2010, pp. 1–17.

[59] Department of Energy, "Electric grid security and resilience: Establishing a baseline for adversarial threats," Jun. 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

[60] Lloyd's and the University of Cambridge. (2015) Business blackout: The insurance implications of a cyber attack on the

U.S. power grid. Emerging Risk Report 2015. [Online]. Available: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf

[61] E. L. Webb, "The internet of things: Cybersecurity, insurance, and the national power grid," *Natural Resources & Environment*, vol. 30, no. 4, pp. 1–5, Spring 2016.

[62] U.S. Department of Homeland Security. (2014) Insurance for cyberrelated critical infrastructure loss: Key issues. Insurance Industry Working Session Readout Report. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20Industry%20Working%20Session_1.pdf

[63] P. Emberchts, C. Klüppelberg, and T. Mikosch, *Risk Theory.* Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 21–57. [Online]. Available: https://doi.org/10.1007/978-3-642-33483-2_2

[64] H. H. Panjer, "Direct calculation of ruin probabilities," *J. Risk and Insurance*, vol. 53, no. 3, pp. 521–529, Sep. 1986.

[65] T. Pentikäinen, "The theory of risk and some applications," *J. Risk and Insurance*, vol. 47, no. 1, pp. 16–43, Mar. 1980.

[66] F. Dufresne and H. U. Gerber, "Three methods to calculate the probability of ruin," *ASTIN Bulletin*, vol. 19, no. 1, pp. 71–90, 1989.

[67] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA system," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[68] ——, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," in *Proc. 2007 IEEE Power Eng. Soc. General Meeting*, Jun. 2007, pp. 1–8.

[69] S. Dahal, S. Paudyal, and J. Wang, "Investigating the factors affecting state estimation of emerging distribution grids," in *2018 Australasian Universities Power Eng. Conf. (AUPEC)*, Auckland, New Zealand, Nov. 2018, pp. 1–6.

[70] J. Wang, G. R. Bharati, S. Paudyal, O. Ceylan, B. P. Bhattarai, and K. S. Myers, "Coordinated electric vehicle charging with reactive power support to distribution grids," *IEEE Trans. Ind. Informat.*, to be published.

[71] Y. Tang, C.-W. Ten, C. Wang, and G. Parker, "Extraction of energy information from analog meters using image processing," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 2032–2040, Jul. 2015.

[72] Y. Tang, S. Zhao, C.-W. Ten, and K. Zhang, "Enhancement of distribution load modeling using statistical hybrid regression," in *Proc. 2017 IEEE PES Conf. Innov. Smart Grid Technol. (ISGT)*, Washington, DC, Apr. 2017, pp. 1–5.

[73] Y. Tang, C.-W. Ten, and L. E. Brown, "Switching reconfiguration of fraud

detection within an electrical distribution network," in *Proc. 2017 Resilience Week (RWS)*, Wilmington, DE, USA, Sep. 2017, pp. 206–212.

[74] C.-W. Ten and Y. Tang, *Electric Power Distributed Emergency Operation*, 1st ed. CRC Press, 2018.

[75] Government Accountability Office (GAO) Report to Congressional Requesters, "Critical infrastructure protection: Multiple efforts to secure control systems are under way, but challenges remain," vol. GAO-07-1036, Sep. 2007.

[76] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Atlantic City, NJ, USA, Oct. 2005, pp. 1–9.

[77] B. F. D. H. S. Almond, S. Baird and A. Mackrell, "Integrated protection and control communications outwith the substation: Cybersecurity challenges," in *Proc. IET 9th Intl. Conf. on Developments in Power Syst. Protection (DPSP)*, Mar. 2008, pp. 698–701.

[78] M. Wei and Z. Chen, "Reliability analysis of cybersecurity in an electrical power system associated wan," in *Proc. IEEE PES General Meeting*, San Diego, CA, USA, Jul. 2012, pp. 1–6.

[79] R. Kuckro, "Simulated cyberattack takes down u.s. power grid,"

Nov. 15 2013. [Online]. Available: https://www.utilitydive.com/news/simulated-cyberattack-takes-down-us-power-grid/195153/

[80] North American Electric Reliability Corporation (NERC), "State of reliability 2013," May 2013. [Online]. Available: https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013_SOR_May%2015.pdf

[81] X. Xu, B. P. Lam, R. R. Austria, Z. Ma, Z. Zhu, R. Zhu, and J. Hu, "Reliability analysis of cybersecurity in an electrical power system associated wan," in *Proc. Intl. Conf. on Power Syst. Tech*, Kunming, China, Jul. 2002, pp. 844–848 vol.2.

[82] X. Xu, F. Dong, L. Huang, and B. P. Lam, "Modeling and simulation of substation-related outages in power flow analysis," in *Proc. 2010 Intl. Conf. on Power Syst. Tech.*, Hangzhou, China, Oct. 2010, pp. 1–5.

[83] K. Sun and Z.-X. Han, "Analysis and comparison on several kinds of models of cascading failure in power system," in *Proc. Trans. and Dist. Conf. and Exhibition: Asia and Pacific, IEEE PES, 2005*, Dalian, China, Aug. 2005, pp. 1–7.

[84] L. Zongxiang, M. Zhongwei, and Z. Shuangxi, "Cascading failure analysis of bulk power system using small-world network model," in *Proc. Intl. Conf. on Probabilistic Methods Applied to Power Syst.*, Ames, IA, USA, Sep. 2004, pp. 635–640.

[85] Q. Chen, C. Jiang, W. Qiu, and J. McCalley, "Probability models for estimating

the probabilities of cascading outages in high-voltage transmission network," *IEEE Trans. Power Syst.*, vol. 21, no. 3, Aug. 2006.

[86] G. C. Ejebe, C. Jing, J. G. Waight, V. Vittal, G. Pieper, F. Jamshidian, P. Hirsch, and D. Sobajic, "Online dynamic security assessment in an EMS," *IEEE Comput. Appl. Power*, vol. 11, no. 1, pp. 43–47, Jan. 1998.

[87] B. F. W. A. J. Wood and G. B. Sheble, *Power Generation Operation and Control*, 3rd ed. Wiley, 2014.

[88] G. C. Ejebe and B. F. Wollenberg, "Automatic contingency selection," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no. 1, pp. 97–109, Jan. 1979.

[89] G. C. Ejebe, R. F. Paliza, and W. F. Tinney, "An adaptive localization method for real-time security analysis," *IEEE Trans. Power Syst.*, vol. 7, no. 2, pp. 777–783, May 1992.

[90] V. Brandwajn, "Efficient bounding method for linear contingency analysis," *IEEE Trans. Power Syst.*, vol. 3, no. 1, pp. 38–43, Jan. 1998.

[91] J. Hazra and A. Sinha, "Identification of catastrophic failures in power system using pattern recognition and fuzzy estimation," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 378–387, Jan. 2009.

[92] Q. Chen and J. McCalley, "Identifying high risk n-k contingencies for on-line

security assessment," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 823–834, May 2005.

[93] C. Davis and T. Overbye, "Multiple element contingency screening," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1294–1301, Aug. 2011.

[94] Federal Energy Regulatory Commission, DOE, "Mandatory reliability standards for the bulk-power system," March 16 2007. [Online]. Available: https://www.ferc.gov/whats-new/comm-meet/2007/031507/E-13.pdf

[95] NERC Board of Trustees, "System performance following loss of two or more BES elements," Apr. 2005. [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/TPL-003-0(i)b.pdf

[96] T. Mikolinnas and B. Wollenberg, "An advanced contingency selection algorithm," *IEEE Trans. Power Syst.*, vol. PAS-100, no. 2, pp. 608–617, Feb. 1981.

[97] G. Irisarri and A. Sasson, "An automatic contingency selection method for on-line security analysis," *IEEE Trans. Power Syst.*, vol. PAS-100, no. 4, pp. 1838–1844, Apr. 1981.

[98] M. Enns, J. Quada, and B. Sacket, "Fast linear contingency analysis," *IEEE Trans. Power Syst.*, vol. PAS-101, no. 4, pp. 783–791, Apr. 1982.

[99] B. Stott, O. Alsac, and F. Alvarado, "Analytical and computational improvements in performance index ranking algorithms for networks," *Intl. Journal of Elec. Power & Energy Syst*, vol. 7, no. 3, pp. 154–160, Jul. 1985.

[100] G. Ejebe, H. V. Meeteren, B. Wollenberg, and H. P. V. Meeteren, "Fast contingency screening and evaluation for voltage security analysis," *IEEE Trans. Power Syst.*, vol. 3, no. 4, pp. 1582–1590, Nov. 1998.

[101] Q. Chen and D. McCalley, "Identifying high risk n-k contingencies for online security assessment," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 823–834, May 2005.

[102] T. Guler and G. Gross, "Detection of island formation and identification of causal factors under multiple line outages," *IEEE Trans. Power Syst.*, vol. 22, no. 2, pp. 505–513, May 2007.

[103] CIGRE C2, "CIGRE session paris 2006: Workshop on large disturbances." [Online]. Available: http://c2.cigre.org/content/download/10140/325796/version/1/file/SC+C2+Minutes+of+Meeting+in+Paris060831ID44VER15.pdf

[104] ——, "CIGRE session paris 2008: Workshop on large disturbances." [Online]. Available: http://c2.cigre.org/What-is-SC-C2/Official-SC-C2-Documents

[105] ——, "CIGRE session paris 2010: Workshop on large disturbances." [Online]. Available: http://www.cigre.org/Events/Session/Session-2010

[106] ——, "CIGRE session paris 2012: Workshop on large disturbances." [Online]. Available: http://c2.cigre.org/Publications/Session-Papers

[107] CIGRE C2 and C5, "CIGRE session paris 2014: Workshop on large disturbances." [Online]. Available: http://www.hro-cigre.hr/session_45_reports_workshop_on_large_disturbance

[108] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *proc. 1st IEEE Intl. Workshop on Smart Grid Modeling and Simulation (SGMS)*, Brussels, Belgium, Oct. 2011, pp. 49–54.

[109] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, May 2012.

[110] D. Gerbec, S. Gasperic, I. Smon, and F. Gubina, "Determining the load profiles of consumers based on fuzzy logic and probability neural networks," *IEEE Trans. Power Syst.*, vol. 151, no. 3, pp. 395–400, May 2004.

[111] R. Bulbul, C.-W. Ten, and A. Ginter, "Cyber-contingency evaluation for multiple hypothesized substation outages," in *Proc. Innovative Smart Grid Technologies Conference (ISGT), IEEE PES*, Washington, DC, USA, Feb. 2014, pp. 1–5.

[112] ——, "Risk evaluation for hypothesized multiple busbar outages," in *Proc. IEEE PES General Meeting Conf. and Exposition*, National Harbor, MD, USA, Jul. 2014, pp. 1–5.

[113] J. Stamp, A. McIntyre, and B. Ricardson, "Reliability impacts from cyberattack on electric power systems," in *Proc. IEEE PES Power Systems Conference and Exposition*, Seattle, WA, USA, Mar. 2009, pp. 1–8.

[114] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[115] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids," in *Proc. IEEE PES General Meeting*, National Harbor, MD, USA, Jul. 2014, pp. 1–5.

[116] A. Stefanov and C.-C. Liu, "Cyber-power system security in a smart grid environment," in *Proc. Innovative Smart Grid Technologies Conference (ISGT), IEEE PES*, Washington, DC, USA, Jan. 2012, pp. 1–3.

[117] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jan. 2013.

[118] C. Wang, C. W. Ten, Y. Hou, and A. Ginter, "Cyber inference system for

substation anomalies against alter-and-hide attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 896–909, Mar. 2017.

[119] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2015.

[120] C.-C. L. J. Yan, M. Govindarasu and U. Vaidya, "A pmu-based risk assessment framework for power control systems," in *Proc. IEEE PES General Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.

[121] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *Proc. IEEE Conf. on Comp. Comm.*, Toronto, ON, Canada, May. 2014, pp. 2625–2633.

[122] B. Chen, K. L. Butler-Purry, and D. Kundur, "Impact analysis of transient stability due to cyber attack on facts devices," in *Proc. North American Power Symposium (NAPS)*, Manhattan, KS, USA, Sep. 2013, pp. 1–6.

[123] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proc. IEEE PES General Meeting*, Vancouver, BC, Canada, Jul. 2013, pp. 1–5.

[124] P. M. Esfahani, M. Vrakopoulou, G. Andersson, and J. Lygeros, "A tractable

nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems," in *Proc. 51st IEEE Conf. Decision Control (CDC)*, Maui, HI, USA, Dec. 2012, pp. 3433–3438.

[125] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in rtds and opnet," in *Proc. North American Power Symposium (NAPS)*, Manhattan, KS, USA, Sep. 2014, pp. 1–6.

[126] H. Li and Z. Han, "Manipulating the electricity power market via jamming the price signaling in smart grid," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Houston, TX, USA, Dec. 2011, pp. 1168–1172.

[127] L. A. Dunstan, "Digital load flow studies," *Trans. American IEE. Part III: Power App. Syst.*, vol. 73, no. 1, pp. 825–832, Jan. 1954.

[128] F. F. Wu, "Theoretical study of the convergence of the fast decoupled load flow," *IEEE Trans. Power App. Syst.*, vol. 96, no. 1, pp. 268–275, Jan. 1977.

[129] V. Ajjarapu and C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," *IEEE Trans. Power Syst.*, vol. 7, no. 1, pp. 416–423, Feb. 1992.

[130] M. Rios, K. Bell, D. Kirschen, and R. Allan. (1999) Computation of the value of security. Mannchester Centre for Electrical Energy, UMIST.

[Online]. Available: http://www2.ee.washington.edu/research/real/Library/Reports/Value_of_Security_Part_I.pdf

[131] P. Rezaei. (2015) Cascading failure risk estimation and mitigation in power systems. University of Vermont. [Online]. Available: http://scholarworks.uvm.edu/cgi/viewcontent.cgi?article=1481&context=\graddis

[132] J. L. Blackburn and T. J. Domin, *Protective Relaying: principles and applications*, 4th ed. CRC press, 2014.

[133] M. J. Eppstein and P. D. H. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[134] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 285–297, Jan. 2015.

[135] Vaiman, Bell, Chen, Chowdhury, Dobson, Hines, Papic, Miller, and Zhan, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, May 2012.

[136] IEC 61850-7-4 Edition 2.0, *Communication Networks and Systems for Power Utility Automation Part 7-4: Basic Communication Structure–Compatible logical node classes and data object classes.*

[137] IEC 61850-8-1, *Communication networks and systems for power utility automation–Part 8–1: Specific communication service mapping (SCSM)–Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, 2nd ed.

[138] IEC 61850-9-2 LE, *Implementation Guideline for Digital Interface to Instrument transformers Using IEC 61850-9-2*, 2nd ed. UCA International Users Group., Sep. 2011.

[139] US-CERT Alert (TA18-074A), "Russian government cyber activity targeting energy and other critical infrastructure sectors," Mar. 15 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-074A

[140] ICS-CERT, "Mar-17-352-01 hatman-safety system targeted malware (update a)," Apr. 10 2018. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20A%29_S508C.PDF

[141] Cable News Network (CNN), "Shodan: The scariest search engine on the internet," Apr. 8 2013. [Online]. Available: http://money.cnn.com/2013/04/08/technology/security/shodan/index.html

[142] NMAP.ORG, "Chapter 15. nmap reference guide," Mar. 25 2011. [Online]. Available: https://nmap.org/book/man.html

[143] R. Sharpe and E. Warnicke, "Wireshark users guide," Nov. 9 2014. [Online]. Available: https://www.wireshark.org/docs/wsug_html/

[144] S. Ward and et al., "Cyber security issues for protective relays; c1 working group members of power system relaying committee," in *Proc. 2007 IEEE Power Eng. Soc. General Meeting*, Tampa, FL, USA, Jun. 2007, pp. 1–8.

[145] Power System Stability Study Group, *Integrated Analysis Software for Bulk Power System Stability.* CRIEPI Report: ET90002, Jul. 1991.

[146] Meter, Relay and Instrucment Division, *Protective Relays Application Guide*, 1st ed. The English Electric Company Limited, 1968.

[147] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[148] Electric Reliability Council of Texas, Inc. (Jun. 1, 2018) ERCOT nodal operating guides, section 2: system operations and control requirements. [Online]. Available: http://www.ercot.com/content/wcm/current_guides/53525/02-060118.doc

[149] U.S. Congress, Office of Technology Assessment. (Jun. 1990) Physical vulnerability of electric system to natural disasters and sabotage. OTA-E-453, Washington DC. U.S, Government Printing Office. [Online]. Available: http://ota.fas.org/reports/9034.pdf

[150] K. K. Kariuki and R. N. Allan, "Evaluation of reliability worth and value of lost load," *IEE Proc. Generation, Transmission and Distribution*, vol. 143, no. 2, pp. 171–180, Mar. 1996.

[151] London Economics International LLC, "Estimating the value of lost load," Jun. 17, 2013. [Online]. Available: http://www.ercot.com/content/gridinfo/resource/2015/mktanalysis/ERCOT_ValueofLostLoad_LiteratureReviewandMacroeconomic.pdf

[152] STATISTA, "Average retail electricity prices in the U.S. from 1990 to 2017 (in U.S. cents per kilowatt hour)," 2018. [Online]. Available: https://www.statista.com/statistics/183700/us-average-retail-electricity-price-since-1990/

[153] R. A. Ponrajah and F. D. Galiana, "Derivation and applications of optimum bus incremental costs in power system operation and planning," *IEEE Trans. Power App. Syst.*, vol. PAS-104, no. 12, pp. 3416–3422, Dec. 1985.

[154] Y. Hou, C.-C. Liu, K. Sun, P. Zhang, S. Liu, and D. Mizumura, "Computation of milestones for decision support during system restoration," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1399–1409, Aug. 2011.

[155] Y. Hou, C.-C. Liu, P. Zhang, and K. Sun, "Constructing power system restoration strategies," in *Proc. Int. Conf. Electrical and Electronics Eng.*, Bursa, Turkey, Nov. 2009, pp. 1–6.

[156] S. Liu, R. Podmore, and Y. Hou, "System restoration navigator: A decision

support tool for system restoration," in *Proc. IEEE Power and Energy Soc. General Meeting*, San Diego, CA, USA, Jul. 2012, pp. 1–5.

[157] National Institute of Standards and Technology (NIST), "Cybersecurity for smart grid systems," Jan. 24, 2014. [Online]. Available: https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems

[158] R. J. Campbell. (Jun. 10, 2015) Cybersecurity issues for the bulk power system. Congressional Research Service (CRS) Report. [Online]. Available: https://fas.org/sgp/crs/misc/R43989.pdf

[159] J. Bertsch, C. Carnal, D. Karlson, J. McDaniel, and K. Vu, "Wide-area protection and power system utilization," *Proc. IEEE*, vol. 93, no. 5, pp. 997–1003, May 2005.

Appendix A

Reuse Permission

The dissertation has obtained the reuse permissions from The Institute of Electrical and Electronics Engineers, Inc. Copyright © 2018 IEEE.

© 2018 IEEE. Reprinted, with permission, from Zhiyuan Yang, Chee-Wooi Ten, and Andrew Ginter, Extended enumeration on hypothesized substations outages incorporating overload implication, IEEE Transactions on Smart Grid, November 2018.

© 2018 IEEE. Reprinted, with permission, from Chee-Wooi Ten, Koji Yamashita, Zhiyuan Yang, Athanasios V. Vasilakos, and Andrew Ginter, Impact assessment of hypothesized cyberattacks on interconnected bulk power systems, IEEE Transactions on Smart Grid, September 2018.

Title: Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems
Author: Chee-Wooi Ten
Publication: Smart Grid, IEEE Transactions on
Publisher: IEEE
Date: Sept. 2018

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already **a RightsLink user** or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Figure A.1: Reuse permission of the paper [1] obtained from IEEE copyright center

Michigan Tech

Zhiyuan Yang <yzhiyuan@mtu.edu>

Request for Permission of Reuse of Journal Paper "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems"

Chee-Wooi Ten <ten@mtu.edu> Wed, Sep 12, 2018 at 11:26 AM
To: Howard Yang <yzhiyuan@mtu.edu>

Hi Howard - I approve of reuse of the paper "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems."

Chee-Wooi

--
Chee-Wooi Ten, Associate Professor
Department of Electrical and Computer Engineering
Michigan Technological University, Houghton, MI
Email: ten@mtu.edu; O: (906)-487-0397

On Wed, Sep 12, 2018 at 10:16 AM Zhiyuan Yang <yzhiyuan@mtu.edu> wrote:
[Quoted text hidden]

Figure A.2: Reuse approval of the paper [1] obtained from the main author