Optimization-based Frameworks for Systemic Vulnerability Assessment in the Electric Power Systems

Abedi, Amin

UNIVERSITÉ DE GENÉVE

Département d'Informatique

FACULTÉ DES SCIENCES
Professeur Bastien Chopard

Département des Sciences de la Terre

FACULTÉ DES SCIENCES
Professeure Costanza Bonadonna

Optimization-based Frameworks for Systemic Vulnerability Assessment in the Electric Power Systems

THÈSE

présentée à la Faculté des sciences de l'Université de Genève
pour obtenir le grade de Docteur ès sciences, mention Sciences de l'Environnement

Par

Amin Abedi

de

Tehran (IRAN)

Thèse N° 5557

GENÈVE

Centre d'Impression de l'Université de Genève

2021

UNIVERSITÉ DE GENÈVE

FACULTÉ DES SCIENCES

DOCTORAT ÈS SCIENCES, MENTION SCIENCES DE L'ENVIRONNEMENT

Thèse de Monsieur Amin ABEDI

intitulée :

«Optimization-based Frameworks for Systemic Vulnerability Assessment in the Electric Power Systems»

La Faculté des sciences, sur le préavis de Monsieur B. CHOPARD, professeur ordinaire et directeur de thèse (Département d'informatique), Madame C. BONADONNA, professeure associée et codirectrice de thèse (Département des sciences de la Terre), Monsieur F. ROMERIO-GIUDICI, docteur (Institute for Environmental Sciences (ISE), University of Geneva), Monsieur G. TOGNOLA, docteur (Azienda Elettrica Ticinese, El Stradun 74 CH - 6513 Monte Carasso), Monsieur L. GAUDARD, docteur (Precourt Energy Efficiency Center, Stanford University, CA 94305 USA), autorise l'impression de la présente thèse, sans exprimer d'opinion sur les propositions qui y sont énoncées.

Genève, le 1 avril 2021

Thèse - 5557 -

Le Doyen

N.B. - La thèse doit porter la déclaration précédente et remplir les conditions énumérées dans les "Informations relatives aux thèses de doctorat à l'Université de Genève".

Summary

The purpose of this thesis is to identify the vulnerabilities of the power system to ensure its robustness and resilience. Like any other critical infrastructure (CI), power systems are subject to disruptions, either unintentional or deliberate, that may have a significant impact on their performance. Hence, to protect and mitigate such vulnerabilities when CIs suffered from an event, first, one has to explore advanced tools for modeling the electric power grid and its components with respect to its vulnerability to disruptions. Then, trying to guarantee the correct flow of electricity from generation facilities to consumers using appropriate countermeasures.

"Vulnerability analysis" in power systems is important for the first step, to determine how vulnerable a system is, and it is used to detect and rank the most critical elements of a power system under a variety of low-probability-high-consequence events such as multiple-components outages. This thesis aims to address two main issues, i.e. (i) the systemic vulnerabilities of the power system under multiple contingencies and different operational uncertainties; (ii) the critical components which must be protected or fortified when the protective resources are limited. These goals are achieved in three parts:

Part one introduces different definitions of the vulnerability concept and compares the state-of-the-art methods in this field. Then, it highlights the advantages and disadvantages of the standard methods in the vulnerability analysis. In this part, we conclude that each method possesses its own limitations and a perfect method does not exist for all circumstances. Then, we provide a guide to choose the best and the most relevant method for different power system hazards and different levels of acceptable accuracy, computational burden, and required input data.

Part two finds out the acceptable level of assumptions and available data to answer the reliability, vulnerability, and resilience questions. Afterward, the cascading failure is addressed, and a framework for the integration of security methods capable of viewing the problem from

different perspectives, e.g. integrating reliability and vulnerability analyses, is also developed. Although traditionally reliability indices have been adopted as reference metrics, we show that they miss some of the key features of the security concept, especially when we have to deal with low-probability-high-consequence events. Hence, we conclude that the vulnerability analysis can complement the reliability analysis for these events. Moreover, the analysis of five different IEEE-RTS topologies shows that a system considered from the vulnerability viewpoint could behave differently compared to a system considered from the reliability viewpoint. Furthermore, we conclude that the assumptions in the power flow equations can significantly affect the final results and may lead to inaccurate predictions.

Part three introduces and develops a hierarchical leader-follower (bilevel) optimization problem where the upper level (leader) tries to maximize the damage, and the lower level (follower) tries to minimize the probable consequences. Thanks to this rational strategy, the critical components whose failures lead to the largest system loss can be determined. Afterward, our proposed model is extended to be used as a multi-period model, and as a model that immunizes the system analysis against the worst uncertainty. The proposed model is applied to the IEEE test systems and a real-life system i.e. modified Iran's transmission network. The results show that our model is much more efficient than the previously reported one, where the approximated power flow equations are used in the lower level. Moreover, our model shows that Iran's expanded network where only some lines are built is more robust in comparison with the existing network. At the end of this part, in order to guarantee the operational security of power systems with uncertainties, an adaptive robust trilevel optimization model for immunizing the system against the worst uncertainty has been carried out. The final one-level model has been applied to the IEEE 24-bus network and to modified Iran's transmission network. Our simulation results show that the power system vulnerability assessment without considering uncertainties leads to optimistic results. We also observe two properties of our model and prove a lemma that improves the computational performance of our final mixed-integer linear program (MILP) model.

In summary, the focus of the present thesis is on modeling, simulation, and optimization of the power systems with respect to their vulnerability to disruptions and hazards. The outcomes of our research can provide valuable inputs and tools of analysis to public and private decision-makers and system operators.

Keywords: Vulnerability assessment, Electric power system, Multi-level optimization problem, Optimal power flow.

Résumé en Français

Le but de cette thèse est d'identifier les vulnérabilités du système électrique afin d'assurer sa robustesse et résilience. Comme toute autre infrastructure critique (IC), les systèmes électriques sont sujets à des perturbations, involontaires ou délibérées, qui peuvent avoir un impact significatif sur leurs performances. Par conséquent, pour mitiger ces vulnérabilités lorsque les IC sont affectées par un événement, il est d'abord nécessaire d'explorer des outils avancés de modélisation du réseau électrique et de ses composants relativement à sa vulnérabilité. Ensuite, il faut essayer de garantir un flux adéquat d'électricité depuis les installations de production jusqu'aux consommateurs en utilisant des contre-mesures appropriées.

"L'analyse de vulnérabilité" est importante dans la première étape, afin de déterminer le degré de vulnérabilité du système électrique. Elle est utilisée pour détecter et classer les éléments les plus critiques d'un tel système, compte tenu d'une variété d'événements ayant une faible probabilité de survenance mais des conséquences très importantes, telles que les pannes de plusieurs composantes. Cette thèse se focalise sur deux questions principales, à savoir (i) les vulnérabilités systémiques du système électrique compte-tenu de contingences multiples et différentes incertitudes opérationnelles; (ii) les composants critiques qui doivent être protégés ou renforcées. Ces objectifs sont réalisés en trois parties.

La première partie présente différentes définitions du concept de vulnérabilité et compare les méthodes correspondantes à l'état de l'art utilisées dans ce domaine. Ensuite, il met en évidence les avantages et les inconvénients des méthodes standards appliquées dans l'analyse de vulnérabilité. Dans cette partie, nous concluons que chaque méthode possède ses propres limites et qu'il n'existe pas la méthode parfaite applicable dans toutes les circonstances. Ensuite, nous fournissons l'orientation nécessaire afin de choisir la méthode la plus pertinente et performante, en prenant en considération différentes menaces pouvant affecter le système électrique, différents niveaux de précision souhaitables, la charge de calcul et les inputs requis.

La deuxième partie détermine le niveau acceptable d'hypothèses et les données requises pour répondre aux questions de fiabilité, vulnérabilité et résilience. Ensuite, on aborde le problème de l'échec en cascade, et on développe un cadre permettant d'intégrer des méthodes d'analyse de la sécurité, capables de visualiser le problème sous différentes perspectives, par ex. en intégrant des analyses de fiabilité et de vulnérabilité. Nous montrons que les indices de fiabilité traditionnellement adoptés en tant que métriques de référence, ne permettent pas de saisir des caractéristiques clés du concept de sécurité, en particulier lorsqu'on est confronté à des événements ayant une faible probabilité mais des conséquences importantes. Par conséquent, nous concluons que l'analyse de vulnérabilité peut compléter celle de fiabilité. En outre, l'étude de cinq topologies IEEE-RTS différentes du point de vue de la vulnérabilité et de la fiabilité montre qu'un système appréhendé du point de vue de la vulnérabilité pourrait se comporter différemment par rapport à un système appréhendé du point de vue de la fiabilité. Nous montrons également que les hypothèses dans les équations des flux de puissance peuvent affecter de manière significative les résultats de ce type d'analyses et conduire à des prédictions inexactes.

La troisième partie présente et développe un problème d'optimisation hiérarchique "leader-follower" (à deux niveaux), où le niveau supérieur (leader) essaie de maximiser les dégâts et le niveau inférieur (follower) tente de minimiser les conséquences probables. Grâce à cette stratégie rationnelle, on peut déterminer les composants critiques dont les défaillances entraînent la plus grande perte du système. Par la suite, notre modèle est ultérieurement développé afin de pouvoir être utilisé comme un modèle multi-période, voire un modèle assurant l'analyse du système contre les pires incertitudes. Le modèle proposé est appliqué aux systèmes d'essai IEEE et à un système réel, i.e. au réseau de transmission modifié de l'Iran. Les résultats montrent que notre modèle est plus efficace que le modèle proposé par la littérature, où les équations de flux de puissance approchées sont utilisées au niveau inférieur. De plus, notre modèle montre que le réseau étendu de l'Iran, où seulement quelques lignes sont construites, est plus robuste que le réseau existant. A la fin de cette partie, afin de garantir la sécurité opérationnelle des réseaux électriques affectés par l'incertitude, on a développé un modèle d'optimisation adaptatif robuste à trois niveaux, assurant le système contre les pires incertitudes. Le modèle final à un niveau a été appliqué au réseau IEEE 24-bus et au réseau de transmission modifié de l'Iran. Nos simulations montrent que l'évaluation de la vulnérabilité du réseau électrique qui ne tient pas compte des incertitudes conduit à des résultats optimistes.

Nous observons également deux propriétés de notre modèle et prouvons un lemme qui améliore les performances de calcul de notre “mixed-integer linear program” (MILP) model.

En résumé, cette thèse se focalise sur la modélisation, la simulation et l’optimisation des systèmes électriques en ce qui concerne leur vulnérabilité aux perturbations et aux aléas. Les résultats de notre recherche peuvent fournir des précieuses informations et méthodes d’analyse aux décideurs publics et privés et aux opérateurs du réseau.

Mots clés: évaluation de la vulnérabilité, système électrique, problème d’optimisation multi-niveaux, flux de puissance optimal.

Acknowledgement

I would like first to thank my thesis advisor, Dr. Franco Romerio, leader of the **energy, policy, and economics group** at UNIGE, who proposed the subject of research and let me join his team as a Ph.D. student. His recommendations, faultless guidance, and everlasting patience allowed me to cope with the inherent difficulties related to this thesis work. I would like to acknowledge Dr. Ludovic Gaudard, of the same group, who was also a very important guide for my research work.

I would like to express my sincere gratitude to my supervisors, Prof. Bastien Chopard and Prof. Costanza Bonadonna for the continuous support and tremendous help, especially after the retirement of Dr. Franco Romerio.

I thank Dr. Franco Romerio who introduced and supported me to attend the CERG-c, the best course of my life on the assessment and management of geological and climate-related risk. The time we spent together in the CERG-c is truly memorable such as different field works in Switzerland, France, and Vulcano island in Italy. I would like to express my most sincere gratitude to the CERG-c team, especially, Prof. Costanza Bonadonna, Dr. Corine Frischknecht, and all of its lecturers for their immense knowledge.

I would like to acknowledge the kind participation in this work of the co-authors of my articles. I spent 6 months in two high-qualified teams, focused on energy markets and the vulnerability of critical infrastructures. First, Prof. Ettore Bompard's group in the department of energy, POLITO, Italy. Second, Prof. Jose Maria Yusta's group (REDCRIT lab) in the department of electrical engineering at UNIZAR, Spain. I would like to express my gratitude to all the people who helped me during my visiting especially Prof. Jose Maria Yusta for his excellent hospitality and immense knowledge. I would like to thank Dr. Ludovic Gaudard, Prof. Mohammad Reza Hesamzadeh, Dr. Jesus Beyza, Prof. Jose Antonio Dominguez-Navarro, and Prof. Jose Maria Yusta who shared their knowledge in our articles.

I would like to thank Dr. Giorgio Tognola, head of energy trading at AET who was kind enough to accept to be a member of the jury for my thesis. I am very pleased to have presented my Ph.D. work in front of such a high-qualified jury. I also thank all people at UNIGE that supported me during the almost 5 years of intense work.

Finally, I wish to dedicate this thesis to my parents, my wife and my twins, Noura and Nika who have stood by me and enriched my life immensely during these years. Without your support and love, I would not be sitting here writing these final words.

Remerciements

Je voudrais tout d'abord remercier mon advisor, le Dr Franco Romerio, responsable du **groupe politique et économie de l'énergie** à UNIGE, qui a proposé le sujet de cette thèse et m'a permis de rejoindre son équipe en tant que doctorant. Ses recommandations, son encadrement et sa grande patience m'ont permis de faire face aux difficultés inhérentes à ce travail. Je voudrais aussi remercier le Dr Ludovic Gaudard, du même groupe, qui a également été une guide précieuse pour mes travaux de recherche.

Je tiens à exprimer ma sincère gratitude à mes supervisors, les professeurs Bastien Chopard et Costanza Bonadonna, pour leur important soutien et extraordinaire aide, notamment après le départ à la retraite du Dr Franco Romerio.

Je remercie le Dr Franco Romerio qui m'a introduit au CERG-C et qui a soutenu ma participation au cours sur l'évaluation et la gestion des risques géologiques et climatiques, qui a été le meilleur cours de ma vie. Le temps passé ensemble au CERG-C est inoubliable, en particulier les travaux de terrain en Suisse, en France et sur l'île de Vulcano en Italie. Je tiens à exprimer ma plus sincère gratitude à l'équipe du CERG-C, en particulier au professeure Costanza Bonadonna, au Dr Corine Frischknecht et à tous les conférenciers pour leurs formidables compétences.

Je tiens à remercier les co-auteurs de mes articles et à reconnaître leur contribution à cette recherche. J'ai eu le privilège de passer 6 mois chez deux équipes hautement qualifiées, focalisées sur les marchés de l'énergie et la vulnérabilité des infrastructures critiques. D'une part, chez le groupe du professeur Ettore Bompard au département de l'énergie de l'École polytechnique de Turin (POLITO); d'autre part, chez le groupe du professeur Jose Maria Yusta (REDCRIT lab) au département d'ingénierie électrique de l'Université de Zaragoza. J'exprime ma gratitude à toutes les personnes qui m'ont aidé pendant ces séjours en Italie et en Espagne, notamment le professeur Jose Maria Yusta pour son excellente hospitalité et son immense

savoir. Je voudrais remercier le Dr Ludovic Gaudard, le professeur Mohammad Reza Hesamzadeh, le Dr Jesus Beyza, le professeur Jose Antonio Dominguez-Navarro, le professeur Jose Maria Yusta, qui ont partagé leur compétences et expériences dans l'élaboration des articles publiés dans le cadre de cette thèse.

Je remercie le Dr Giorgio Tognola, responsable du négoce de l'énergie chez l'Azienda Elettrica Ticinese (AET), qui a eu la gentillesse d'accepter de faire partie du jury de ma thèse. Je suis très heureux d'avoir pu présenter mes travaux de recherche devant un jury hautement qualifié. Je remercie également toutes les personnes d'UNIGE qui m'ont soutenu pendant près de 5 ans de travail intense.

Enfin, je souhaite dédier cette thèse à mes parents, à ma femme et à mes jumeaux, Noura et Nika, qui ont été à mes côtés et ont énormément enrichi ma vie pendant toutes ces années. Sans votre soutien et votre amour, je ne serais pas assis ici à écrire ces derniers mots.

Contents

Chapter 1

Overall introduction

1-1 Motivation and background

Nowadays, more than ever, electrical energy has become a key commodity in any growing society. A power system as the main energy infrastructure has the characteristics of large-scale critical infrastructures (CIs) [1], i.e.:

- A network of human-made systems and processes that function cooperatively and synergistically to produce and distribute a continuous flow of essential goods, services, and social needs;
- Is subject to multiple events, namely natural hazards, intentional attacks, and random failures;
- An interdependent system, both physically and through a communication system which is subject to rapid changes;
- Disconnection of even single component could potentially provoke cascading effects that cause more portions of the network to be disconnected and finally a total power loss (the blackout);
- Has no single owner/operator.

Any failure or destruction of CIs, especially power systems, has a considerable impact on safety, security, economy, health, and the well-being of a community [2]. Like any other critical infrastructure, power systems are subject to disruptions, either unintentional or deliberate, that

may have a significant impact on their performance. Recently, a large number of people have been affected by blackout throughout the world, for instance, about 128 million people in Iran, the USA, Canada, and Italy due to different events (2003), 670 million people in India (2012), 70 million people in Turkey (2015) and so on [3-6]. In the USA, the annual impact/cost of weather-related blackouts ranges from $20 to $55 billion and the trend of such events shows that their frequency has increased over the last 30 years [7, 8]. According to a report from the National Academy of Sciences of America, the US power system is extremely vulnerable to intentional attacks which may lead to several weeks or even months of large-area blackouts [9]. In addition, VSE[1] reported the cost of a blackout is 2-4 billion CHF per day in Switzerland [10, 11].

Many questions stem from the occurrence of these extreme incidents and potential low-probability-high-consequence events involving the power systems: What is the inherent vulnerability of a power system and which are its critical components that if they fail cause large consequences? What is the mechanism of the propagation of disruptions in the power system? How will the power system react to unexpected events and how large can be the consequences? Are there particular properties that allow the power system to resist systemic disruptions? How close to the limits are they operating? What are the limits? To what type of disruptions are these systems vulnerable? How does the choice of a specific vulnerability metric affect the result of power grid robustness analysis? What countermeasures can be proposed to reduce vulnerability? In short, how vulnerable are these complex interconnected "systems-of-systems"? The main motivation behind this thesis is to address the type of questions stated above.

According to the reported events, some infrastructures are at risk, in particular the electric power system [1]. Hence, some countries have increased the investments aiming at improving CI protection and resilience. The US government has created the National Infrastructure Simulation and Analysis Center (NISAC) [12]. China has allocated 20 trillion CNY during 2015–2020 to increase resilience [13]. Furthermore, the modeling and simulation of CIs for protection and resilience purposes have received significant attention and interest among the universities, national laboratories, and private companies [14]. On the practical side of the issue, the matter of fact is that these understandable concerns are due to the danger that [15]:

[1] Verband Schweizerischer Elektrizitätsunternehmen(VSE)

- The designed system capacities may not be adequate to support the growing demands when we have greater CI integration and market deregulation;
- The safety margins preventively designed may not be sufficient to cope with the expected and, most of all, unexpected events.

To protect and mitigate such vulnerability when CIs suffered from the events, first it is needed to explore advanced tools for modeling of the system and its components and then, trying to guarantee the correct flow of electricity from generation facilities to consumers under different adverse conditions [15]. "Vulnerability analysis" in power systems is important for the first step so as to determine how vulnerable a power system is in case of any potentially unforeseen catastrophic events [16] and it is used to detect and rank the most critical elements of a power grid under a variety of attack scenarios [17]. The final solutions of this analysis are relevant for the system planner and the system operator in order to devise an effective and budget limited set of protective and corrective measures in the second step. There are several strategies for vulnerability reduction such as (*i*) adding the redundant components e.g. new transmission line, (*ii*) hardening the infrastructure, or improving its active defenses such as appropriate surveillance measures, patrolling localized assets, and undergrounding specific transmission components [18].

In the past, several innovative methods have been developed to determine critical components whose failures lead to the largest power-system loss (i.e. for the first step indicated above) [19]. These developed methods can range from analytical approaches (such as complex network, flow-based, logical, and functional methods) to Monte Carlo simulations (a detailed comparison of these methods and approaches is addressed in Chapters 2 and in [20]). But, none of the methods and tools can tackle all challenges of today's energy systems because of their assumptions and further, new introduced challenges [1] or briefly, there is not one single modeling approach that "captures it all" [15]. Moreover, current reliability policy and associated security standards in the energy sector are limited to assessing a reduced set of failures such as the "N-1" criterion and reliability assessment where the potential low-probability-high-consequence events and a larger number of simultaneous outages are typically neglected [18]. Hence, we still lack efficient tools addressing more realistic models that are also suitable for large-scale systems. To bridge this gap, this thesis focuses on the context of vulnerability analysis in the power system to propose new approaches in order to address the shortcomings of traditional approaches.

1-2 Objectives and scope of the research

The general objective of the thesis is to study and develop advanced modeling, simulation, analysis, and optimization methods for the vulnerability analysis of the power systems in order to proactively and properly, protect, and mitigate such vulnerability when they suffered from low-probability-high-consequence failures such as multiple-components outages. The major objectives of the research are, more precisely:

- To develop more reliable methods for structural and systemic vulnerability analysis of the power system, identifying scenarios that can lead to large consequences more reliable than existing methods; (*addressed in Chapters 3-8 and in* [21-25])
- To develop a framework for the integration of security methods capable of viewing the problem from different perspectives e.g. integrating reliability and vulnerability analyses; (*addressed in Chapter 3 and in* [22])
- To find out the characteristics of a good network topology, and good operations in the overall power system security; (*addressed in Chapters 4,6 and in* [22, 25])
- To develop a method for identifying, screening and ranking critical components (due to their location, function, or the load they carry) in a proactive manner; (*addressed in Chapter 4 and in* [23])
- To analyze the vulnerabilities due to changing operational constraints, such as changing load demands within the network system; (*addressed in Chapter 6 and in* [24])
- To immunize the solutions of vulnerability analysis against all possible realizations of the model uncertainty. (*addressed in Chapter 7*)

To achieve the above-stated objectives, several sub-objectives should be addressed to assure the coherence and originality of the research. These sub-objectives are thus in short:

- Definition of vulnerability and reviewing and comparing the previous methods and find out the relations to other concepts such as risk, reliability, and resilience; (*addressed in Chapters 2-4 and in* [20, 22])
- To find out the acceptable level of assumptions and available data to answer the reliability, vulnerability, and resilience questions; (*addressed in Chapter 4 and in* [23])
- To model realistically the cascading failures and domino effects; (*addressed in Chapter 4 and in* [23])
- Find out different methods to solve the multilevel optimization problem. (*addressed in Chapters 6-8 and in* [24, 25])

1-3 Structure of the thesis

The following chapters include 7 articles submitted to international reviews, 6 of which are already published. Figure 1-1 points out the links between different articles (chapters). This figure shows that my thesis content includes three main parts, i.e. literature review part, chapters that present the single-level and multi-level (optimization-based) vulnerability analyses in parts two and three, respectively. Chapter 2 summarizes about 100 papers in the tables and reviewed totally about 300 articles. It shows the advantages and disadvantages of the standard methods in vulnerability analysis. Preliminary results based on the complex network are presented in Appendix A. Chapter 3 compares and integrates the vulnerability and reliability quantitative measures. This lets us distinguish between similar security concepts i.e. vulnerability and reliability analyses. Before the next step, finding the benefits and limitations of power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems is needed. Chapter 4 thoroughly investigates the effects of modeling assumptions, especially when the model is used for line capacity-based assessments such as reliability, vulnerability, and contingency analyses.

In the third part of the research, a new ACOPF-based mathematical framework is proposed to analyze the vulnerability of the power system in Chapter 5. Furthermore, the effects of reactive power dispatch, losses, and voltage profile on the results of the interdiction model are examined in this chapter. Chapter 6 represents a further step of the model in Chapter 5. It proposes a multi-period vulnerability analysis of power grids under multiple outages. Chapter 7 proposed a new model based on the previous models in Chapters 6 and 7 to consider the uncertain parameters using a robust optimization approach. The conclusions are provided in Chapter 8. The abstracts of Chapters 2-7 are as follows:

Chapter 2: The failure of a power system as a critical infrastructure causes considerable damage to society. Hence, the vulnerabilities of such facilities should be minimized to cope with several sources of disruption. Various methods have been proposed to identify and address the weaknesses of power systems to enhance their robustness and resilience. As the field is evolving quickly, understanding the pros and cons of each approach and the trends could be challenging. This chapter aims to guide the reader toward choosing the most effective method according to the issue investigated. We focus on studies on power grids; however, research on other critical infrastructure could also benefit from this review. We identified three classes of events, namely natural hazards, intentional attacks, and random failures. These events affect the adopted method that can range from analytical approaches—complex network, flow-based,

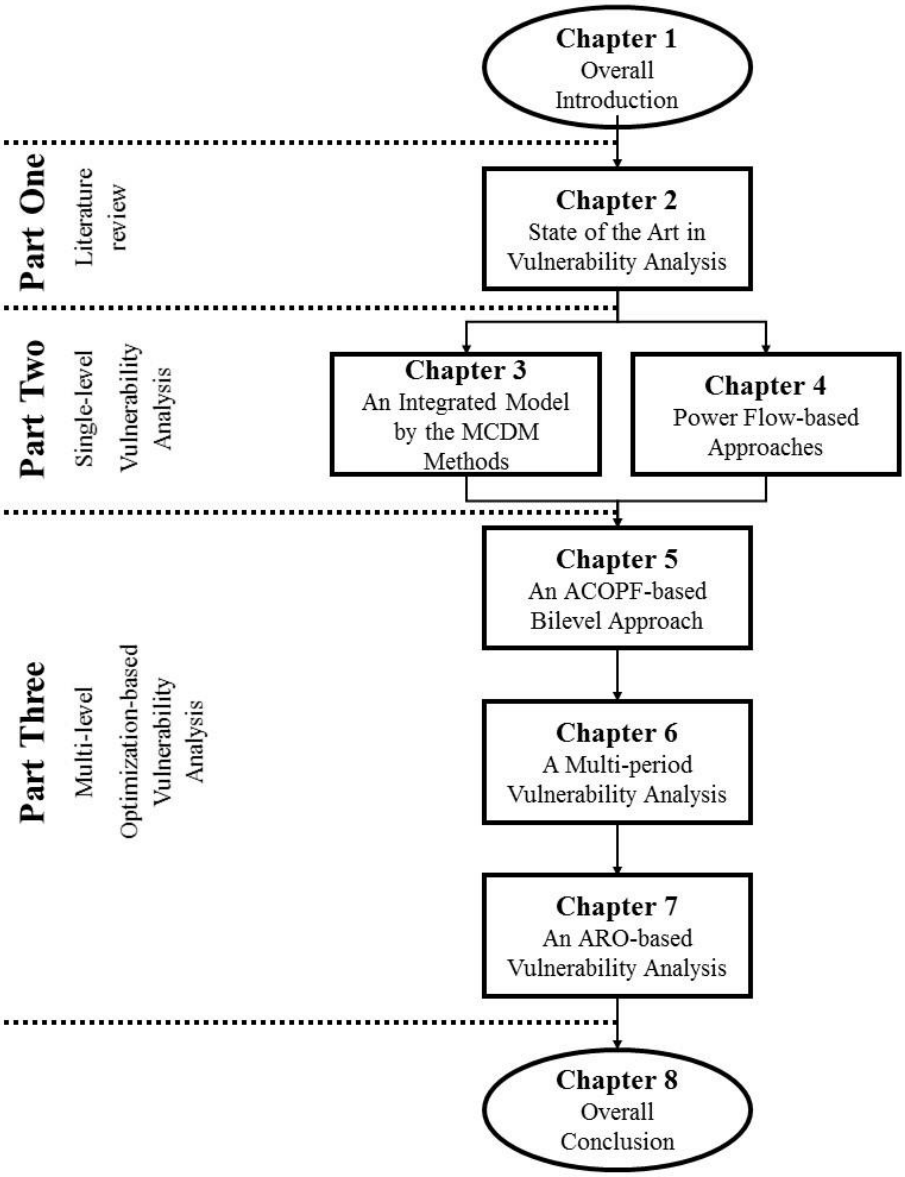

Figure 1-1. Thesis contents

logical, and functional methods—to Monte Carlo simulations. At present, hybrid approaches are emerging with the growing complexities of power grids. Various methods are used in combination to benefit from the strengths of one another. We identified three emerging topics and challenges that require further investigations, namely the N-k problem, trade-off between robustness and optimality, and emerging drivers in power grids.

Chapter 3: Fault analysis of modern power systems cannot be only addressed on classical reliability techniques but also considering the impact of cascading failures. This study proposes an original integrated approach for the risk management of a power system subject to random contingencies by using vulnerability and reliability quantitative measures. Five different

systems based on the IEEE-RTS have been studied from the vulnerability and reliability perspectives. According to the calculation carried out and the multi-criteria decision making (MCDM) method applied to better consider the integration of both concepts, the vulnerability and reliability perspectives are complementary viewpoints that can help to design a more robust critical infrastructure.

Chapter 4: Both steady-state AC and DC power flow models are commonly used for techno-economic studies of power systems. The DC-based approach limits the computational burden by assuming small-angle approximation, ignoring power losses, reactive power flows, and voltage variations. It, therefore, matters to understand if this approach affects system vulnerability, reliability, and contingency assessments. To this aim, we use the time sequential Monte Carlo simulation and an N-k'-1 scenario for reliability and contingency analyses, respectively. Further, we introduce a new index for vulnerability assessment. The IEEE reliability test system (RTS) and the modified RTS are modeled. The results show that the DC model underestimates the reliability indices by about 20% and more than 90% in a stressed network. We also show a small error of 5%, owing to the assumptions of the DC model, which can lead to inaccurate simulations concerning the cascading failures. Finally, the sources of the inaccuracy in the DC-based model are investigated. The results prove that AC power flow model should be privileged for the line capacity-based assessments.

Chapter 5: This chapter examines the effects of reactive power dispatch, losses, and voltage profile on the results of the interdiction model to analyze the vulnerability of the power system. First, an attacker-defender Stackelberg game is introduced. The introduced game is modeled as a bilevel optimization problem where the attacker is modeled in the upper level and the defender is modeled in the lower level. The AC optimal power flow (ACOPF) is proposed as the defender's tool in the lower-level problem to mitigate the attack consequences. Our proposed ACOPF-based mathematical framework is inherently a mixed-integer bilevel nonlinear program (MIBNLP) that is NP-hard and computationally challenging. This work linearizes and then transforms it into a one-level mixed integer linear program (MILP) using the duality theory and some proposed linearization techniques. The proposed MILP model can be solved to the global optimum using state-of-the-art solvers such as Cplex. Numerical results on two IEEE systems and Iran's 400-kV transmission network demonstrate the performance of the proposed MILP for vulnerability assessment. We have also compared our MILP model with the DCOPF-based approach proposed in the relevant literature. The comparative results show that the reported damage measured in terms of load shedding for the DCOPF-based approach is always

lower than or equal to that for the ACOPF-based approach and these models report a different set of critical lines, especially in more stressed and larger power systems. Also, the effectiveness and feasibility of the proposed MILP model for power-system vulnerability analysis are discussed and highlighted.

Chapter 6: This chapter describes a methodology for the *N-k* contingency analysis of bulk power systems. The method encompasses the evaluation of contingencies' effects on the power system over a range of system demand levels. The proposed model is inherently a multi-period bilevel optimization problem. Unlike the conventional bilevel optimization problems for the *N-k* contingency analysis, the proposed model considers the effects of reactive power dispatch, losses, and voltage profile. In doing so, the problem is formulated as a multi-period AC-based bilevel mixed-integer nonlinear programming (MINLP) problem. To guarantee the global optimality of the solution, this work linearizes and then transforms it into a one-level mixed-integer linear programming (MILP) problem using different linearization techniques and the duality theory. The simulation results on the annual load profile of the IEEE Reliability Test System (RTS) verify the effectiveness of the proposed model.

Chapter 7: With the growing level of uncertainties in today's power systems, the vulnerability assessment of a power system with uncertain parameters becomes a must. This paper proposes a two-stage adaptive robust optimization model for the vulnerability assessment of power systems. The main goal is to immunize the solutions against all possible realizations of the modeled uncertainty. In doing so, the uncertainties are defined by some pre-determined intervals defined around the expected values of uncertain parameters. In our model, there are a set of first-stage decisions made before the uncertainty is revealed (attacker decision) and a set of second-stage decisions made after the realization of uncertainties (defender decision). This setup is formulated as a mixed-integer trilevel nonlinear program that is non-convex and NP-hard. Then, this paper transforms the proposed trilevel program into a one-level mixed-integer linear program (MILP) using the duality theory and some proposed linearization techniques. We also prove a lemma which makes our final MILP model much easier to solve. The proposed MILP model can be solved to the global optimum using state-of-the-art solvers. Numerical results on the IEEE test system and modified Iran's transmission network demonstrate the performance of our proposed MILP model for vulnerability assessment under uncertainty.

Appendix A: It is important to increase the security and robustness of power grids under a variety of events. In this case, "Vulnerability analysis" is usually used to identify the most vulnerable elements of a power grid under different hazards. There are different kinds of

methodology to identify vulnerability such as complex network, logical, functional methods and Monte Carlo simulation. In this work, complex network, Swiss power grid and seismic hazard are used as an approach, a test system and a scenario, respectively. First, Swiss power grid is modelled using Gephi software and five different metrics of complex network are applied on the model. Then, TOPSIS as a multi-criteria decision method is used to combine the results of previous step. Finally, to find out the most exposed nodes in the case of earthquake, Swiss seismic hazard data is used and combined with TOPSIS outputs. In this work, the cost of blackout in different Swiss cantons during a blackout is also calculated using VSE report. In addition, different strategies such as power management, monitoring, power system improvement and hardening measures are presented.

1-4 Research outputs and publications

The focus of the present thesis is on the modeling, simulation, and optimization of power transmission networks as critical infrastructure with respect to their vulnerability to cascading failures and high-impact, low-probability events. The following list of publications form the basis of the present doctoral thesis, which will be addressed in the following chapters:

Peer-reviewed Journal Publications

1- Abedi, A., L. Gaudard, and F. Romerio-Giudici, *Review of major approaches to analyze vulnerability in power system.* Reliability Engineering and System Safety, 2019. **183**: p. 153-172.

2- Abedi, A., Beyza, J., Romerio, F., Dominguez-Navarro, J. A., & Yusta, J. M., *MCDM approach for the integrated assessment of vulnerability and reliability of power systems.* IET Generation, Transmission & Distribution, 2019. **13**(20): p. 4741-4746.

3- Abedi, A., L. Gaudard, and F. Romerio, *Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems: The benefits and limitations.* Reliability Engineering & System Safety, 2020. **201**: p. 106961.

4- Abedi, A., M.R. Hesamzadeh, and F. Romerio, *An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system.* International Journal of Electrical Power & Energy Systems, 2021. **125**: p. 106455.

5- Abedi, A. and F. Romerio, *Multi-period vulnerability analysis of power grids under multiple outages: An AC-based bilevel optimization approach.* International Journal of Critical Infrastructure Protection, 2020: p. 100365.

6- Abedi, A., M.R. Hesamzadeh, and F. Romerio, *Adaptive Robust Vulnerability Assessment of A Power System: A Trilevel OPF-based Optimization Approach [Submitted]*

Peer-reviewed Conference Publication and Presentation

1- Abedi, A. and F. Romerio-Giudici. *Systemic Vulnerability of Swiss Power Grid to Natural Events*. in *MATEC Web Conf. 7th International Conference on Power Science and Engineering (ICPSE 2018)*. 2019. *(selected as an excellent oral presentation winner, Ref: http://www.icpse.org/2018.html)*

2- Abedi, A. and F. Romerio. *An AC-based bilevel optimization approach to assess vulnerability of a power system under multiple contingencies.* in *5th International Conference on System Reliability and Safety (ICSRS 2019), 2019. (selected as an excellent oral presentation winner, Ref: http://www.icsrs.org/icsrs19.html)*

Part One

Literature review: Different concepts and methodologies

This part has been published in:

Abedi, A., L. Gaudard, and F. Romerio-Giudici, *Review of major approaches to analyze vulnerability in power system.* Reliability Engineering and System Safety, 2019. **183**: p. 153-172.

Chapter 2

Review of major approaches to analyze vulnerability in power system

2-1 Introduction

An electric system represents a "critical infrastructure" (CI) [15]. Any failure or destruction affects the safety, security, economy, health, and well-being of a community [2]. According to a recent report [26], increasing energy consumption exceeds the slow deployment of energy infrastructure in many countries. An ill-designed electricity reform can even worsen the problem [27]. Deregulation, the opening of the market to competition, and decarbonization may represent a challenge for an electric system [28]. The operators must deal with capacity and design limitations [29, 30] to avoid perturbation.

The risk of blackouts must be handled, and this includes managing the cascading effect. It happens when a triggering event, e.g. the disruption of a transmission line, leads to the overload of the remaining lines and disconnects them from the network [31, 32]. Even in a network with a low probability of occurrence of a blackout, the risk remains high as the impact of an event involves substantial social and economic costs. Power failures have recently affected hundreds of millions of people. In 2003, three independent events in Iran, North America, and Italy hit a total of 128 million people. In 2012 and 2015, 670 million Indian people and 70 million Turkish people respectively were temporarily deprived of power [3-6]. In the USA, the annual cost of

weather-related blackouts ranges from $20–$55 billion. The frequency has even increased over the last 30 years [7, 8]. In Switzerland, 24 hours without electricity costs about $2–4 billion, exceeding the daily GDP [10, 11].

Deploying robust and resilient CI can limit this risk. Operators must detect and rank the most vulnerable elements of a system under a variety of attack scenarios [16]. They can therefore design and control systems to reduce their vulnerability to unpredictable events [33]. Scientists have been developing innovative methods to support decision-makers in this task. However, grasping the pros and cons of such methods is becoming challenging, as the field evolves quickly. Three contributions have already reviewed the field, but they have focused on complex network (CN) concepts [17, 34, 35]. Cuadra et al. [17] considered both pure and extended CN approaches; Bompard et al. [34] focused on their own previous research works, while Pagani and Aiello [35] reviewed literature from a statistic perspective. In 2015, reviews on a specific approach were relevant and insightful. However, the field has considerably expanded since. Besides a required update, an overview of a larger spectrum of methods is becoming critical. New investigations tend to favor hybrid approaches; scholars must understand the pros and cons of each method to merge the complementary ones.

In this chapter, we review the most recent scientific studies on the vulnerability of power grids. It introduces CN but also considers power flow, logical, and functional methods. We compare and categorize them according to several criteria, including the methodology used, assumptions, test cases, failure scenarios, and modeling capability (node and/or line modeling). To further contrast the methods, we provide a correlation analysis of results, and, finally, highlights the emerging challenges.

The rest of this chapter is organized as follows. Section 2-2 provides some basic definitions. Section 2-3 introduces different methods of vulnerability analysis. We compare the methods in Section 2-4 and underline some emerging topics and challenges in this field. Finally, Section 2-5 summarizes the main findings and presents the conclusions.

2-2 Definitions

2-2-1 Critical infrastructure

Infrastructure is large-scale man-made systems that operate interdependently to provide and deliver essential goods and services [15, 36]. They are considered critical if their failure or destruction has a considerable impact on the safety, security, economy, health, and well-being

of a community. Typical examples are energy and communication networks, transportation systems, and water and gas distribution systems [15, 37, 38].

Interdependency among CIs leads to the concept of "systems-of-systems" (SOS) [39]. While interdependencies can improve the CIs' operational efficiency, they also increase their vulnerability [40]. In this perspective, assessing the mutual interdependency of CIs to develop adequate protection is necessary [41]. A range of literature [42-51] introduces four types of interdependencies: physical, cyber, geographic, and logical.

2-2-2 Cascading outage and blackout

"Cascading outage" starts from a specific event that leads to a sequence of disconnections and failures. It turns into a "blackout" when it affects a wide area [17]. According to [52], the probability of a blackout decreases with its size. Doubling the blackout size (power, energy, or number of failures) halves its probability, which approximately follows a −1 to −2 power law [53-55]. However, Prieto et al. [56] suggest that the probability rather obeys a Pareto II distribution, i.e. a shifted power law distribution. Thus, despite a low probability of blackouts, the likelihood of large blackouts seems higher than expected [55, 57]. Even with a low probability, the risk of blackouts is still high. Indeed, the risk assessment also considers the size of the impact, which could be large, as shown in Table 2-1. Some studies also [57-62] provide lessons to be learned from historical events.

Table 2-1. Some recent large-scale blackouts in the world and their consequences

No.	Country	Year	Load loss (GW)	Economic loss	People affected (*Million)	Duration (hours)	Reference
1	Iran	2003	~7	Not available	22	8	[3, 6]
2	USA, Canada	2003	61.8	$ 6.4 billion	50	16–72 (USA), up to 192 (Canada)	[3-5]
3	Italy	2003	24	Over €120 million	~56	Up to ~18	[3, 5]
4	Russia	2005	~3.5	$ 1–2 billion	4	~4	[59, 63]
5	Western Europe	2006	~14	Not available	15	~2	[5]
6	USA and Mexico	2011	4.3	Up to $118 million	Over 5	~11	[63]
7	India	2012	~48	Not available	670	2–8	[6, 64]
8	Turkey	2015	32.2	Not available	70	More than 7	[6]

2-2-3 Power system hazards

CIs are usually subject to many types of hazards and events [15, 65]. Based on the literature review, Figure 2-1 suggests a consistent taxonomy that differentiates random failures, natural hazards, and intentional attacks (pointwise and regional attacks). It represents a finer categorization than the one suggested by Murray and Grubesic [66], who distinguished accidental events from deliberate ones. We further describe and justify the three suggested categories:

Random failures: Random failures affect all similar components of an infrastructure with the same probability distribution. The position of a specific node in the network has no impact on the probability of failure. The literature usually considers the following random disruptions:

- Power system component failures due to component aging, communication system failures, an IT fault, etc. [67],
- Hidden failures that play an important role in cascading events due to an incorrect removal of the power system components by a protection system [68, 69],
- Sabotages, as far as terrorists or enemies do not possess any information about the power grid [70],
- Imbalances between load and generation [17],
- Human errors [71].

The impact of such an event is usually investigated by randomly removing a number of CI components [40]. The system behavior without these elements highlights its vulnerability and robustness. Other studies also consider vulnerability due to the imbalance between load and

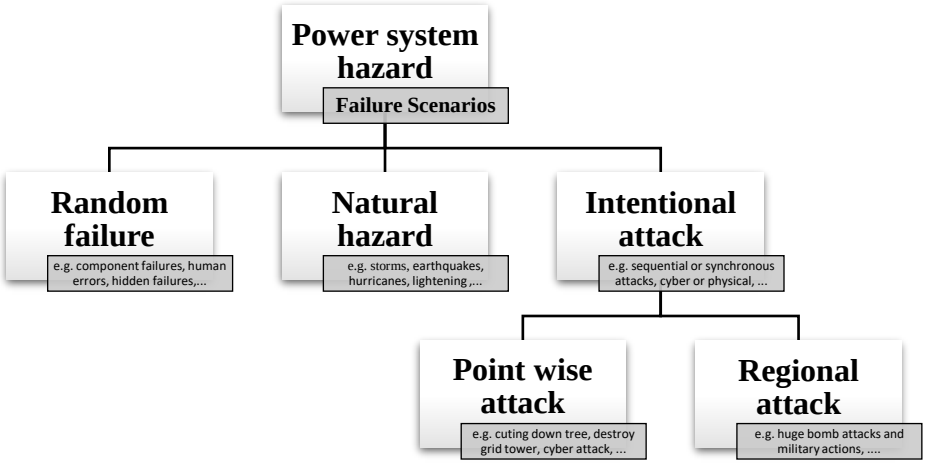

Figure 2-1. Different failure scenarios in power systems.

generation. They alter the loads or power generation in some randomly selected nodes and observe the system reaction [72].

Natural hazards: Natural phenomena, e.g. earthquakes, hurricanes, and lightning, can also alter CIs [8]. Contrary to random failures, the geographic position affects the probability of disruption of a component. Natural events can directly destruct CIs' elements, such as high winds or landslides that damage electric towers. They also indirectly perturb the system. For instance, cold waves and ice can reduce the distance between conductors up to that of generating flash [7]. Heat waves can lower the capacity of an electric line up to the point of overloading it. In Europe, four nuclear power plants had to be shut down in 2003 due to the increase in the temperature of rivers, water from which is used for cooling the reactor cores. Such events affected 4 GW of power supply, leading to approximately $14.5 billion financial losses [73].

Natural hazards represent a significant cause of power system disruptions. Adverse weather conditions caused approximately 33% of the outages in Canada over a 20-year period [74]. Meteorological events caused 43% of 400-kV and 48% of 154-kV line failures in Turkey over a 2-year period [26]. These events usually impose relatively long-duration interruptions, ranging from hours to days, resulting in heavy losses. In the USA, weather-related blackouts cost about $20 to 55 billion per year [7].

Intentional attacks: An effective intentional attack targets the critical elements of the CIs. Therefore, the probability of failure and randomness are not at stake. Power grids are attractive for intentional attacks, as they suffer from the following inherent characteristics [30]:

- Components of power grids are usually distributed in some wide geographical areas,
- Critical elements are spatially concentrated (e.g., substations) and vulnerable to common-cause initiating events,
- Most of the components are not guarded,
- Most of the critical components are located outdoor and thus particularly vulnerable to several threats,
- The impact of a blackout may be significant for a society.

The intentional attacks might be cyber or physical. Physical damage can be as simple as cutting down trees or tripping transmission lines. An individual physically destroyed a local high-voltage transmission line in Arkansas, which resulted in 10,000 customers suffering without electric power on October 6, 2013 [75]. Sudden bursts of electromagnetic radiation (electromagnetic pulse) can also be generated to destabilize the power grid [76]. According to

[64], successful or failed attacks targeted 528 substations and 2,539 transmission towers in the world between 1996 and 2006.

In contrast, cyber attackers inject false data to mislead the system operator. If they know the entire power grid topology and attributes, they can fulfill the physical laws (e.g. power flow laws) without being detected by the system operator [77, 78]. They can also send false topology information to control centers. For instance, they can indicate a tripped line as a connected one and vice versa [78, 79]. Attacks can also rely on partial information. False data can target smart meters in a specific area that require only local information. Then, the disruption can spread to the rest of the network without being detected by the system operator [80, 81].

Intentional attacks can be divided into pointwise (nonproximity-based) and regional (proximity-based) [40, 82, 83]. Pointwise attack scenarios ignore the geographical location of the components. The attacker optimizes the impact by considering the centrality of each node or edge, as defined in Section 2-3. The regional attacks select a set of local nodes, edges, or paths [84] to sabotage, e.g., with bombs and weapons [40].

2-2-4 Vulnerability

Despite vulnerability being a common concept, Wolf et al. [85] observed more than 20 definitions of vulnerability. Various disciplines have been considering this concept, resulting in its diverse definitions and making consensus difficult. Vulnerability can be social, organizational, economic, environmental, territorial, physical, and systemic [86, 87]. As the literature we reviewed is more specific, we can identify some trends. Table 2-2 provides the list of definitions we found during our review process. Most studies focus on physical and systemic vulnerability.

Physical vulnerability represents the degree of loss of an element due to external pressure such as natural hazards [88]. It mainly focuses on the features and assets that can lead the whole system to fail, as in definitions 1 to 4. In contrast, definitions 5 to 7 are related to systemic vulnerability. They consider the degree of redundancy, functionality, and dependency of a system due to the failure of a specific element or interconnected system [89]. Therefore, understanding the conditions or states that can lead the system to fail is crucial. Some papers, especially in the field of natural hazards, integrate both physical element failures (physical vulnerability) and system functionality (systemic vulnerability) [37, 90], as seen in definition 8. Finally, we added a third group of definitions that focus on the measure of the system weakness to hazards: definitions 9–11.

Table 2-2. Different vulnerability definitions

Group	No.	Definition	Reference (Page)
Physical vulnerability	1	"A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard."	[91] (2)
	2	"The weakness level of a system to failures, disasters, or attacks."	[36] (1)
	3	"A susceptibility (sensitivity) to threats and hazards that substantially reduce the ability of a system to maintain its intended function."	[66, 92] (39,23)
	4	"A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard."	[91] (2)
Systemic vulnerability	5	"The manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system."	[93] (1)
	6	"The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards."	[94] (13)
	7	"The inability of a system to withstand strains and the effects of failures."	[95] (2)
Systemic and physical	8	"Any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary."	[38] (10)
Measure	9	"A measure of the system's weakness with respect to a sequence of cascading events that may include line or generator outages, malfunctions or undesirable operations of protection relays, information or communication system failures, and human errors."	[96] (1)
	10	"Robustness or vulnerability (its opposite concept) are often used to measure to what extent a power grid has high or low reliability, respectively."	[17] (2)
	11	"The performance drop of a power grid under a disruptive event."	[97] (2)

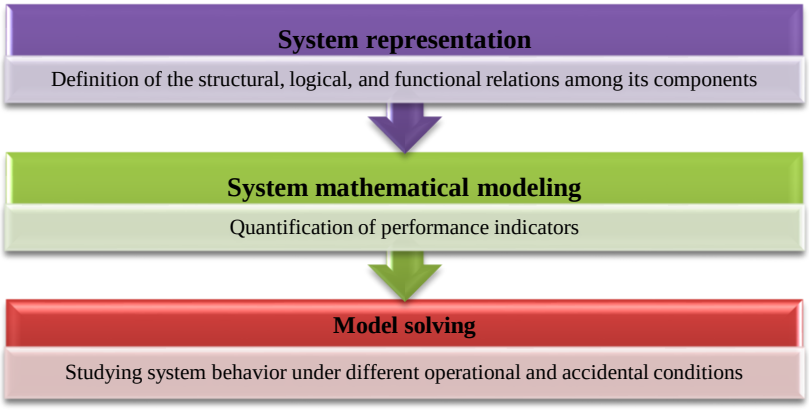

Figure 2-2. Main steps of vulnerability analysis.

2-3 Approaches to vulnerability analyses

Vulnerability analysis usually includes the different steps shown in Figure 2-2. It aims to [15, 41, 66, 98, 99]:

- Determine the critical components that require protection (according to their location, function, or carried load [100]),
- Identify possible undesirable events and their impacts,
- Prioritize the components based on the consequence of loss, e.g., the rate of important blackouts (number per year) and their severity, e.g. power lost and not supplied energy [95],
- Identify potential and inherent vulnerabilities,
- Identify existing countermeasures and their level of effectiveness [101, 102],
- Estimate the degree of vulnerability relative to each component.

Vulnerability analysis can be carried out within two different scenarios: static and dynamic [103, 104]. In the static analysis of robustness, one removes a node from a network without any redistribution of its loads (or flows). In the dynamic analysis, flows are redistributed in the network after a node or link failure. This approach is more complicated and may need to be solved numerically [103-105].

Scientists have been developing various methods to assess the vulnerability of CIs. The approach to be adopted depends on the relevant issue and the type of hazards investigated. This chapter guides the reader in the choice of the right/relevant method. Figure 2-3 provides a first overview.

Vulnerability analysis is performed either by using analytical techniques or by simulation [7, 95]. The main conceptual differences are as follows [95, 106-108]:

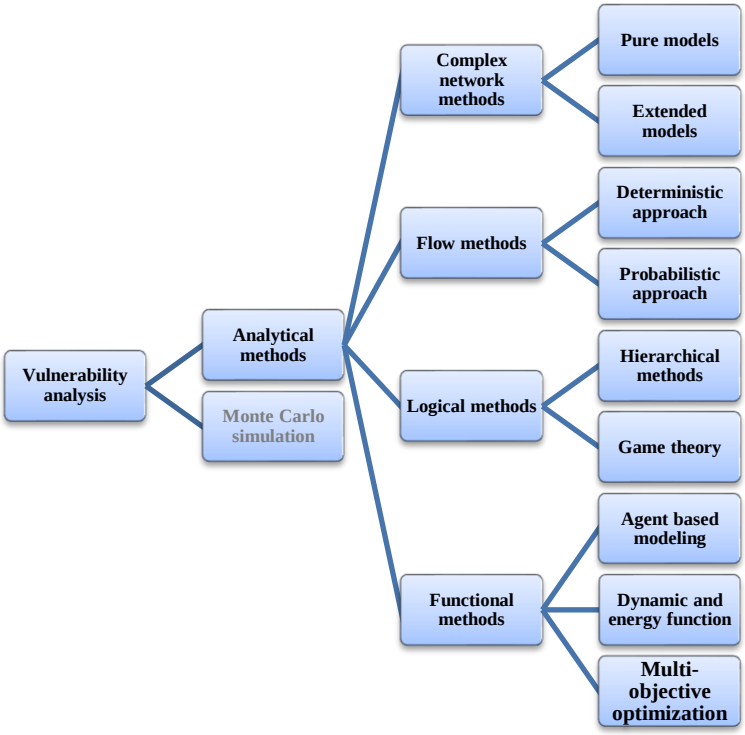

Figure 2-3. Different methods for vulnerability analysis.

- Analytical techniques give an exact solution to a simplified problem, whereas simulations provide an accurate solution to an exact problem,
- Analytical techniques are quicker for the assessment of several similar systems. It performs well at solving a problem for a given set of parameters. In contrast, building a simulation model can consume less time than deriving the equations,
- Analytical techniques evaluate the indices of a simplified model using mathematical solutions. Monte Carlo simulation methods [109] estimate the indices by simulating the actual process and the random behavior of the system,
- With increasing complexity, formulae become more challenging to derive. The last resort is often simulation,
- Analytical approaches use mathematical equations and models, e.g. block diagrams or fault trees, to derive related indices. These approaches require approximations and simplifications when analyzing complex systems.

The forthcoming section will follow the structure of Figure 2-3. We introduce each method one by one. However, we omitted to develop Monte Carlo simulations to avoid making this chapter excessively long. The above-presented differences with analytical approaches already provide a good overview.

The four following sections, each ending with a table, categorize the reviewed papers according to three aspects of information (metric/indicator; case study dimensions; assumptions, and failure scenarios). We collected these data because they affect each other. In particular, despite

no fixed rules existing, the size of a case study tends to determine the suitable assumptions. Studies are presented in a chronological order in the tables to provide a good understanding of the evolution in this field of research. These tables also save time and help a researcher efficiently select the studies that are relevant for a specific research topic.

2-3-1 Topological method (complex network analysis)

Complex network analysis (CNA) has been developed recently [110]. The first systematic studies appeared in the late 1990s to study and analyze the structure, dynamics, and evolution of many complex systems [35, 111]. CNA is performed not only in power grids but also in several other human-made systems, including railway networks, public transportation networks, road and rail transportation, airports, process plants, the Internet, the topology of web pages, airline routes, and electronic circuits [99, 112-120]. It has also been applied to socioeconomic systems, e.g. communication and social networks [121-124]. This method also works for systems stemming from nature, e.g. evolution, metabolic networks, protein interactions, biology, and food webs [17, 125, 126].

CNA considers a set of nodes or vertices, e.g. substations or power plants, interconnected by means of links or edges, e.g. power transmission lines [17]. Some metrics and indices, namely centralities, identify the most critical nodes and edges [31, 119]. According to this concept of centrality, an individual closer to many people will obtain more critical information. This opportunity increases his/her power and influence [127].

CNA is segmented into two broad approaches. Pure models focus on topological definitions, such as degree, closeness, betweenness, clustering coefficient, and efficiency. In the second approach, extended models add electrical elements into the CNA. For instance, they account for the electrical and reliability features of power grids, e.g. impedance, power, and capacitance of the components. This approach triggered the development of extended centralities, such as electrical betweenness and net-ability [17, 128].

Some papers also distinguish weighted/unweighted and directed/undirected models. Weights allow considering the properties of a component, e.g. its cost, reliability, capacities, power, and impedance [103, 129]. Directions are applied to edges to include the actual constraint of flows or goods between nodes. For instance, power always flows from generators to loads [17]. While [130-136] provide extended information about CNA, we also introduce pure and extended CNA, ending with the introduction of four fundamental centralities, namely degree, betweenness, closeness, and efficiency.

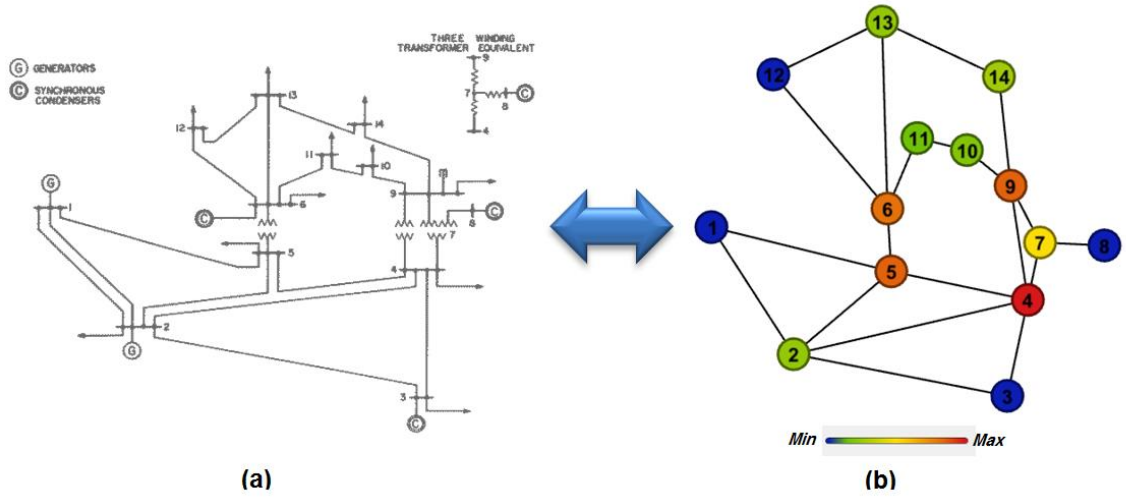

Figure 2-4. (a) IEEE-14 test case, (b) undirected, unweighted, and pure representation of its related complex network using Gephi (an open source software). The color scale and the numbers in the nodes provide the betweenness centrality.

Pure complex network method: In pure CNA, components schematize buses in nodes and transmission lines in edges, as illustrated in Figure 2-4. However, it neglects weight and direction; all the nodes and edges are identical [137]. Two groups of centralities exist in complex network theory. The first one calculates the closeness of nodes/edges to each other, e.g. degree and closeness centralities. The second group evaluates the tie between nodes/edges, e.g. efficiency (shortest path) or flow betweenness centralities [138]. Some metrics also try to merge both groups, e.g. delta centrality (or Δ centrality) [139] and combined degree–betweenness centrality [140]. We introduce the fundamental centralities below. For an in-depth description, the reader can refer to references [130-136, 141] and Table 2-3.

Degree: The degree of a node goes from 0 (if it is isolated), to k (if it is connected to k nodes of the network). The degree probability distribution of all nodes expresses the topological features of a network. For example, some networks have a node degree distribution that follows a power law as in (2-1) [142, 143]:

$$P(k) \sim k^{-\gamma}, \gamma > 1 \tag{2-1}$$

Where $P(k)$ denotes the probability that a randomly selected node has a degree of k, and γ is a constant. With this specific distribution, a few nodes possess a high number of links, i.e. they form hubs. This type of network, namely "scale-free" [17, 144], are particularly vulnerable to intentional attacks but robust to random failures [145]. Other generic networks follow an exponential distribution as in (2-2):

$$P(k) \sim e^{-k/\tau} \tag{2-2}$$

This is the case of the random graph model [146] and the small-world model [147]. Power grids have the features of a small-world network because they form many clusters with a relatively small path length [96].

Closeness: The closeness centrality sums all the shortest paths of a node. It quantifies how fast the injected information spreads in the network [2].

Betweenness: It measures the ratio and the total number of shortest paths in a graph. Nodes with high values of betweenness can control or regulate information flowing within a network [2].

Efficiency: Efficiency assumes that the load of transmission (electricity, information, packets, gas, water, and so on) between two nodes is proportional to the reciprocal of their distance [17, 148]. Table 2-3 presents the mathematical definitions of these centralities, as well as those considered in extended CNA.

Extended complex networks methods: Conventional CNA ignores the physical properties, electrical characteristics, and operational limits of power grids. It limits the scope of the analysis [137, 147, 149]. Binary entities hardly represent the real world [150], as lines have different materials, voltage levels, impedances, and related losses. The graph must be weighted to consider such specificities as well as nodes differences [72]. An improvement required to simulate active and reactive power flows, which are governed by Kirchhoff's law and the topology of the network. In addition, directed edges allow simulating the power flow direction, voltage magnitudes, and angles [17]. Scholars have updated the "pure" centralities to take these "extended" characteristics into account. Some studies consider the physical resistance and impedance of lines and cables as the weight on the edges [17, 151]. Others introduce the reliability characteristics of a power transmission system [152]. Weight or P-Q network decomposition [72] features active power flow and the capacity of the generator and the load [2, 137, 153]. Table 2-3 presents prominent mathematical definitions of metrics in the pure and extended methods. This table highlights how extended centralities are derived from pure ones. In addition, the most important components of the studied papers are categorized in Table 2-4.

Table 2-3. Some pure centralities in complex network theory and related extended metrics

pure methods			extended methods			Ref.
No.	**Centrality**	**Formula**	**No.**	**Centrality**	**Formula**	
1	Degree	$\frac{\sum a_{ij}}{N-1}$	1	Reliability-based degree	$\frac{\sum a_{ij} \sum p_{ij}}{(N-1)^2}$	[103, 154]
			2	Power-based degree	$\frac{\sum P_{ij}}{N-1}$	[155]
2	Closeness	$\frac{N-1}{\sum d_{ij}}$	3	Reliability-based Closeness	$\frac{N-1}{\sum rd_{ij}}$	[103]
3	Betweenness	$\frac{1}{(N-1)(N-2)} \sum_{i \neq j \neq k} \frac{n_{jk}(i)}{n_{jk}}$	4	Electrical Betweenness	$\sum_{i \neq j \neq k} \frac{P_{jk}(i)}{P_{jk}}$	[103, 128, 155]
4	Efficiency	$\frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}$	5	Reliability-based Efficiency	$\frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{rd_{ij}}$	[103]
			6	Net ability	$\frac{1}{N_g N_d} \sum_{g} \sum_{d} C_g^d \frac{1}{Z_e^{gd}}$	[34, 137, 156]

G: the graph descriptive of the structure of the real network with N nodes, $\boldsymbol{i, j, k} \in \boldsymbol{G}$, $\boldsymbol{p_{ij}}$: the overall probability of connection from node i to node j, $\boldsymbol{a_{ij}}$: is 1 if node i is connected to node j, 0 otherwise, $\boldsymbol{rd_{ij}}$: the most reliable path connecting node i to node j, $\boldsymbol{d_{ij}}$: the shortest path from node i to node j, $\boldsymbol{n_{jk}(i)}$: the number of shortest paths that contain i; $\boldsymbol{n_{jk}}$: the number of shortest paths from node k to node j, $\boldsymbol{P_{ij}}$: power flowing in the line connected in between nodes i and j; $\boldsymbol{P_{jk}}$: the maximum power flowing in the shortest electrical path between buses j and k, $\boldsymbol{P_{jk}(i)}$: the maximum of inflow and outflow at bus i within the shortest electrical path between buses j and k, $\boldsymbol{N_g}$ and $\boldsymbol{N_d}$: the numbers of generation and load buses, respectively, $\boldsymbol{Z_e^{gd}}$: an equivalent impedance from a generation bus g to a load bus d as the impedance between the two buses, $\boldsymbol{C_g^d}$: the transfer capacity of the transmission network from generator *g* to load *d*.

Table 2-4. Literature on complex network analysis

Year	Metrics / indicators	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2005	Global efficiency	U	P	PA	YN	Y	98, 146, 127	175, 223, 171	Spanish PG, French PG, Italian PG	[157]
2006	Clustering coefficient, degree distribution, and average path length	U	P	R,PA	Y	Y	4,789, 4,941	5,571, 6,594	Nordic PG, Western U.S. PG	[158]
2007	Weighted line betweenness	W	E	R,PA	N	Y	39, 3,315	46, 3,142	I39, Huazhong-Chuanyu PG	[159]
2007	Clustering coefficient	U	P	R,PA	Y	N	> 3,000 nodes	up to 4,300	UCTE	[104]
2008	Electrical betweenness	B	B	NS	Y	N	300	411	I300	[145]
2008	Topological and reliability efficiency	B	B	R,PA	Y	Y	14	20	I14	[160]
2009	Entropic degree and net-ability	B	B	NS	Y	Y	34, 521	54, 679	I34, Italian PG	[137]
2009	Degree , closeness, betweenness, information, and reliability centralities	B	B	NS	Y	N	14	20	I14	[154]
2009	Efficiency and net-ability	B	B	NS	N	Y	30, 57	41, 78	I30, I57	[156]
2009	Clustering coefficient, information and edge betweenness centrality	B	P	NS	Y	Y	-	6-291	Evolution of French 400-kV PG (1960–2000)	[161]
2009	Complex network analysis and object-oriented modeling	B	B	R,PA	Y	Y	161	219	The Swiss high-voltage PG	[162]
2009	Average and damaged efficiency	B	B	R,PA	Y	Y	14, 300	20, 411	I14, I300	[163]
2010	Developed betweenness index	W	E	NS	Y	N	14	19	I4	[72]
2010	Topological, flow [127], and random betweenness centralities	W	E	NS	Y	N	14	20	I14	[164]
2010	Electric and topological betweenness	B	B	PA	Y	Y	300	409	I300	[165]

2010	Parallel betweenness centrality	W	E	NS	N	Y	14,090, 46,010, 92,370, 172,930	17,346, 57,323, 116,980, 220,648	14,000-bus, 46,000-bus, 90,000-bus, 170,000-bus	[166]
2010	Electrical and topological betweenness centralities	B	B	NS	Y	Y	2935, 300	6567, 409	NYISO-2935 system, I300	[167]
2010	Clustering coefficient, efficiency, and the max indicator of power supply	B	B	R,PA	Y	N	320	441	regional PG in China	[168]
2010	Characteristic path length, connectivity loss, blackout sizes	B	B	R,PA	Y	N	300, 336–1473	409[165], -	I300, 40 areas within the Eastern U.S. PG	[169]
2010	Net-ability, paths redundancy, and survivability	B	B	R,PA	YN	Y	30, 118, 300, 521	41[156], 179 [170], 409[165], 679	I30,, I118, I300, Italian PG	[171]
2011	Electrical closeness and betweenness centralities	W	E	NS	Y	N	5	7	I5	[128]
2011	Electrical betweenness, loss of load index	W	E	R,PA	Y	N	118 [170], 138	179 [170], -	I118, Central China PG	[172]
2011	State transition graph [173] and characteristic length	W	E	NH,PA	Y	Y	118	More than 180	118-bus PG China	[90]
2011	Extended betweenness and net-ability	B	B	PA	Y	Y	118, 300, 521	179, 409, 641	I118, I300, Italian PG	[174]
2012	Structural vulnerability, contingency vulnerability and operational vulnerability indices	W	E	NS	N	Y	93	124	93-bus with DG	[153]
2012	Degree, reliability degree, electrical degree, electrical reliability degree	B	B	NS	Y	Y	24	38	I96	[152]
2012	Degree and betweenness indices	W	P	R,PA	Y	N	118, 4,941	179, 6,594	I118, U.S. PG	[170]
2012	Power flow and random flow betweenness centralities	W	E	R	Y	N	14	20	I14	[175]
2012	Topological and extended betweenness centralities	B	B	R,PA	N	Y	521	641	Italian PG	[176]
2013	Modified pair dependency, closeness and betweenness	B	B	R,PA	Y	N	13, 68, 140, 145	12, 86, 233, 453	4-, 16-,48-, 50-Generators	[2]
2013	Purely topological model, betweenness-based model and direct current power flow model	B	B	NS	Y	Y	57[156], 118 [170], 300[165]	78[156], 179 [170], 409[165]	I57, I118, I300	[67]
2013	Energy-based centrality	W	E	NS	Y	Y	14	20	I14	[177]
2013	Network efficiency and betweenness	U	P	R,PA	Y	N	295	413	Huazhong PG, China	[178]

2013	Local load-redistribution, the normalized avalanche size	W	E	R	Y	N	572	871	Indian PG	[179]
2013	Clustering coefficient, mean shortest path length, degree distribution	U	P	R,PA	N	Y	105	142	Iranian 400-KV PG	[180]
2014	Combined degree-betweenness index	U	P	R,PA	YN	Y	118 [181]	179 [181]	I118	[140]
2014	Degree, betweenness, information, efficiency and closeness and their new reliability-based ones	B	B	R,PA	Y	N	105	142	400-KV PG (IRAN)	[103]
2014	Blackout size and connectivity loss indices	B	B	PA	Y	Y	57[156], 118 [170],300[165]	78[156], 179 [170],409[165]	I57, I118, I300	[97]
2014	Efficiency, source–demand considered efficiency, connectivity level, clustering coefficient, and power supply	B	B	NH,PA	Y	Y	57[156], 118 [170], 300[165]	78[156], 179 [170], 409[165]	I57, I118, I300	[182]
2014	Clustering coefficient	W	E	R	Y	Y	84	200	Floridian high-voltage PG	[183]
2014	Effective graph resistance	W	E	R,PA	N	Y	118 [170], 30[156]	179 [170], 41[156]	I118, I30	[53]
2014	Largest component size, connectivity level, DC power flow model, largest attack efficiency	B	B	R,PA	Y	Y	300	409	I300	[70]
2014	Power transfer distribution factors, extended betweenness, net-ability, risk graph	W	E	PA	Y	Y	57, 118, 2,383	80, 179, 2,896	I57, I118, Polish PG	[184]
2014	PageRank algorithm	B	B	PA	Y	N	118	179	I118	[185]
2015	Degree and betweenness-based method	B	B	R,PA	Y	Y	10-884	9-1,059	Dutch medium and low voltage networks	[151]
2015	Net-ability, electrical betweenness and entropy degree	B	B	PA	Y	Y	300	409	I300	[34]
2015	local load-redistribution, the normalized avalanche size	W	P	PA	Y	N	4,941	6,594	Western U.S. PG	[186]
2015	Degree centrality, electrical degree centrality, betweenness centrality and electrical betweenness centrality	B	B	NS	Y	Y	9, 16, 33, 65, 107	10, 20, 41, 96, 171	BPTS 9, BPTS 16, BPTS 33, BPTS 65, BPTS 107	[187]

2015	Grid vulnerability index (GVI), Efficiency-based vulnerability index	W	E	NS	Y	N	57	78	I57	[188]
2016	Pseudo-Laplacian, pseudo-adjacency, pseudo-degree matrices, susceptance-based degree, modified susceptance-based degree, power traffic degree, and power loss degree centrality	B	B	R,PA	Y	N	30[156], 57[156], 300[165], 4,941	41[156], 78[156], 409[165], 6,594	I30,I57, I300, WSCC 4941-bus USA	[31]
2016	Ratio of post-event and pre-event total generator nodes and active power	B	B	R,RA	Y	Y	417	551	Harris county, USA	[40]
2017	A model based on co-citation (MBCC)-hypertext induced topic selection (HITS) algorithm (MBCC-HITS algorithm)	W	E	NS	Y	N	14, 118	20, 179	I14, I118	[189]
2017	Line-graph-based model, bus-based model	U	P	R,PA	Y	Y	14, 30, 57, 118, 300, 4,941	20, 41, 78, 179, 409, 6,594	I14, I30, I57, I118, I300,WECC(USA)	[190]
2017	Motif-based analysis	U	P	PA	Y	N	417, 254, 647, 461, 79, 190, 193, 63	537, 357, 880, 664, 80, 224, 252, 82	Germany, Italy, France, Spain, TenneT, RTE, Amprion, 50 Hertz	[191]
2017	Three node-based measures and three network-based measures	U	P	R,PA	Y	N	2,083	2,571	South Korean PG 3.3–765 KV	[181]
2017	Efficiency, source–demand-considered efficiency, largest component size, connectivity level, and clustering coefficient	B	B	RA	Y	Y	295	413	Central China PG	[192]
2017	Power flow index, vulnerability index, electric closeness	W	E	NS	N	Y	30	42	I30	[193]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, YN: Yes (not shown), N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), UCTE: Union for the Coordination of Transmission of Electricity, PG: power grid, IX: IEEE X-bus.

2-3-2 Flow-based methods

Complex network methods originally ignored the physics of the power system operation, an issue that was partially overcome with extended CNA. Nevertheless, power flow-based methods intrinsically consider physical features [15, 194]. They simulate power flows in power system planning and operations [195] with deterministic and probabilistic approaches:

Deterministic flow-based approach: Power or load flow studies calculate the steady-state solutions of the power system. In a deterministic approach, the modeler/operator knows the injected active powers (P_i) at all buses (N) except the slack bus, i.e. the other (N-1) buses, the injected reactive powers (Q_i) at all load buses (PQ buses), and the voltage magnitude (V_n) at all generator buses (PV buses) [67]. P_i and Q_i can be expressed in terms of unknown and known state variables as follows:

$$P_i = f_i(\delta_1, \delta_2, ..., \delta_n, V_1, V_2, ..., V_n) \quad (2\text{-}3)$$

$$Q_i = g_i(\delta_1, \delta_2, ..., \delta_n, V_1, V_2, ..., V_n) \quad (2\text{-}4)$$

Where $i = 1,2,3, \ldots, n$, n being the number of buses in the system. According to (2-3) and (2-4) , the injected active and reactive powers are functions of voltage magnitudes (V_i) and angles (δ_i) of all buses. These alternative current (AC) power flow equations are nonlinear. Therefore, iterative numerical solutions must be used, such as the Gauss–Seidel, Newton–Raphson, or the decoupled power flow methods. These equations and their solutions are detailed in books on electrical power systems [196-198].

Solving AC power flow equations causes a significant computational burden. The direct current (DC) approach limits this issue by linearizing the equations and is required in large-scale simulations or when analyzing many failure scenarios [199]. It considers active powers but ignores reactive powers and transmission losses [200]. Its efficiency approximates the AC power flow, without being iterative and complex [67, 199]. It misrepresents transmission line flows by less than 5%, while being 7 to 10 times faster than the exact solution provided by the AC load flow approach [53]. The estimation is even more accurate in high-voltage low-load power grids [200]. Both power flow approaches are applied to vulnerability analysis. Yan et al. [154] compare a modified DC power flow-based cascading failure simulator using transient stability analysis (TSA). Cavalieri et al. [37] contrast AC power flow-based approach with hierarchical and topological methods. Cascading failures and blackouts were assessed with the Oak Ridge–PSERC–Alaska (OPA) model [55, 201] that uses the DC power flow equation. It

solves power flow models under restriction conditions while minimizing the cost function. Nevertheless, the small number of nodes and controlling parameters limit the scope of this model [68]. The University of Manchester developed an AC power blackout model [202] that can consider the cascading failure of transmission lines, post-contingency dispatching of active and reactive powers, or load shedding to prevent a complete blackout. Finally, the CASCADE model [203] describes qualitatively the nature of cascading failure in power systems. However, it ignores the times between adjacent failures and generation re-dispatching during failure [204, 205].

Some studies apply the maximum flow theorem, a deterministic method [150, 206]. It identifies the maximum power flow that a power system can withstand [194]. It works well with weighted networks such as electrical power systems, communication networks, or computer networks. It maximizes the flows from the source to the sink in a network [150, 206]. The maximum flow theorem observes limits similar to that in the power flow calculation, because power grids usually function within capacity and design limitations [29]. Transmission line capacities, bus voltage levels, and generator output greatly influence the power flows. Therefore, the system's state can become abnormal with small perturbations [207].

Various vulnerability analyses of power grids have applied the maximum flow theory. Dwivedi and Yu [100] proposed a maximum-flow-based complex network version. Fan et al. [207] employed the maximum flow theorem to investigate the robustness of a power grid with a tunable load distribution parameter. Fang et al. [208] recently innovated with a multisource multisink problem. They connected virtual nodes to source and sink nodes. Then, all virtual components were connected to a new virtual one. Table 2-5 will further compare different works based on power flow and maximum flow modeling.

Probabilistic flow-based approach: Uncertainties are ignored in deterministic power flow methods. They require fixed values of load, generation, and transmission line conditions, which are relevant for cases with minimal changes [195, 209, 210]. Probabilistic approaches are preferred when there are large variations of load demand, network configurations, and rates of generator outages or generation, as with wind power. These methods evaluate the system vulnerability according to the uncertainty level [211]. Power system uncertainties can apply both Monte Carlo simulations and analytical methods [210, 212]. Different analytical probabilistic load flow algorithms exist, such as linear approximation, point estimate method, combined cumulants and Gram–Charlier expansions, statistical least square estimation and

Nataf transformation, and Latin hypercube sampling [195, 209, 213]. They all linearize the AC power flow equations but use probabilistic density function instead of assuming fixed inputs [209, 210]. Table 2-5 concludes this section about deterministic and probabilistic flow-based approaches. It summarizes the studies that applied these approaches in vulnerability analysis.

2-3-3 Logical method

Game theory: Von Neumann [214] developed the game theory to analyze strategic behavior [215]. Recently, infrastructure security research applied this method in the context of electricity grids [216], transportation networks [217], and supply chains [218]. It deals with intentional attacks and intelligent threats [219] by simulating the behavior of the players, e.g. infrastructure operators and attackers. They reach the Nash equilibrium, if it exists. It occurs when no players can gain to unilaterally change his/her strategy, while others keep their strategies [220]. Non-cooperative games perfectly model strategic interactions between defenders and attackers in malicious attacks. Indeed, each player maximizes his payoff functions, such as the expected damage and the energy loss, independently of the strategy of the other players [215, 221]. Particularly, the Stackelberg strategy as a leader-follower (sequential) game model is recently deployed for modeling security problems [222, 223]. Table 2-6 will present some applications of game theory.

Hierarchical method: Clustering gathers similar or closely related components together. Dissimilar elements are put in new clusters [224]. The diagram of all clusters is called the hierarchical model of the system [225]. It represents the different levels of the internal related elements in a system. It helps in identifying the critical elements in different potential failure scenarios [224]. Figure 2-5 illustrates hierarchical clustering, where the similarity criterion is the distance between the nodes. Figure 2-5(a) is the tree of clusters for the network illustrated in Figure 2-5(b). This method reduces the computational cost by changing the level of detail of the analysis [226, 227].

Vulnerability analysis considers various hierarchical methods such as the graph representation [33], clustering [224], and logic-based hierarchies [228]. They support both a qualitative and quantitative analysis of CIs [33]. Schaeffer [229] synthesizes a systematic review of this approach.

Table 2-5. Literature on flow-based methods

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2010	Probabilistic, combined cumulants and Gram–Charlier Expansions	W	E	R	Y	Y	~16000	~17000	Western North American PG	[211]
2010	DC power flow method, error and attack tolerance methodology)	B	B	R,PA	Y	Y	118	186	I118	[69]
2010	Deterministic, max-flow theorem	W	E	PA	N	Y	39	-	I39	[230]
2011	Maximum flow algorithm, network efficiency, and flow betweenness	W	E	PA	Y	Y	5, 30[156]	7, 41[156]	I5, I30	[231]
2013	Deterministic, power flow models, ORNL–PSerc–Alaska (OPA) model	B	B	R	Y	Y	300, 300, 300, 418, 400	-	I300, SCALE300, ER300, I418, and SCALE400	[204]
2013	Deterministic, max-flow theorem	W	E	R,PA	N	Y	118	186	I118	[100]
2013	Power flow modeling, eccentricity, radiality, betweenness, centroid, degree centralities	B	B	R,PA	Y	Y	242	310	Swiss PG	[30]
2014	Deterministic, max-flow theorem	W	E	PA	N	Y	14	20	I14	[232]
2014	global efficiency (average efficiency), DC power flow method	B	B	R,PA	Y	N	14, 118	20, 186	I14, I118	[233]
2014	Deterministic, AC power flow, and hierarchical and topological methods	B	B	NH	Y	Y	118	186	I118	[37]

2015	Deterministic, DC power flow	W	E	NS	Y	Y	39, 68	46, 86 [234]	I39, I68	[200]
2015	Deterministic, flow models	B	B	R	Y	Y	24	38	I24	[199]
2013, 2015	Efficiency, connectivity of the network index, load shedding index, severity index, geodesic strength, and power flow modeling	B	B	R,PA	Y	N	5, 14, 24, 30, 57, 118, 300	7[231], 20[175], -, 41[156], 78[156], 179 [170], 409[165]	I5, I14, I24, I30, I57, I118, I300	[235, 236]
2015	AC power flow, bilevel optimization	W	E	PA	Y	Y	118, 2,383	186, 2,896	I118, Polish 2383-bus	[237]
2015	DC power flow method	W	E	PA	N	Y	57, 118, 247	78[156], 179 [170], -	I57, I118, , I247	[238]
2016	Max-flow theorem and electrical efficiency	W	E	R,PA	N	Y	9, 118 [170]	9, 179 [170]	I9, I118	[194]
2016	Deterministic, max-flow theorem	W	E	PA	Y	N	90	128	500-kV China PG	[207]
2016	Deterministic, max-flow theorem	W	E	PA	N	Y	-	-	Danish PG	[208]
2016	Linear DC optimal power flow (OPF), static performance indices (SPI), and dynamic performance indices (DPI)	W	E	NS	Y	N	43	-	Brazilian Birds test system	[239]
2016	Deterministic, power flow	W	E	NH, R,PA	Y	Y	24[240]	38[240]	I24 [240]	[26]
2016	Maximum flow network algorithm	W	P	NH	N	Y	20,000	-	USA	[241]
2017	AC-based power flow	B	B	PA	Y	Y	30, 57, 118	41[156], 78[156], 179 [170]	I30, I57, I118	[242]
2017	Power flow entropy, flow betweenness	W	E	PA	N	Y	39	-	I39 integrated with a 75-MW wind farm	[243]
2017	AC power flow, net-ability, and node electrical centrality	W	E	NS	Y	N	30, 57	41[156], 78[156]	I30, I57	[244]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus.

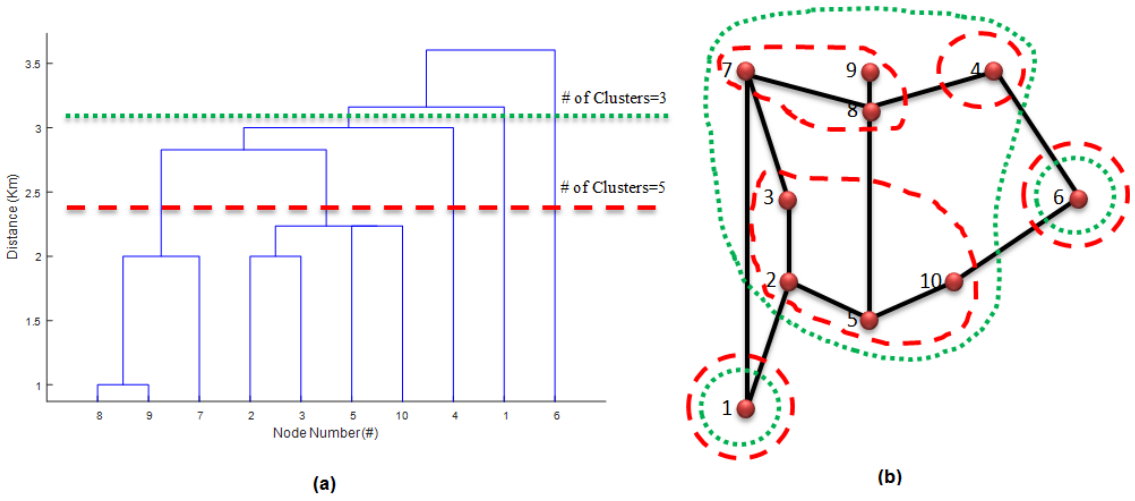

Figure 2-5. Illustrative example of hierarchical clustering: (a) a hierarchical clustering dendrogram (a tree of clusters) and two different levels of abstraction (dotted lines) and (b) the network and its clustered nodes.

Table 2-6. Literature on logical methods

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	#. of nodes	# of links	Name	
2007	Game theory	W	E	R,PA	Y	Y	-	-	Swedish PG	[221]
2009	Game theory, zero-sum game, and the mixed-strategy equilibrium	W	E	PA	Y	Y	24	38	I24	[215]
2011	Fault chain theory	W	E	R,PA,RA	N	Y	14	20	I14	[245]
2013	Hierarchical modeling by recursive unsupervised spectral clustering	W	P	R,PA	N	Y	127	171	380-KV Italian PG	[129]
2015	Hierarchy-based approach, node traffic, node betweenness, and node degree	B	B	NH	Y	N	118	186	I118	[226]
2015	Game theory, a discrete simultaneous game, and the mixed-strategy equilibrium	W	E	PA	N	Y	73	117	IEEE RTS 96	[246]
2016	Hierarchical graph representation and clustering and Monte Carlo simulation	W	E	R	Y	Y	114	112	I123 bus	[33]
2016	Game theory, power flow and topological analysis	B	B	PA	N	Y	30	42	I30	[216]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus.

2-3-4 Functional methods

Agent-based modeling: Agent-based modeling describes complex systems. It simulates the behavior of the actors, referred to as agents, to determine their impact on the whole system. Each individual acts according to predetermined rules modeled with a set of if-then relationships or decision trees. Probabilistic models can simulate probable heterogeneity of agents' responses/reactions [247]. Agent-based modeling supports systematic analysis, both conceptually and computationally. It applies to contamination in a water distribution system [247], modeling a local multicarrier energy network [248], resilience analysis [249], dynamics calculations [250], and simulation of large-scale electric mobility [251].

Several programming environments implement and test agent-based models. For instance, JADE, a Java-based platform, models micro grid, electric vehicle management system, fault detection, protection, and self-healing [252]. The U.S. Pacific Northwest National Laboratory (PNNL) has recently developed VOLTTRON in Python [253, 254]. It considers various programming languages, unlike other models, and can support fault detection, renewable energy integration, smart monitoring and diagnostic systems [255]. Particularly, Sujil et al. [252] introduce different platforms for agent-based modeling.

Dynamic modeling: Great disturbance generates a large magnitude of transient energy. For instance, the kinetic energy of generator rotors will be converted to potential energy in the power system. If the power system cannot absorb and control this energy, it will lose its stability [256]. Different time domain [196] and direct methods based on energy functions [257] examine the stability of a power system. The second method [258] performs well in power system dynamics and security analysis [259-263]. For further understanding, Table 2-7 compares applications of functional methods.

Multi-objective optimization: Multi-objective optimization (MOO) is a mathematical approach to find values of decision variables which correspond to the optimum of more than one objective function [264]. Cho et al. [265] presented the state-of-the-art modeling and techniques such as weighted sum, goal programming, ε-constraints and so on, to solve MOO problems and also, discussed advantages and disadvantages of each modeling and solution technique in detail. Different bi-level (e.g. attacker-defender) and tri-level (e.g. design-attack-defend) frameworks are introduced for vulnerability analysis of different critical infrastructure using MOO [237, 266]. Recently, Faramondi et al. [267] employed MOO in vulnerability analysis of a power system as well as an airline network. They used pairwise connectivity

concept (a degree graph based concept). Also, the defined objectives are simultaneously minimizing the degree of connectivity and minimizing the cost of the attack from attacker perspective using MOO.

Table 2-7. Literature on functional methods

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	# of nodes	# of links	Name	
1994	Transient energy function (TEF) method	W	E	NS	Y	N	50	-	I50	[262]
2005	Particle swarm optimization, energy margin	W	E	R	N	Y	179	203	WSCC, U.S.	[268]
2007	Radial basis function, neural network	W	E	R,PA	Y	Y	300	411	I300	[269]
2007	Nonlinear optimization method, power flow	W	E	PA	N	Y	30, 118	41, 179	I30, I118	[270]
2008	Energy model	W	E	R	N	Y	9	-	3-generator system	[271]
2009	Potential energy model	W	E	NS	N	Y	30	41	I30	[272]
2011	Multi-agent CNM	W	E	R,PA	Y	Y	2,556	2,892	North China PG	[273]
2012	Energy function, degree index, and vulnerable sensitivity index	W	E	NS	N	Y	30	41	I30	[274]
2014	Transient energy function, CNM	W	E	NS	Y	Y	~31	-	Six-generator system	[256]
2016	Dynamic model of AC power grids	W	E	R,PA	N	Y	120 236 118	165 320 179	Great Britain HV line, Scandinavia, I118	[275]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus.

2-4 Discussion

2-4-1 Overview

This chapter reviews the most cited and recent papers on vulnerability analysis of power grids. We have summarized them in four tables according to several criteria, such as methodology, assumptions, test cases, failure scenarios, and the proposed modeling capability (node and/or line modeling). They allow readers to grasp the differences, but this section extends the comparison and discussion.

Figure 2-6 presents the distribution of the reviewed papers in the last decade according to our categorization. Scholars first applied CNA and functional methods to power system vulnerability analysis. While the number of studies applying the functional approach has been remaining stable, CNA application grew and led the field. Flow-based methods, despite appearing later, seem to attract interest in the past five years. Finally, logical methods are marginally applied.

Figure 2-7 provides the distribution of the chosen approaches and the used scenarios. As we already observed in the previous figure, most of the studies applied CN in multiple scenarios.

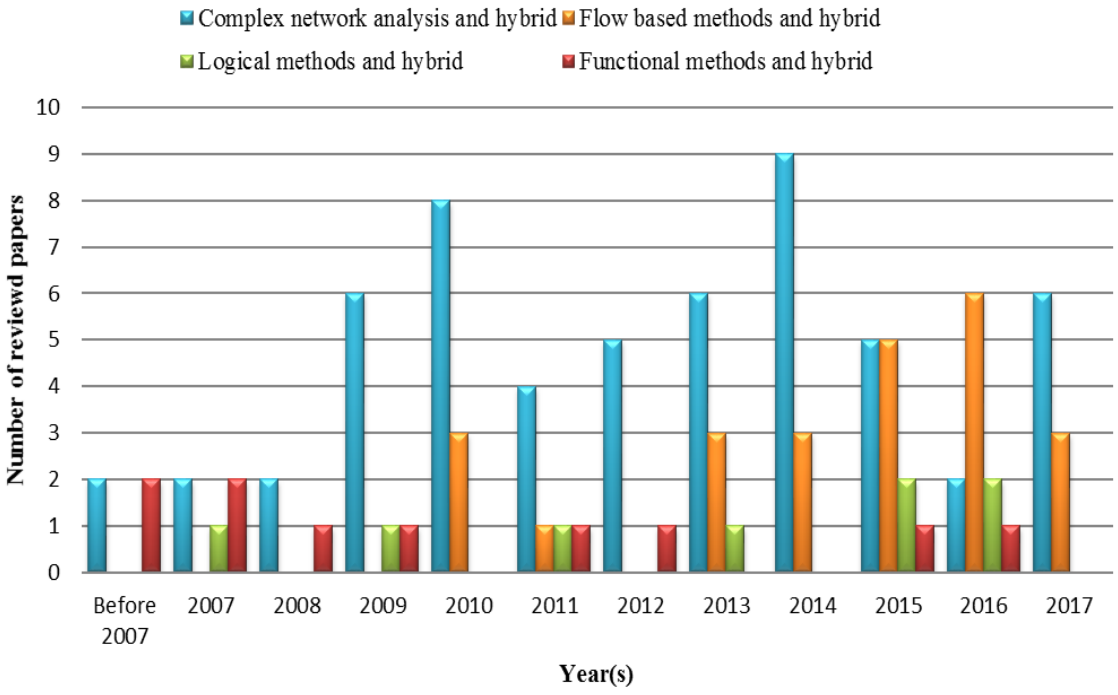

Figure 2-6. Number of reviewed papers according to different categories, from before 2007 to 2017.

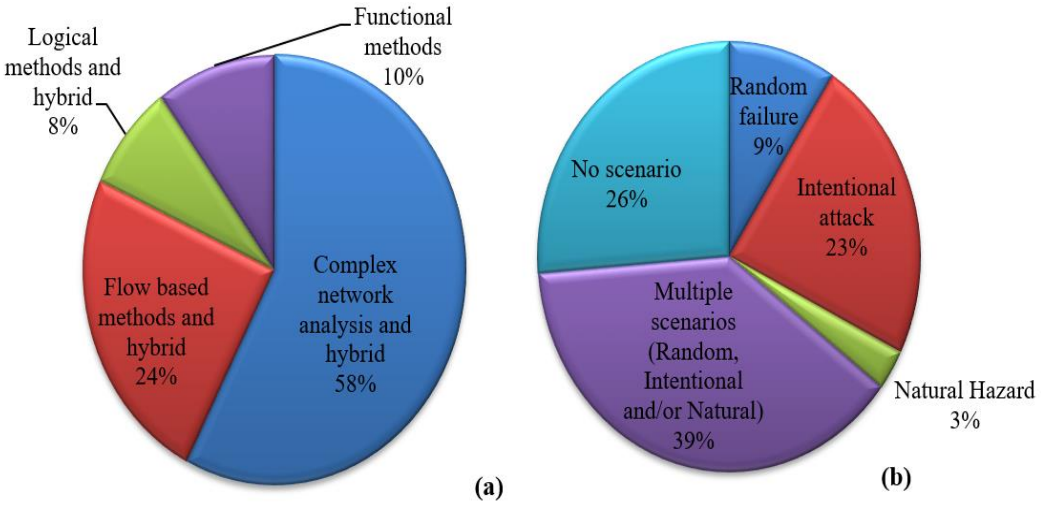

Figure 2-7. Distribution of reviewed papers based on (a) approach and (b) scenarios.

The statistics about the scenarios shows that few papers are devoted to natural hazards. This is surprising given the enormous extent of their impacts, indicating that more studies are required in this area. Finally, we also computed the share of studies that consider generic models (58%), real cases (29%), or both (13%). Generic models provide the opportunity to compare the results and replicate them, possibly explaining the increased interest in this type of models.

2-4-2 Comparison of methods

Table 2-8 maps a chosen method to its respective scenario, although it should be noted that other combinations may also work. Each method possesses its own limitations, implying that the perfect method does not exist. Table 2-9 helps the reader to understand the advantages and disadvantages of each method. We compare the scalability and the computational burden of the analytical methods according to the case study dimensions (number of simulated nodes and edges). The comparison demonstrates that complex network methods better model larger grids compared to other methods owing to the lesser computational burden.

Table 2-8. Methods used for different power system hazards

Power system hazard		Nature	Scenario basis	Used methods in reviewed papers
Random failure		Accidental/random	Random	Complex network analysis [2, 31, 40, 53, 70, 103, 104, 140, 151, 158-160, 162, 163, 168-172, 175, 176, 178-181, 183, 190] Flow-based methods [26, 30, 69, 100, 194, 199, 204, 211, 233, 235, 236] Logical methods [33, 129, 221, 245] Functional Methods [268, 269, 271, 273, 275]
Natural hazard		Accidental	Hazard maps and affected areas	Complex network analysis [90, 182] Flow-based methods [26, 37, 241] Logical method [226]
Intentional attacks	Pointwise attack	Intentional/strategic	Critical component	Complex network analysis [2, 31, 34, 53, 70, 90, 97, 103, 104, 140, 151, 157-160, 162, 163, 165, 168-172, 174, 176, 178, 180, 181, 184-186, 190, 191] Flow-based methods [26, 30, 69, 100, 194, 207, 208, 230-233, 235-238, 242, 243] Logical methods [129, 215, 216, 221, 245, 246] Functional Methods [269, 270, 273, 275]
	Regional attack	Intentional/strategic	Critical area	Complex network analysis [40, 192] Logical method [245]

Table 2-9. Some major advantages and disadvantages of different methods used in vulnerability analysis

Methods			Advantages/capability	Disadvantages/limitations	Ref.
Analytical methods	Topological methods	Pure models	• Very fast and simple for calculation of indicators • Scalable and can model small to very big power systems • Can be applied to real-time application because of high computing efficiency	• Neglect the realistic and basic power flow and network constraints and operation • Excessive simplification can lead to inaccurate results. • Not reliable, cannot be used alone for decision-making	[17, 35, 70, 151, 204, 216]
		Extended models	• As above • Consider the realistic and basic power flow and network constraints and operation	• Consider few constraints of the network	[17, 35, 70, 151, 204, 216]
	Flow methods	Deterministic approach	• DC models are computationally efficient. • AC models consider the realistic and basic power flow and network constraints. • The maximum flow theorem is fast and simple for calculation of indicators.	• DC models may fail to simulate the cascading failure. • DC models ignore some network parameters such as the reactive power balance equations, line losses. They also assume that all voltage magnitudes equal one per unit. • DC models misestimate the importance of components. • AC power flow equations cause significant computational burden and have convergence problem.	[242]
		Probabilistic approach	• Can simulate realistic model with uncertainty	• Lower scalability in comparison with topological methods	[204]
	Logical methods	Hierarchical methods	• A clustering algorithm can reduce the dimension of the network. • Can be applied to qualitative and quantitative analysis • Reduce the complexity of the network.	• Cannot model interdependency between networks • Hardly applicable to large power systems • Not flexible; adding or removing the component may change all representations	[33]
		Game theory-based modeling	• Simulate the actions of intelligent adversaries	• Needs probabilities of different consequences (e.g., attack probability or failure) for various possible combinations of players' actions	[38]
	Functional methods	Agent-based modeling	• Can model interactions between network components • Flexibility to add or remove the components • Can consider different environments, as a sublayer of the model • Can model a large-scale complex network with a large number of dynamic and nonlinear interactions	• Large number of required parameters for modeling real systems • High computational burden	[254, 276]
		Dynamic and energy function	• Can simulate a realistic model with its dynamic behavior	• Hardly applicable to large power systems (time domain methods) • Large number of required parameters for modeling real system (time domain methods).	[196]
		Multi-objective optimization	• Achieve the best action in intentional attacks considering different objective functions	• Computationally inefficient without feasible solution space	[265]

2-4-3 Correlation analysis

Spearman's rank correlation coefficient allows comparing the results of different methodologies. It tests the association between two sets of ranked data. The results are always between 1.0 (a perfect positive correlation) and –1.0 (a perfect negative correlation) [277]. A positive correlation means two variables increase or decrease together. In contrast, a negative correlation means the variables increase/decrease in opposite directions. Herein, the correlation coefficient compares the ranking of critical components using different methods.

Figure 2-8 shows the matrix of Spearman's rank correlation coefficient for some available results from only CN approaches, which are the most applied in the field. We consider five works [154, 164, 175, 189, 278], already listed in Table 4, because they used the same IEEE 14-bus generic case study. Three groups appear. First, global topological/reliability efficiency, topological/reliability closeness, and reliability degree are highly correlated at more than approximately 80%. They have a very low (even negative) correlation with power flow betweenness and the MBCC-HITS algorithm. Finally, reliability betweenness, topological degree, and random flow betweenness have a moderate level of positive correlation with the first group. These results show that not all CN approaches have a good correlation to each other, demonstrating a need for further comparing and even developing new methods and centralities in this field.

Method	Global topological efficiency	Global reliability efficiency	Topological closeness	Reliability closeness	Topological betweenness	Reliability betweenness	Topological degree	Reliability degree	Random flow betweenness	Power flow betweenness	MBCC-HITS algorithm
Global topological efficiency	1.00	0.84	0.93	0.88	0.91	0.55	0.78	0.92	0.65	-1.00	0.38
Global reliability efficiency	0.84	1.00	0.74	0.94	0.84	0.61	0.49	0.82	0.23	-1.00	-0.05
Topological closeness	0.93	0.74	1.00	0.88	0.95	0.54	0.84	0.90	0.69	-0.99	0.44
Reliability closeness	0.88	0.94	0.88	1.00	0.93	0.60	0.62	0.87	0.38	-1.00	0.09
Topological betweenness	0.91	0.84	0.95	0.93	1.00	0.57	0.83	0.91	0.66	-0.95	0.45
Reliability betweenness	0.55	0.61	0.54	0.60	0.57	1.00	0.50	0.64	0.16	-0.94	-0.10
Topological degree	0.78	0.49	0.84	0.62	0.83	0.50	1.00	0.86	0.76	-0.80	0.53
Reliability degree	0.92	0.82	0.90	0.87	0.91	0.64	0.86	1.00	0.60	-0.95	0.25
Random flow betweenness	0.65	0.23	0.69	0.38	0.66	0.16	0.76	0.60	1.00	-1.00	0.88
Power flow betweenness	-1.00	-1.00	-0.99	-1.00	-0.95	-0.94	-0.80	-0.95	-1.00	1.00	0.88
MBCC-HITS algorithm	0.38	-0.05	0.44	0.09	0.45	-0.10	0.53	0.25	0.88	0.88	1.00

Figure 2-8. Matrix of Spearman's rank correlation coefficient for some CN approaches using the same test case (IEEE14).

Recently, Li et al. and Rocchetta and Patelli [242, 279] presented a similar analysis to show the correlation, but between the power flow approach and CN methods. They demonstrated that a relatively high correlation (0.6–1) exists between AC- and DC-based power flow models. Rocchetta and Patelli [279] also concluded that there is a weak (-1 to 0.3) and moderate (0.3–0.6) correlation between the power flow method and selected CN metrics. Li et al. [242] present the same results between the power flow method and the selected CN metrics but the selected CN metrics are moderately and highly correlated. Particularly, Cortes et al. [226] show that hierarchical method as a logical method shows a higher correlation with power flow results in comparison with CN methods.

However, some studies (e.g. [235, 242]) present a high correlation between CN and other methods but according to Figure 2-8 and some articles (e.g. [15, 279]), it is not possible to rely on CN completely. That is why the extended and pure CN methods are currently improving and new centralities are being proposed to consider the realistic properties of networks and operating limits. This improvement in CN centralities may increase its disadvantages (e.g. accuracy) as well as maintain its advantages (e.g. being easy and fast) at the same time.

2-4-4 Emerging topics and future research work

Based on the literature review and the comparisons, we can point out four emerging topics that require further research efforts.

N-k problem (N-k contingency analysis): Most power transmission networks fulfill the so-called “N-1 security criterion”. If any single component fails, the loads can be restored without load shedding [5, 272]. However, blackouts often result from cascading failures rather than a single-component failure. Unpredictable combinations of circumstances or inadequate controls can disconnect further lines or nodes [280], jeopardizing the common N-1 (or even N-2) security criteria [28]. Topical research analyzes the N-k ($k \geq 2$) contingency and its impacts on the robustness of the power system [166].

Models cannot consider all combinations of failures. Real systems consist of thousands to tens of thousands of components (N). A single failure requires the verification of only N cases. However, an N-k analysis must consider $\binom{N}{k}$ cases [281]. For an illustrative example, using an Opteron processor with 2.2-GHz clock speed, and 3-GB memory per processor, N-2 and N-3 contingency analysis of the IEEE-118 system with 118 nodes will take around 1 day and 65 days, respectively [270]. Fortunately, Li et al. [242] and Rosato et al. [282] show that N-3

analyses suffice to measure the importance of a bus or a branch in a single or coupled networks, and modern algorithmic approaches are promising to investigate the optimal N-k level [242].

Robustness and optimal decision: Many factors affect the development of CI. Economic, political, demographic, social, and technological drivers can cause delay or stop deployment [161]. Operators should consider a holistic perspective, which integrates robustness, resilience, and reliability [283, 284]. It also means computing trade-off between cost and benefits [285]. For instance, small and low-cost changes in power grids can substantially increase robustness [286]. Changing 5.5% and 2% of links could increase the EU power grid's robustness by 45% and 27% [286]. In contrast, installing new lines can decrease the grid's robustness, as presented in the so-called Braess paradox [238].

Technology evolution and emerging threats: The power system is observing various fundamental transformations, which generate vulnerability. We introduce three major threats below.

Prosumers: Most literature focuses on the high voltage level, at which large blackouts happen [6]. However, some studies [151, 287] show that large blackouts could increase with the shift towards distributed generation and prosumers (producers and consumers of energy). The main role of high-voltage grids will change in the future and hence distribution systems must be considered to be at risk and in need of vulnerability analysis.

Prosumers come with the concept of smart grids. A smart grid uses communication technology to improve efficiency, load balancing, and network management [60, 149, 283, 288-291]. It also increases the potential for cyber-attacks and jeopardizes the security of the power system. These changes complicate the analysis and management of the grid [6].

The interdependency and combination of CIs: CIs are becoming increasingly interconnected [292]. An accident in a specific infrastructure, e.g. water and energy, can trigger a cascading failure in the other sectors. For instance, an event in a gas network can cause the shutdown of the gas-fired generators, and in turn in the energy sector. The interdependency significantly affects power security [288]. It requires a holistic analysis, including the nexus perspective.

Climate change and renewable energy: Many countries are engaged in decarbonizing their energy mix, while some are phasing out nuclear energy. Renewable energies are deployed around the world. However, the intermittent forms of renewable energy bring network operators the challenge of balancing production with the real-time demand. This threatens the stability

and security of the power system. In particular, extreme weather, which could increase with climate change, can disturb the energy system [288, 293].

Most energy policies aim to increase energy efficiency, thus decreasing energy consumption. However, limiting carbon emissions can actually increase electricity demand. Heat and transport sectors tend to move from fossil fuels to electricity [294]. Therefore, electricity supply and transmission capacity must follow the growing demand to limit threats to the security of power systems.

Hybrid approaches: The growing complexity of some networks jeopardizes the reductionist methods [295]. A holistic approach requires a hybrid one because each method possesses its own limitations. This means the perfect method does not exist, Table 2-9 shows. An emerging idea is to integrate different methods to obtain better, faster, and more accurate results at the same time. For instance, complex network methods require low computing burden while the power flow method is more accurate but slow. To take advantage of their respective strengths, they can be integrated using "importance and criticality" definitions, as discussed below.

Importance and criticality are two key concepts that should not be confused [296]. The important component in a system possesses a high portion of responsibility (e.g. provides or carries more power in power grids), while the critical components drastically affect the performance of that system if they are disconnected [297]. Figure 2-9 presents the differences between these two concepts with a simplified three-line network. Line 2 is always important because it transports a large volume of electricity. However, in Figure 2-9(a), line 2 is not critical. If it is disconnected, the system keeps delivering the full load through lines 1 and 3. In Figure 2-9(b), line 2 is both important and critical because the full load (here 700) can no longer be supplied without it.

Indeed, some centralities such as "degree" and "betweenness" show very well the importance of components but not their criticality. Briefly speaking, for a large network with thousand components, applying a more accurate approach like the AC power flow is impossible. We can apply complex networks to rank the importance of components, and then apply a more accurate approach like the AC power flow to the top important components (e.g. 30% of the top important components in the list) to exactly find the most critical ones, not to all components. In this manner, we can integrate both the approaches.

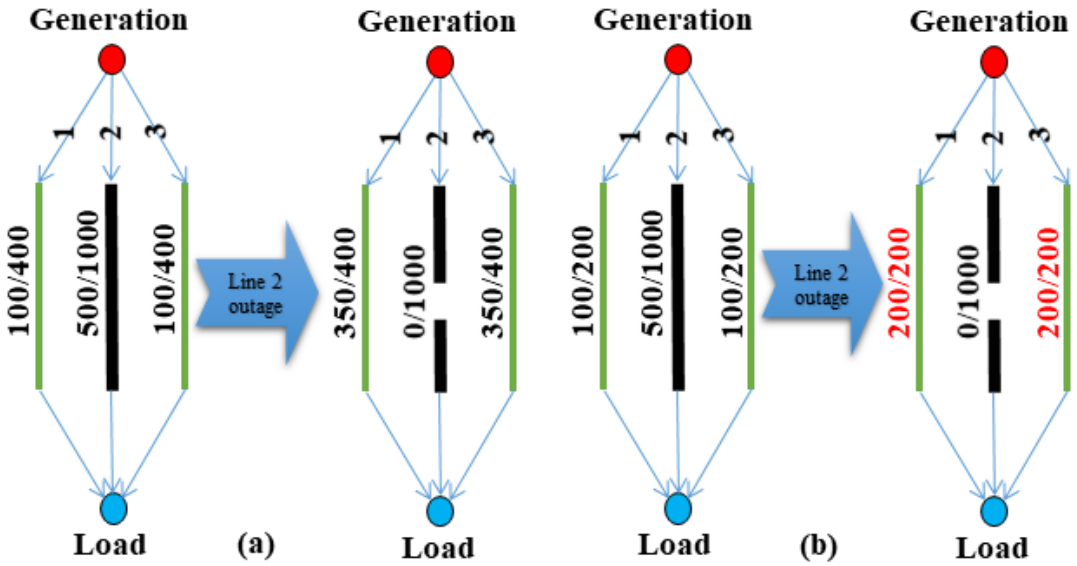

Figure 2-9. Important vs. critical components: (a) line 2 (black line) is an important component but not a critical one (b) line 2 (black line) is an important as well as a critical component (x/y on the line: x is the operating power and y is the installed capacity).

2-5 Conclusion

Literature on vulnerability analyses of CI incessantly grows. Scientists innovate in this field, and this review provides a snapshot of the current state-of-play. New approaches will emerge in the coming years. Unavoidably, this review should be continued in the future. Nevertheless, we trust it will remain relevant for a while for two main reasons.

First, this chapter filled a gap in other published reviews. It provided a broad overview of the methods, rather than focusing on a specific one. We devoted substantial effort in summarizing, categorizing, and identifying the strengths of each analytical method. The chapter therefore guides the reader through this field of research, as illustrated in Figure 2-3. We also focused on three classes of events, namely natural hazards, intentional attacks, and random failures (Figure 2-1) that will help scholars determine the relevant application of the various methods available, including emerging methods. Finally, we provided and compared various relevant definitions of vulnerability. They cover a broad set of interpretations, which are unlikely to evolve significantly.

Second, scientists are currently innovating with hybrid approaches. Ongoing research focuses on integrating the above-presented methods, rather than developing new ones. With AI and

deep learning, new boxes could emerge in Figure 2-3. However, knowing and comparing the established methods can support scholars in choosing the more relevant integrative approaches.

This chapter summarized about 100 papers in the tables and reviewed totally about 300 articles. Rather than providing a take-home message, we recommend keeping in mind Table 2-9. It summarizes the advantages and disadvantages of the standard methods in vulnerability analysis. It highlights that no modeling approach can investigate all aspects of this field. In fact, the appropriate model depends on the type of event and the specific case study. Thus, this chapter contributes to guiding the reader in this fascinating and topical field.

Part Two

Single-level vulnerability analysis

This part has been published in:

Abedi, A., et al., *MCDM approach for the integrated assessment of vulnerability and reliability of power systems.* IET Generation, Transmission & Distribution, 2019. **13**(20): p. 4741-4746.

Abedi, A., L. Gaudard, and F. Romerio, *Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems: The benefits and limitations.* Reliability Engineering & System Safety, 2020. **201**: p. 106961.

Chapter 3

MCDM approach for the integrated assessment of vulnerability and reliability of power systems

3-1 Introduction

In the last years, increasing efforts have been developed on the analysis and prevention of possible disruptions of electricity supply. Two complementary approaches can be taken into account to manage these risks in power systems, considering high probability but low-impact events and low probability but high impact events [182, 193, 298]. The first kind of events is related to N-1 contingencies and it comes under the scope of the reliability. Reliability can be defined as the ability of the electric power system to meet the demand with continuity and an acceptable level of quality. Several approaches are possible to assess the reliability of the power systems, from analytical to Monte Carlo probabilistic models. Monte Carlo is a more flexible methodology in comparison with analytical approaches but it takes more computation time, especially when complex operating conditions and system states are considered [299].

The second kind of events is related to N-k contingencies and it refers to cascading failures in power systems. Vulnerability can be defined as the level of degradation of a system when deliberate attacks or random failures make the network elements successively out of operation.

A single outage of a transmission line of the power grid can lead to an overload of other lines, making more likely the failure of other electric assets and finally resulting in a catastrophic failure of the whole system. Some of the biggest blackouts have occurred in recent years, causing serious economic damage and driving the need for vulnerability assessment of the electric power critical infrastructures [6]. In the scientific literature, some works analyze the vulnerability of electrical infrastructures by using different techniques. For instance, some authors justified that the statistical measures of graph theory are adequate to carry out assessments of structural vulnerability on power systems [182].

Other researchers are using alternative measures, such as [300] that incorporated several topological and power-flow-based indices into a general framework able to evaluate system vulnerability and, consequently, provide information about the susceptible areas of the energy infrastructure. The concepts of reliability and vulnerability are both related to the continuity of operations of critical infrastructures, and their study is required to prevent potentially destructive events [301]. However, researchers have not considered integrating both risk analysis perspectives into a unique decision framework. Few papers can be found in literature about joint consideration of reliability and vulnerability [95, 302]. Reliability analysis has been the main approach for risk management in electrical critical infrastructures and vulnerability analysis has received attention only in the last years, but both concepts should be taken simultaneously into account to improve the planning of the expansion of power systems.

Previous research applied to power systems concluded that vulnerability analysis should be used as a complement to reliability analysis but it did not address how to use the results from vulnerability and reliability analyses for making decisions on critical infrastructures [95]. In contrast, our research provides a robust calculation of reliability and vulnerability indices and, at the same time, a combination of both approaches to improve the decision-making process on the best network topology under an integrated risk assessment framework using multi-criteria decision making (MCDM). We propose a method to compare the performance of different networks under reliability and vulnerability criteria.

The rest of this chapter is organized as follows: first, Section 3-2 introduces the methodology and the algorithms proposed to calculate vulnerability and reliability. A case study is presented in Section 3-3. Then, simulation results of the vulnerability and reliability analyses are shown and explained in Section 3-4. Finally, in Section 3-5, the comparison and discussion of results are done, and an MCDM method is applied to jointly analyze both concepts. The chapter summary and conclusions will be provided in Section 3-6.

3-2 Methodologies

3-2-1 Structural vulnerability assessment

Vulnerability is an internal characteristic of critical infrastructures that measures the inability of the system to withstand the effects of failures [276]. Frequently, it is quantified based on the largest connected component, both before and after cascade events [303].

To determine the impact of cascading failure events, power grid performance is measured according to the electrical loads that remain connected after several interdiction events. Some measures have been applied to previous research works to estimate load shedding as a percentage of the total system demand [304-306]. In this chapter, we propose the unsatisfied demand (UD) index to measure the power system performance when it is subject to cascading failures caused by disconnection of overloaded power lines.The UD metric allows determining the impact of cascading failures by quantifying the demand that can be satisfied in the electrical infrastructure after multiple line removals. The UD index is calculated as follows:

$$UD = 1 - \frac{\sum_{i} Demand_i}{Demand_{base}} \tag{3-1}$$

Where $Demand_i$ is demand met on island *i*, $Demand_{base}$ is the total demand for base case.

The UD index varies between 0 and 1. Thus, as the UD index increases, the impact on satisfied demand in the power system also increases. The flowchart of the algorithm presented in Figure 3-1 allows determining the structural vulnerability of the power grids. The calculation is performed using (3-1) where the UD index is calculated during each disintegration stage of network. Initially, the algorithm calculates DC power flows and determines power line overload limits using a user-defined parameter α as

$$Overload_{threshold} = \alpha_j \times Flow_{base_j} \tag{3-2}$$

Where α_j is the tolerance parameter of line *j*, and $Flow_{base_j}$ is the base power flow of line *j*. Cascading failures are initiated by removing the most heavily loaded line. The algorithm then calculates the new power flows and verifies that the power lines do not exceed the overload threshold determined in Equation (3-2). If the latter is not achieved, the overloaded electrical lines are removed, and then the formation of islands or isolated elements caused by the previous

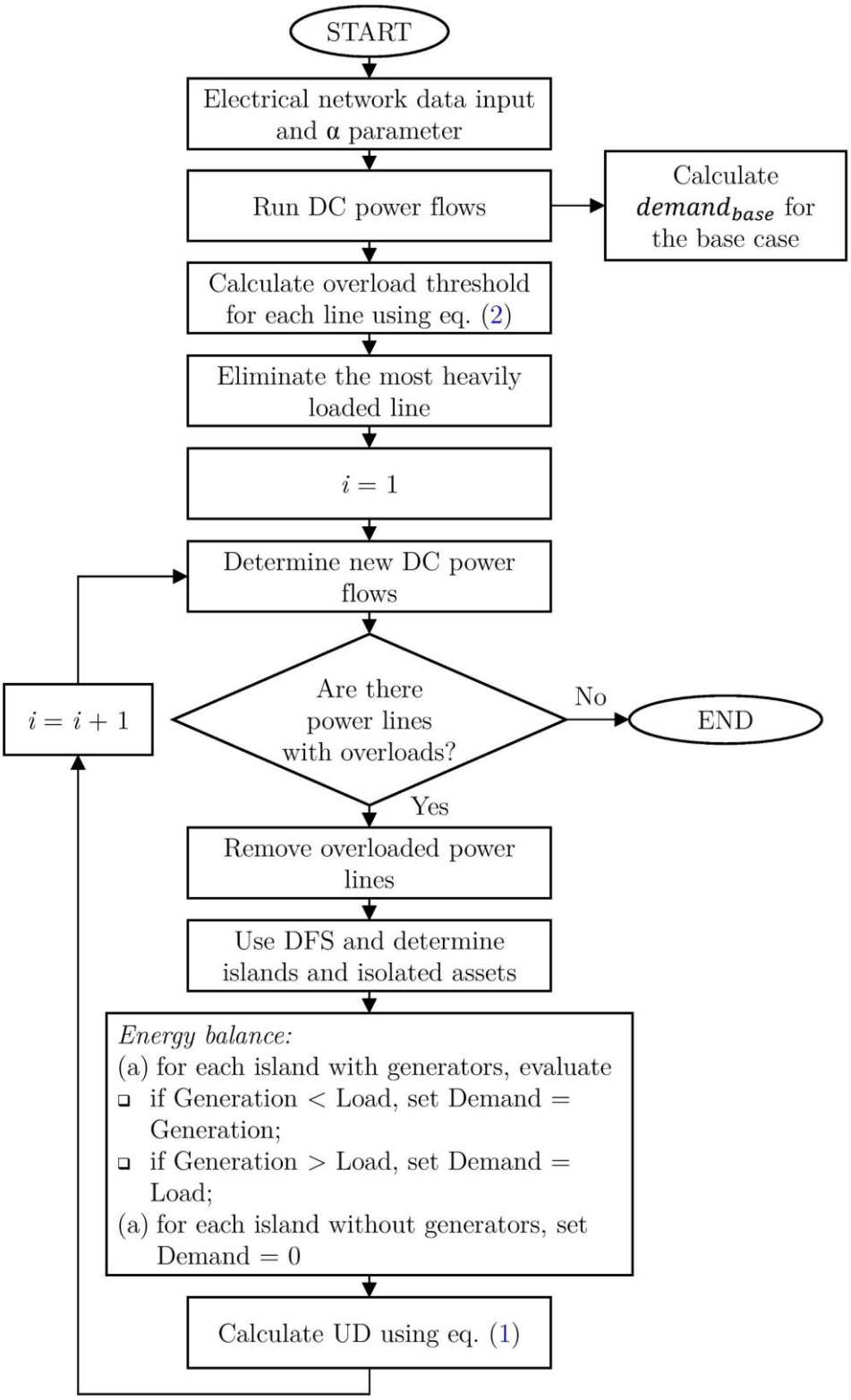

Figure 3-1. Flowchart to calculate the structural vulnerability of power systems

event is determined. We used deep first search algorithm to solve the problem mentioned above [307].

Due to the formation of multiple islands, the developed algorithm incorporates an energy balance routine to determine the maximum demand that can be satisfied in each subnet. In other words, islands with a generation higher than their demand will be able to satisfy the connected load, while islands with a generation lower than their demand will only be able to satisfy the load equivalent to the generation. Islands without generation or isolated buses are considered as unsatisfied load in the algorithm.

Cascading events also continue on these islands. In this way, DC power flows are run in each subsystem and, in parallel, the UD index is calculated. The algorithm ends once all power lines have been removed or there are no more overloads in the system. DC load-flow models provide a suitable capability for this kind of power system security analysis. In this regard, voltage magnitudes might not be a major concern and DC power flow studies provide sufficient accuracy [308]. The algorithm has been programmed in the MATLAB programming environment.

3-2-2 Reliability assessment

In Monte Carlo simulation, two main techniques are usually employed: time-sequential and non-sequential. In non-sequential techniques (system state sampling) each time step or system state are considered independently while sequential techniques can be used realistically to simulate the actual chronological process and random behavior of system [108, 309]. Time-sequential Monte Carlo technique is used here for the reliability assessment because it is more flexible, accurate and provides calculation of different indices such as expected frequency of load curtailments (EFLC) but it needs more computation time [108, 299, 309, 310]. For an in-depth description, some useful references can be found in the literature [298, 311, 312].

Implemented time-sequential Monte Carlo technique for reliability assessment of a power system is presented in the flowchart of Figure 3-2 using the following steps [108, 299, 309] :

Step 1: Specify the initial state and number of components that can fail. It is assumed that all components are in a normal state and have only two states (normal and failure).

Step 2: Calculate the residing time (the time the component spends in each state). In this case, uniform random numbers (r) are used, and time to failure (TTF) and time to repair (TTR) are sequentially calculated employing failure rates (λ) and mean time to repair (MTTR) of components, using (3-3) and (3-4):

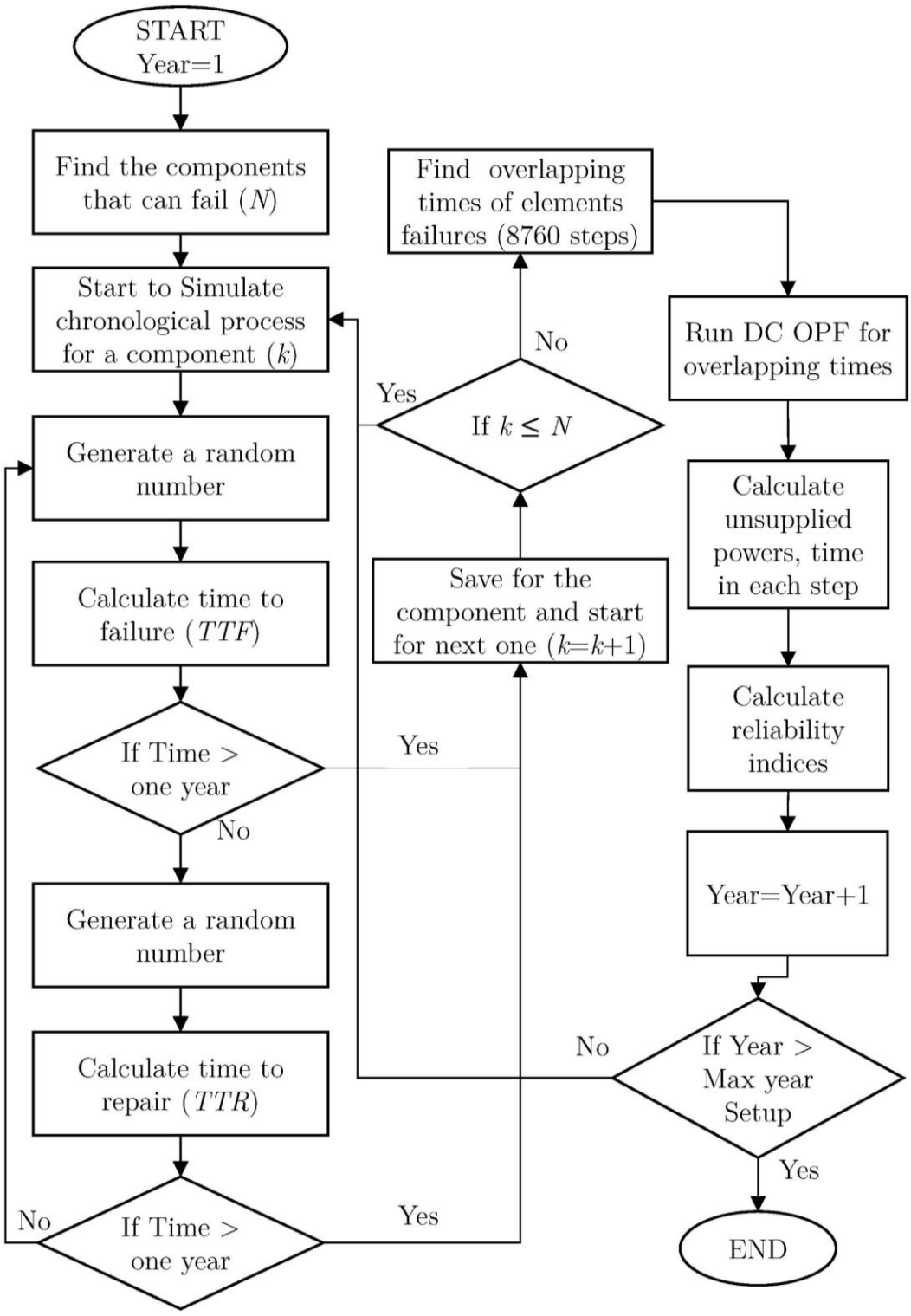

Figure 3-2. Flowchart of reliability analysis of power systems.

$$TTF = -\frac{\ln(r)}{\lambda} \times 8760 \tag{3-3}$$

$$TTR = -\ln(r) \times MTTR \tag{3-4}$$

This step should be repeated for each component for a specific time span, normally one year.

Step 3: After providing the artificial history of the system in above steps, overlapping times of elements failures are needed. The time steps considered are hours of one year (8760 steps).

Step 4: Power flow calculation of new topology by considering the element failures. Optimal DC power flow (OPF) is employed to specify the effects of failed elements removal on supplied energy and normal operation of system. MATLAB is used for OPF calculations [313].

Step 5*:* Calculate the reliability indices using the results provided from previous step and following reliability indices [95, 108, 299, 309]:

- **Expected energy not supplied (EENS) (MWh/year):**

$$EENS = \frac{\sum_{i=1}^{N_y}(\sum_{j=1}^{N_i} E_{j,i})}{N_y} \tag{3-5}$$

where, $E_{j,i}$ is power system energy not supplied of j^{th} power interruption, in year *i*, N_y is total number of simulated years and N_i is total number of interruption in year *i*.

- **Expected demand not supplied (EDNS) (MW):**

$$EDNS = \frac{EENS}{8760} \tag{3-6}$$

- **EFLC or loss of load frequency (LOLF) (outages/year):**

$$EFLC = \frac{\sum_{i=1}^{N_y} N_i}{N_y} \tag{3-7}$$

- **Expected duration of load curtailment (EDLC) or loss of load expectancy (LOLE) (hours/year):**

$$EDLC = \frac{\sum_{i=1}^{N_y}(\sum_{j=1}^{N_i} D_{j,i})}{N_y} \tag{3-8}$$

Where $D_{j,i}$ is duration of j^{th} power interruption, in year *i*.

- **Probability of load curtailment (PLC) or loss of load probability (LOLP) (%):**

$$PLC = \frac{EDLC}{8760} \tag{3-9}$$

- **Average duration of load curtailments (ADLC) or loss of load duration (LOLD) (hour/disturbance):**

$$ADLC = \frac{EDLC}{EFLC} \tag{3-10}$$

Step 6: Steps 2–5 are repeated and the indices are accumulated until the coefficient of variation EENS is less than tolerance error. According to previous works, a relative tolerance error of 6% is established [299].

3-3 Case studies

In this chapter, the IEEE Reliability Test System (RTS-96) [314] is used as a test system. This network is a good test case for bulk power system reliability evaluation studies because of available required data (see Figure 3-4). IEEE RTS-96 bus system has three areas that are mirrored copies of Figure 3-4. These areas are interconnected with different components (Figure 3-3). For example, Area 1 is connected with three lines to Area 2, Area 2 with 1 line to Area 3 and Area 3 is connected with an extra bus, a transformer and a line to Area 1 [314]. In this chapter, five different combinations of the three areas are used for reliability evaluation in five case studies. In each area, 94 components can fail i.e. 24 buses, 32 generators and 38 branches and transformers. In addition to data which are available in [314], failure rate and MTTR of buses are considered 0.001(/year) and 24 h, respectively [95]. It is assumed that the annualized peak power demand for each area is 2850 MW [314].

3-4 Simulation results

3-4-1 Results of vulnerability analysis

Figure 3-5 reports the degradation of the networks under study caused by the outage of transmission line 14–16. This power line is the most loaded in all systems. We obtain the plotted results after applying the algorithm shown in Figure 3-1 by considering a parameter $\alpha = 1$ in all cases.

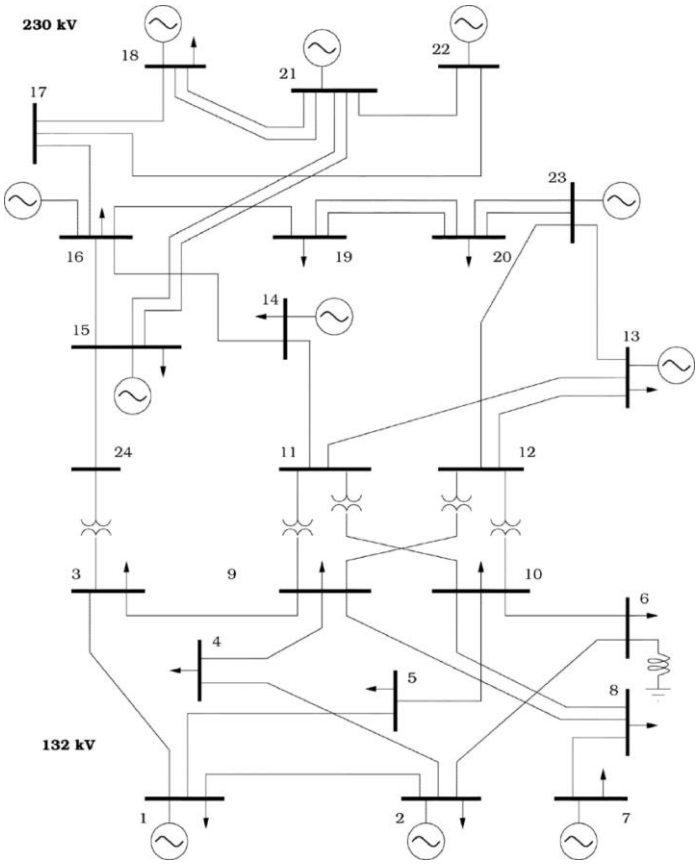

Figure 3-4. Diagram of IEEE 24-bus reliability test system.

The curves represent the UD calculated during each disintegration step of the network. Initially, the UD index has a value equal to 0 when all the loads in the power grid are satisfied. Then, the UD index progressively increases until a value equal to 1 when the whole system is disintegrated due to the removal of the overloaded lines. At this point, the system cannot meet the demand of the power grid.

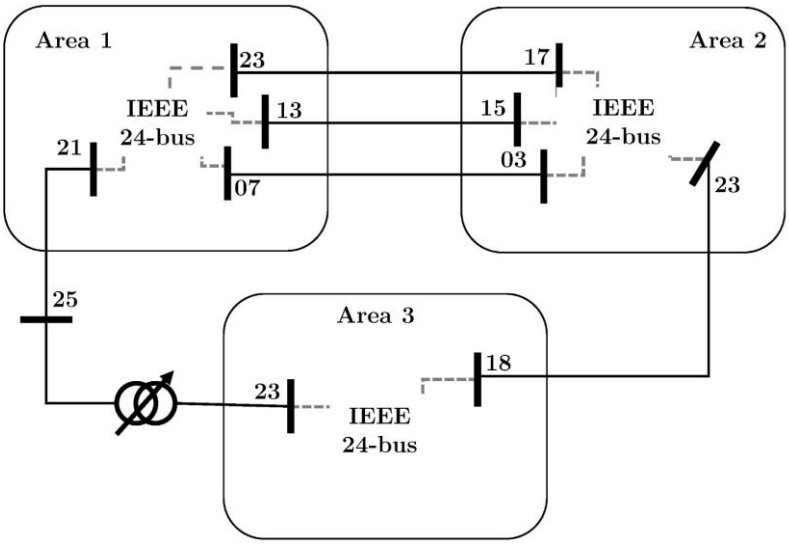

Figure 3-3. Diagram of IEEE 24-bus reliability test system.

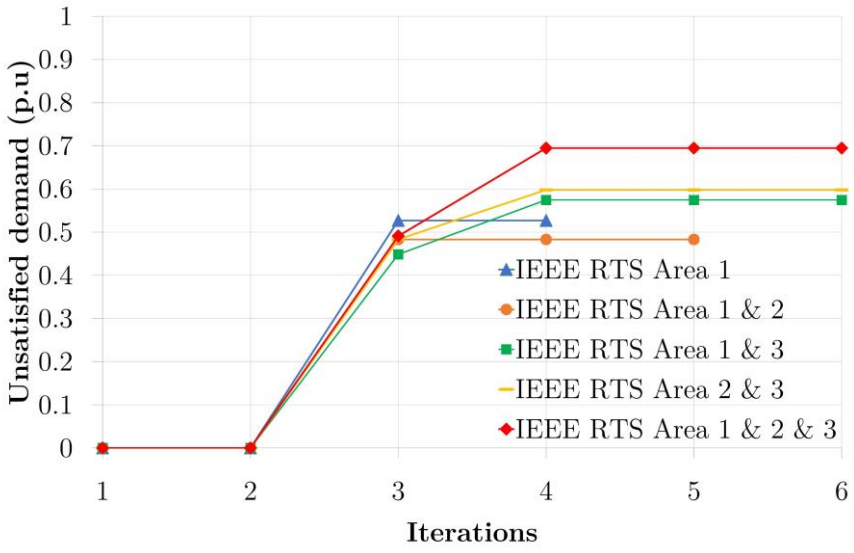

Figure 3-5. Vulnerability curves.

Figure 3-5 shows that Area 1&3, Area 2&3 and Area 1&2&3 reach their maximum point of disintegration in iteration six, while Area 1&2 in iteration five and Area 1 in iteration four. The above indicates that the propagation of cascading effects grows as the network increases in size.

Therefore, it can be observed that Area 1&2&3 is the most vulnerable network since 70% of the demand is not satisfied, while Area 1&2 proves to be the most robust network since ~50% of the load on the power network remains satisfied. In short, the most vulnerable systems can be determined graphically from least to most vulnerable as follows: Area 1&2, Area 1, Area 1&3, Area 2&3 and Area 1&2&3. In this manner, we have a measure of the behavior of the networks under study, which allows us to classify them according to their degree of vulnerability.

3-4-2 Results of reliability analysis

The time-sequential Monte Carlo simulation approach has been applied to the same five different topologies from IEEE RTS-96. Figure 3-6 shows the deviations of EENS and coefficient of variation (COV) for a 1500-years simulation. The simulation process can be stopped when the COV for EENS or EDNS is less than 6%, following recommendations from [299]. Convergence for EENS or EDNS is slower than others [95]. It is also clear from comparing the COV of different reliability indices in Table 3-1. As it can be concluded from

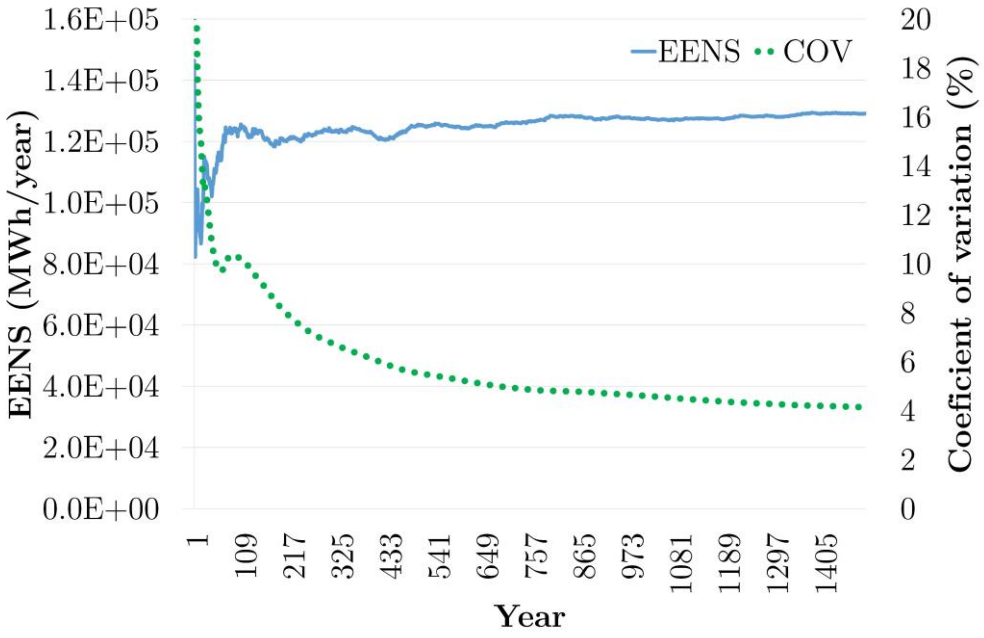

Figure 3-6. EENS and coefficient of variation for area 1 and 1500-year time span.

Figure 3-6, it is not necessary to run a 1500-year simulation to reach a COV below 6%. Thus, results plotted in Figure 3-7 are obtained from calculations done for a 500-year simulation.

Table 3-1. Annualized system indices for the IEEE-RTS (Area1)

Reliability index	**Ref. [95]**	**Ref. [315]**	**This work**	**COV (%)**
EENS	127,546	134,590.60	130,513.96	5.54
EDNS	14.56	15.36* (134,590.6/8760)	14.90	5.54
EFLC	18.8	18.57	19.12	3.83
EDLC	732	740.22* (0.0845 ×8760)	744.69	3.43
PLC	8.3	8.45	8.50	3.43
ADLC	38.8	39.86* (740.22/18.57)	38.95	3.23

* These are calculated using available data in [315].

Figure 3-7 shows that connecting similar networks that can meet their demands by self-generation increases the reliability index (relative EENS). Moreover, how the three coupled

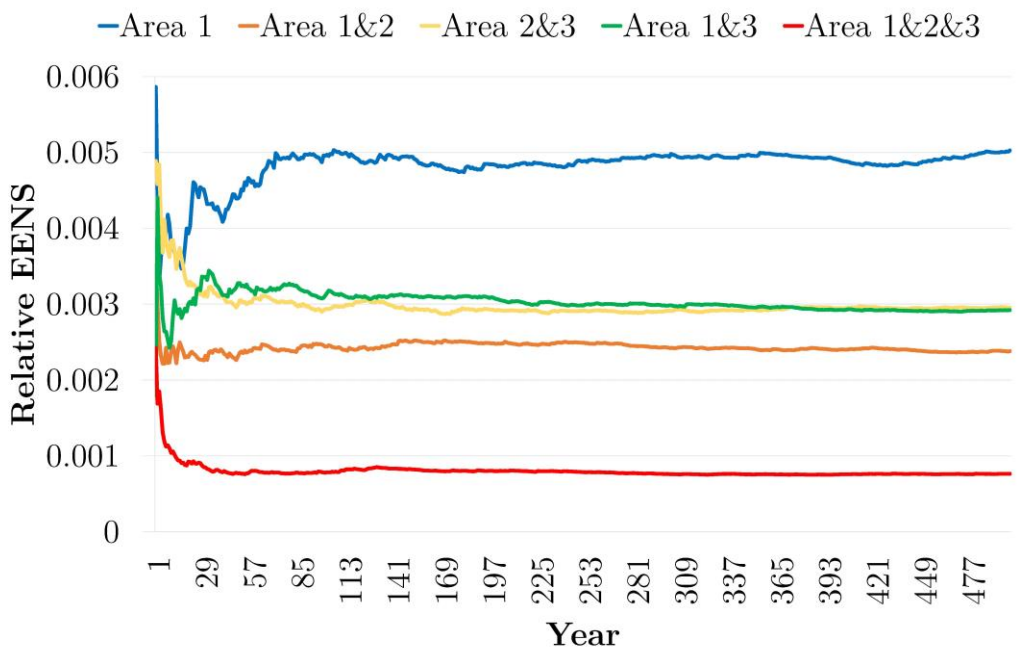

Figure 3-7. Comparison of reliability index (relative EENS) for different topologies.

networks are connected is also important. Here, Area 1&2 is more reliable because there are three interconnecting lines between the networks 1 and 2, providing redundancy to the system. Area 1&3 that has three interconnecting components has similar behavior. However, Area 2&3, with only one interconnecting component, is less reliable. The reason can be the small failure rates of the bus (0.001/ year) and the transformer (0.02/ year). Therefore, these components can be ignored in one-year simulation span. So, we can assume that Areas 1&3 and 2&3 have interconnecting lines with failure rates of 0.52 and 0.53/year, respectively.

3-5 Discussion

3-5-1 Reliability and vulnerability concepts

Reliability and vulnerability assessment study the ability of a system to perform its desired functions under given conditions for a period of time and the weakness level of a system to failures, disasters or attacks, respectively [95, 316]. Reliability assessment is dependent on probability of component failure but vulnerability assessment does not consider probability. Other difference relies on the different number of simultaneous failures that both techniques take into account.

Figure 3-6 and Figure 3-7 show that vulnerability assessment considers 0 to 100% of components removal. On the other hand, in order to show the number of simultaneous failures in reliability assessment, 1500-year time span (1500×8760 h) for all topologies is simulated.

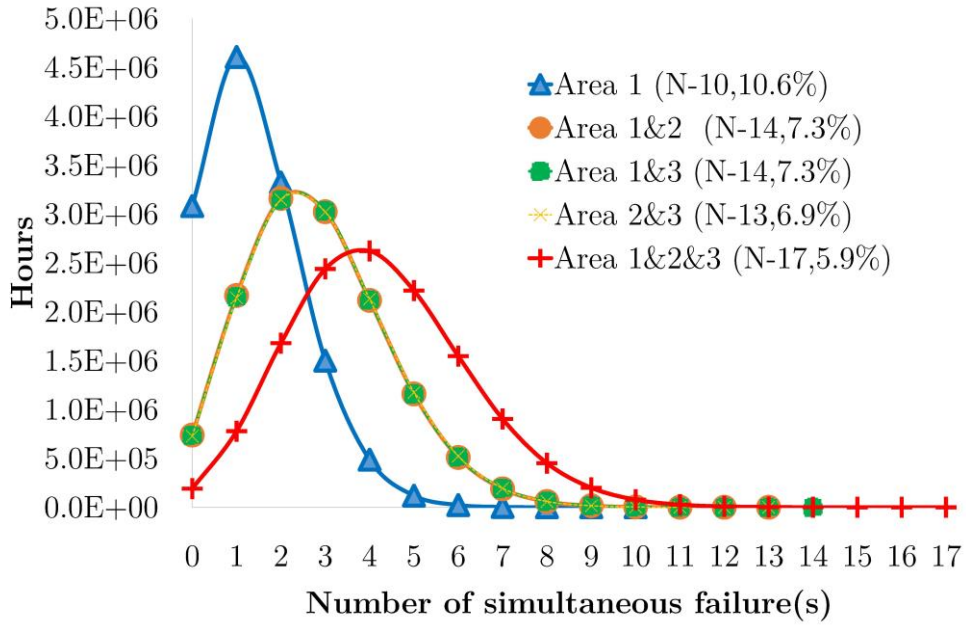

Figure 3-8. Distribution of number (hours) of simultaneous failures in different topologies for a 1500-year time span (maximum number of possible simultaneous failure and maximum percentage of simultaneous component failures are presented in parenthesis).

The results are presented in Figure 3-8. It shows that the percentage of simultaneous failures decreases when the dimension of the network increases. In addition, it shows that reliability analysis only considers maximum 10.6% of component outages. Vulnerability assessment can complement the reliability analysis considering the rest of N-k failures.

3-5-2 Reliability and vulnerability comparison

This section is intended to the joint comparison and discussion of the results of reliability and vulnerability assessment, integrating both risk analysis perspectives. With respect to the structural vulnerability analysis, observing Figure 3-5 it is possible to conclude that Area 1&2&3 is the least robust case since the UD is higher than in the remaining cases under study. In other words, large systems are highly vulnerable, when compared to those systems with small size but more compact. With respect to the reliability analysis, it is possible observing Figure 3-6 and Figure 3-7 how the largest system (Area 1&2&3) is the less sensitive to power outages as a consequence of any element malfunctioning, i.e. the most reliable. In fact, the ranking of relative EENS from Table 3-2 (Area 1&2&3, Area 1&2, Area 1&3, Area 2&3, and Area 1) seems to be quite different to that obtained from the vulnerability results shown in Figure 3-5 plotted from lowest to highest vulnerability (Area 1&2, Area 1, Area 1&3, Area 2&3, Area 1&2&3). This reasoning suggests that a vulnerable power system may not be unreliable, or inversely, an unreliable energy power system is not necessarily vulnerable. The interconnection

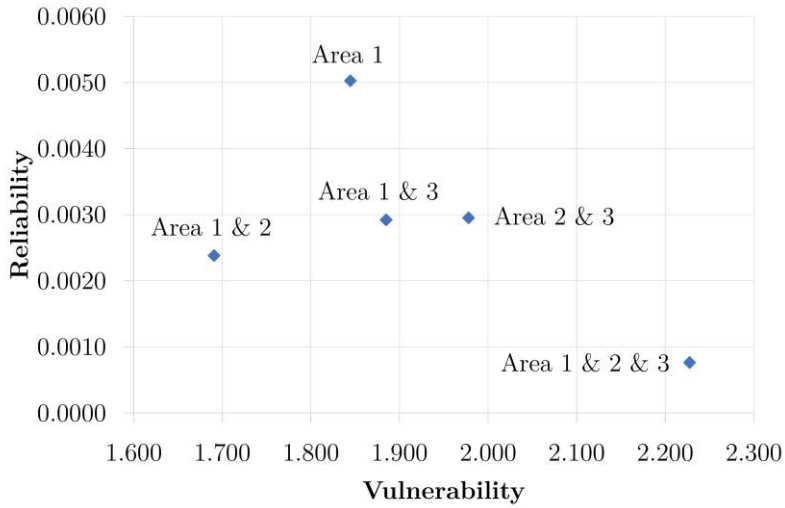

Figure 3-9. Comparison of relative EENS (reliability index) and vulnerability index for different systems.

of energy sub-systems 1, 2 and 3 results in a global system with higher reliability, i.e. the lowest value of relative EENS for Area 1&2&3 in Figure 3-9. However, the amount and type of interconnection links between the sub-systems are crucial from the vulnerability perspective. The values of vulnerability in Figure 3-9 have been obtained through the parameter area under curve (AUC) for each curve in Figure 3-5. The values of reliability have been taken from the results of relative EENS shown in Table 3-2. The pairwise comparison in Figure 3-9 lets us confirm the previous conclusions: the system named as Area 1 is the least reliable, but more robust, because of its compact size, and the system of Area 1&2&3 is the most reliable, but less robust, since reliability improves with interconnections, but vulnerability becomes worse due to faster propagation of cascading failures.

Table 3-2. Annualized system indices and data for the IEEE-RTS

Reliability index	**Area 1**	**Area 1&2**	**Area 1&3**	**Area 2&3**	**Area 1&2&3**
Total demand, MW	2850	5700	5700	5700	8550
Number of components	94	191	191	189	289
EENS, MWh/year	130,513	118,913	145,876	147,422	56,990
Relative EENS (EENS/total demand/8760 h)	0.0052	0.0024	0.0029	0.0030	0.0008
EDNS, MW	14.90	13.57	16.65	16.83	6.50
EFLC, outages/year	19.12	26.33	26.86	26.69	18.08
EDLC, hours/year	744.69	901.17	1017.94	1029.78	439
PLC, %	8.50	10.29	11.62	11.76	5.01
ADLC, hour/disturbance	38.95	34.22	37.90	38.58	24.30

3-5-3 Reliability and vulnerability integration

In this section, the goal is to show how the decision-makers' priorities on reliability and vulnerability could be taken into account to select the best topology. MCDM methods are usually applied to provide a ranking of alternatives using different measures and criteria. The Technique for Order Preferences by Similarity to an Ideal Solution (TOPSIS) is one of the MCDM methods to find the best alternative that is the closest to the positive ideal solution and farthest to the negative ideal solution [317, 318]. In our case, we consider five different topologies of IEEE RTS as the alternatives and vulnerability and reliability indices as the measures.

Thanks to TOPSIS approach, the ranking of five IEEE RTS topologies based on the decision-makers' priorities are shown in Figure 3-10 scoring each topology. Reliability (R) and vulnerability (V) weights are considered for decision making. For example, from decision-makers' perspective 'R(10%), V(90%)' means the weights of reliability and vulnerability are 10 and 90%, respectively, and the final scores of topologies are from 1 (the best) to 5 (the worst).

Figure 3-10 shows that IEEE RTS Area 1&2 would be mostly the best topology. However when considering vulnerability weights between 0 and 20% (reliability between 80 and 100%) IEEE

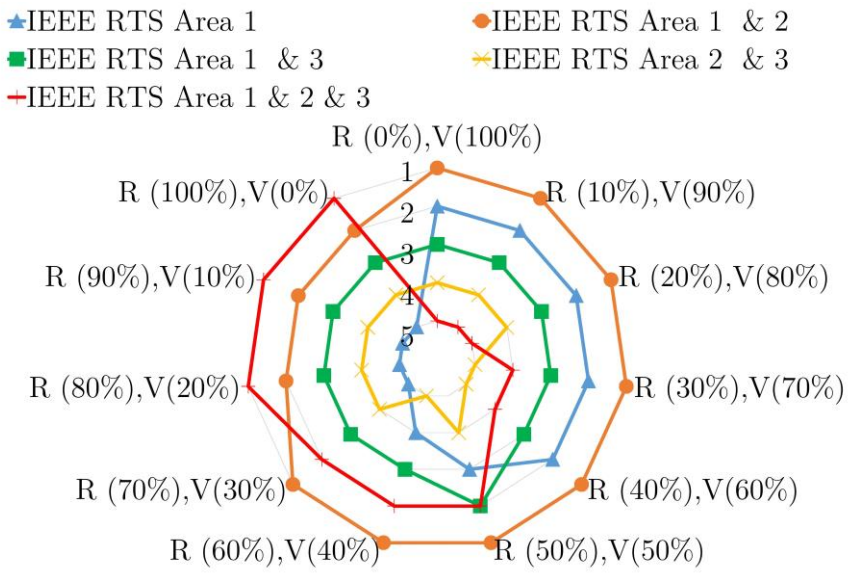

Figure 3-10. Ranking of five IEEE RTS topologies based on the decision makers' priorities on reliability (R) and vulnerability (V).

Area 1&2&3 becomes a better topology. These two solutions dominate the other three networks IEEE Areas 1, Areas 1&3, and 2&3 as it can be also checked in Figure 3-9.

3-6 Conclusion

In this chapter, a novel methodology has been developed for the joint consideration of vulnerability and reliability of power systems. Indices to measure system vulnerability as well as power and energy related definitions frequently used on reliability studies (EENS, EFLC, EDLC, among others) have been integrated into a wide discussion, aiming to quantitatively determine the pros and cons of the current energy transmission system designs. Five different topologies based on the IEEE RTS-96 test case have been studied from the vulnerability and reliability perspectives. According to the information available and calculation carried out, the behavior of the system from the vulnerability viewpoint could be different to that observed from the reliability perspective. For example, the largest system, Area 1&2&3, shows the highest reliability (relative EENS value, 0.0008) but the worst vulnerability (value of AUC of UD, 2.2275). On the contrary, the smallest system, Area 1, has low reliability (0.0050) but good vulnerability measure (1.8446). Thanks to the use of a multi-criteria approach, TOPSIS, rankings of the five IEEE RTS-96 topologies have been obtained, considering different reliability (R) and vulnerability (V) weights based on the decision-makers' priorities. The analysis also depends on how each topology is planned and interconnected. Reliability improves with interconnections between the systems, making a power system more reliable as more interconnected is but making it simultaneously more vulnerable as it is more exposed to propagation of cascading failures. Then, a compromise solution can be found for each power system, weighting reliability and vulnerability into an integrated decision framework.

Chapter 4

Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems

4-1 Introduction

Energy systems are critical, and their reliability and robustness are fundamental requirements for the well-being of modern society. Any failure can affect a large population and generate high costs. For instance, three independent events in Iran, North America, and Italy hit a total of 128 million people in 2003. More recently, 670 million Indian people and 70 million Turkish people were temporarily deprived of power in 2012 and 2015, respectively [3-6]. In the USA, the annual cost of weather-related blackouts ranges from $20 to $55 billion [319]. Thus, improving the robustness and reliability of power grids against different hazards and threats has become essential in the implementation of the energy strategies, such as in Europe [320], and the USA [321].

While reliability assesses the ability of the electric power system to meet the demand with continuity and an acceptable level of quality, vulnerability analysis identifies the level of degradation of a system when deliberate attacks or random failures make the network elements successively out of operation. Reliability analysis has been the main approach for risk

management in electrical infrastructure and vulnerability analysis has received attention only in the last years, but both concepts should be taken simultaneously into account to improve the planning of the expansion of power systems [22].

Scientists have been developing innovative methods to assess the reliability and determine critical components whose failures lead to the largest system loss (i.e., vulnerability analysis) [322]. They can range from analytical approaches to Monte Carlo simulations. A detailed comparison of these approaches is recently conducted in [20] and [323] for vulnerability and reliability assessments in power systems, respectively. Generally, these kinds of capacity-based assessments need iterative power flow-based approaches to model the power system behavior. Solving accurate but non-linear alternating current (AC) power flow equations, needs a significant computational burden. Direct current (DC) approach limits this issue by linearizing the equations, which is necessary for large-scale simulations or when analyzing many failure scenarios.

Some researchers investigated the effects of the assumptions in their respective fields. LaRocca et al. [199] and Cetinay et al. [324] show that in a normal state of a power system, the DC model (DCM) shows accurate results and efficiently approximates the AC model (ACM). However, DCM can lead to inaccurate and optimistic predictions for cascading failures. Qi et al. [325] compare three different DC-based approaches in contingency analysis without considering the effects of reactive power. Overbye et al. [326] determine the accuracy of DCM on locational marginal pricing (LMP) calculations. Qin et al. [327] and Benidris and Mitra [328] show the effects of voltage and reactive power assumptions on composite system reliability indices. Kile et al. [329] also present the differences in the models' results for contingency and reliability analysis. Others compare the power flow-based approaches with topology-based methods [279, 330]. They found that a DCM, although better correlated to ACM in comparison with topology-based methods, still fails to report some critical components of the power system.

All of the above-mentioned works only compare the different measures of power flow-based models and analysis of the sources of inaccuracy is missing. Hence, we aim to figure out the sources of inaccuracy in power flow-based models of different line capacity-based assessments including vulnerability, reliability and contingency assessments. First, time-sequential Monte Carlo simulations, an N-k′-1 contingency analysis, and a novel vulnerability index are used to evaluate numerically different line capacity-based assessments. We investigate both low-load and stressed networks using ACM and DCM. Then, the impacts of each parameter (i.e., power losses, reactive power flows, voltage variations and small-angle approximation) on the

inaccuracy of power flow-based models are considered. In this regard, we provide an in-depth analysis of the reliability indices using Monte Carlo simulation, and we duplicate the results using a fixed seed to investigate the sources of inaccuracy in both models.

The rest of this chapter is organized as follows: First, the methodologies and assessment are introduced in Section 4-2. Then, the test cases and the results of different line capacity-based assessments are presented in Sections 4-3 and 4-4, respectively. The sources of inaccuracy in the results will be discussed in Section 4-5. The conclusions will be provided in Section 4-6.

4-2 Methodologies

4-2-1 AC and DC power flow models

Power flow-based approaches study the steady-state model of the power system [331]. For a network with *N* buses and *G* generators, the AC power flow equations are [332]:

$$Pg_{i|i\in G} - Pd_{i|i\in D} = \sum_{j\in N} P_{ij}; \quad \forall i, j \in N \tag{4-1}$$

$$Qg_{i|i\in G} - Qd_{i|i\in D} = \sum_{j\in N} Q_{ij}; \quad \forall i, j \in N \tag{4-2}$$

$$P_{ij} = V_i^2 G_{ij} - V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}); \quad \forall i, j \in N \tag{4-3}$$

$$Q_{ij} = -V_i^2 B_{ij} - V_i V_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij}); \quad \forall i, j \in N \tag{4-4}$$

$$Pg_i^{\min} \le Pg_i \le Pg_i^{\max}; \quad \forall i \in G \tag{4-5}$$

$$Qg_i^{\min} \le Qg_i \le Qg_i^{\max}; \quad \forall i \in G \tag{4-6}$$

$$\left(P_{ij}\right)^2 + \left(Q_{ij}\right)^2 \le \left(S_{ij}^{\max}\right)^2; \quad \forall i, j \in N \tag{4-7}$$

$$V_i^{\min} \le V_i \le V_i^{\max}; \quad \forall i \in N \tag{4-8}$$

$$\theta_{ij}^{\min} \le \theta_{ij} \le \theta_{ij}^{\max}; \quad \forall i, j \in N \tag{4-9}$$

Where, Pg_i and Qg_i are generated active and reactive powers at bus *i*, respectively. Pd_i and Qd_i are active and reactive demands at bus *i*, respectively. P_{ij}, Q_{ij} and $S_{ij}^{\max}$ are active and reactive power flows and line capacity between buses *i* and *j*, respectively. V_i and θ_{ij} are voltage magnitude at bus *i* and voltage angle difference between buses *i* and *j*, respectively. Finally,

$Y_{ij} = G_{ij} + jB_{ij}$ is the admittance between buses *i* and *j*. Equations (4-1) and (4-2) are the nodal power balance equations for active and reactive powers, respectively. Equations (4-3) and (4-4) represent the line flows of active and reactive powers, respectively. Constraints (4-5)-(4-9) enforce the limits of active and reactive power generations, transmission line capacity, voltage magnitude, and voltage angle difference, respectively.

These AC power flow equations are nonlinear. To solve them, iterative numerical solutions must be used, such as the Gauss-Seidel, the Newton-Raphson or the decoupled power-flow methods [332]. Unfortunately, these equations require a large computational burden, which may lead to a convergence problem and are sensitive to initial guess. Thus, the linearized model of ACM (i.e., DCM) is usually used, as it is faster and discards any convergence problems [53, 200]. However, DCM makes various simplifications. It ignores reactive power, the variation of voltage magnitude, power losses, and line resistance [331]. It also approximates the small angle. In other words, it considers that the differences in the voltage angles between the neighboring buses *i* and *j* are insignificant. Therefore, DCM assumes that $\sin(\theta_{ij}) \approx \theta_{ij}$ and $\cos(\theta_{ij}) \approx 1$ [324]. The main goal of this chapter is to investigate the impacts of such hypotheses on vulnerability, reliability and contingency analyses.

4-2-2 Vulnerability assessment

"Vulnerability analysis" ranks the critical components to the unforeseen events. It detects the components that highly impact the whole system if they fail. A vulnerability can be physical, systemic, social, organizational, economic, environmental, and territorial. However, this study focuses on systemic vulnerability [333]. It investigates how the whole system behaves when some components or interconnected systems fail. Redundancy, functionality, and dependency matter for this vulnerability analysis [20]. Figure 4-1 presents the flowchart of vulnerability assessment in which two scenarios are proposed:

1) Increasing the load.

In this scenario, the model incrementally increases the load by 5%. Both ACM and DCM are used simultaneously to calculate the system parameters such as voltage, line power flow and so on. The stopping criterion will be satisfied as soon as the first difference in the topology of the network is seen. This difference can be provoked by the inaccuracy of DCM in power flow modeling in comparison with ACM (e.g., reporting a safe line when it is actually overloaded and vice versa).

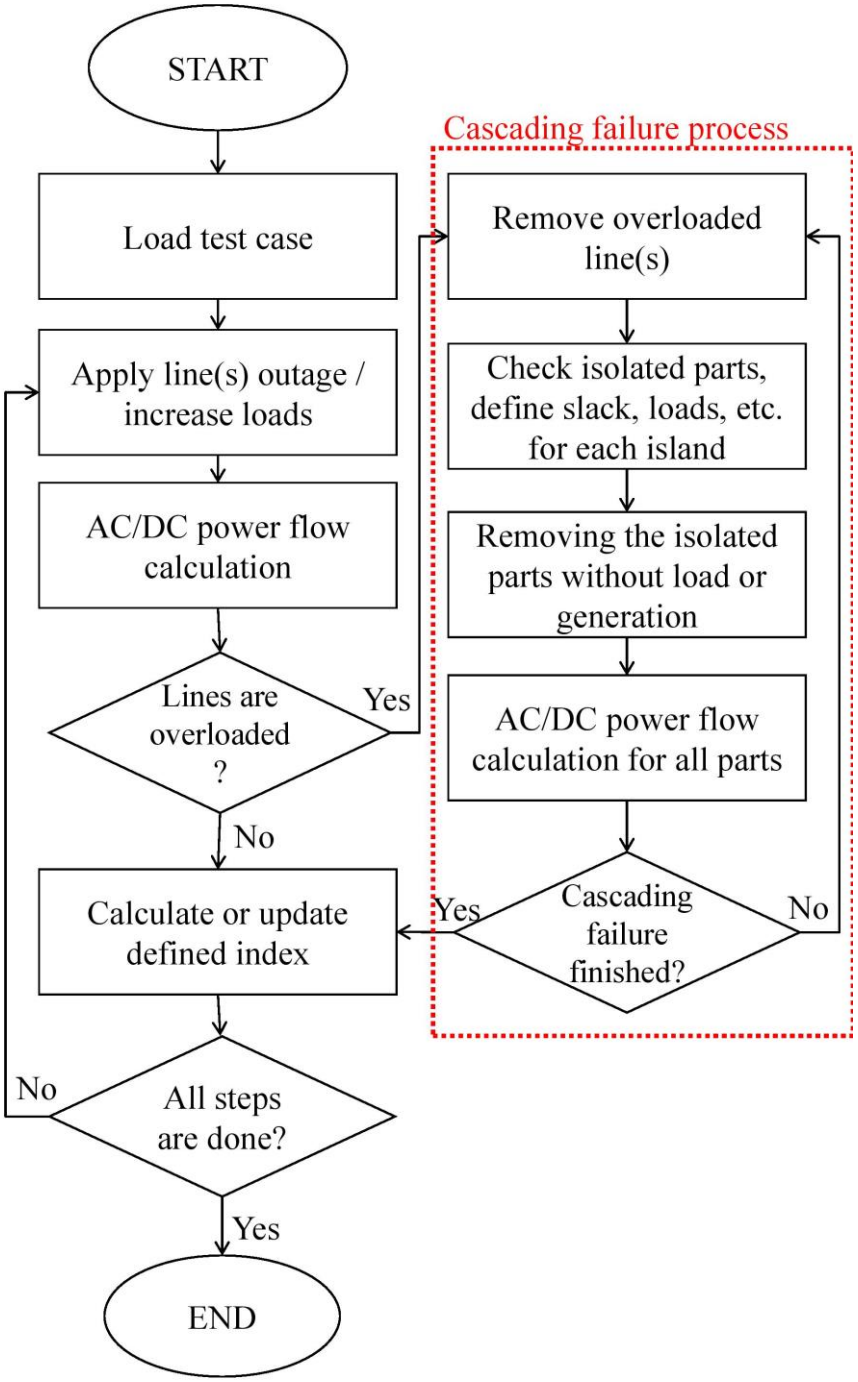

Figure 4-1. The flowchart of vulnerability analysis.

2) Calculating the number of overloading (NOL).

Removing a transmission line in a power system shifts the power flow to other lines (where they usually operate near their limits) to compensate the load demand. This event could overload some lines and finally lead to their disconnection by triggering their protective relays.

The main aim is to find the number of times the lines are overloaded (NOL) during the N-k contingency analysis using the following equation:

$$NOL = \sum_{k=1}^{N} \sum_{c=1}^{C_k} S_{kc} \tag{4-10}$$

Where, C_k is the number of *k*-combinations from *N* components (i.e., $C_k = \binom{N}{k}$). S_{kc} is equal to 1 if there is any overloading, otherwise 0. Following Li et al. [242] and Rosato et al. [282], the results are accurate enough for the N-k contingency analysis if *k* is less than or equal to 3 (i.e., up to N-3). In our test case, 9177 simulations are needed to perform the N-k ($k \leq 3$) contingency analysis.

Based on these two scenarios, we can quantify the vulnerability of the grid and identify divergence between ACM and DCM. For both scenarios, cascading failures due to the overloaded lines are considered [324, 334]. To simulate a cascading failure, the overloaded lines are removed and the disintegration of the grid is checked at every cascading stage. Figure 4-2 shows a tree structure of a cascading failure process. Some islands may not be completely affected by flow redistribution. These islands have enough generation resources and can satisfy their demands such as green islands in Figure 4-2. Some islands may not have electricity generation or load after the disintegration of the grid. These "dead" islands are marked in red in Figure 4-2. The cascading failure process still iterates on all islands with overloaded lines (i.e., black islands in Figure 4-2). The stopping criterion is when there is not any overloaded line in all islands [334]. It should be noted that curtailing the generation and load shedding are the supply and demand balancing rules in the islands where the load and generation are not balanced. Furthermore, the amount of active and reactive power demands and active power supply are decreased (e.g., by 1%) until either convergence is reached or the island becomes a dead island for probable convergence problems in ACM. In contrast to ACM, no supply or demand shedding due to convergence problems is needed in DCM after the supply and demand balancing in the islands [324, 334].

4-2-3 An N-k′-1 scenario

In contrast to the N-k contingency analysis, an N-k′-1 scenario studies the consecutive loss of k'+1 (or k) components in which k' components are removed consecutively in the previous k' steps and the next step, one critical component will be removed based on the predefined criteria.

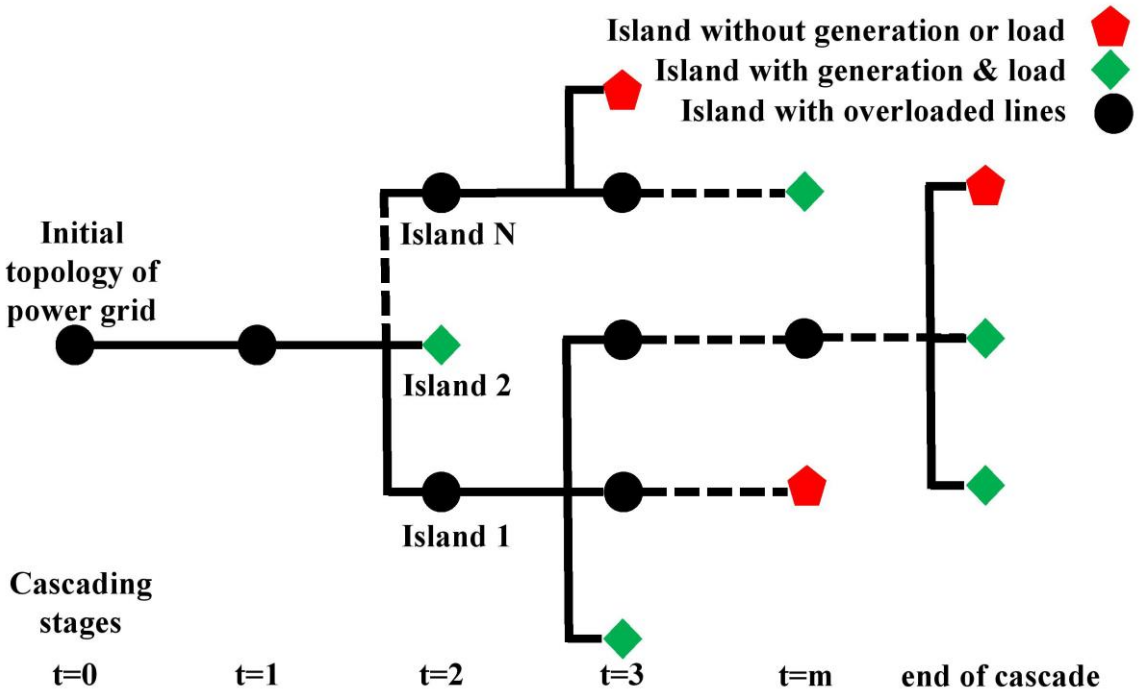

Figure 4-2. A tree structure of a cascading failure process.

For instance, the N-1-1 scenario studies the consecutive loss of two components while the N-2 contingency analysis studies the simultaneous loss of two components in a power system [335]. In this work, the N-k′-1 concept is used and the aim is to compare ACM and DCM for this type of analysis.

To remove the most critical and important line in each step, the following criteria are considered on all active islands, i.e. the islands with both load and generation:

1st) the line that maximizes the load shedding if removed,

2nd) the line that minimizes the total line capacity if removed,

3rd) the line with a minimum capacity margin.

The main criterion is the first one, i.e. the line that maximizes the system damage (e.g., the load shedding). On the other hand, criterion 2 is considered only if criterion 1 does not find a solution and so on. Then, the model defines a new topology and considers the probable load-generation balancing, cascading failures, and other disruptions like the introduced procedure in Figure 4-1. The end is when all lines are removed, and all generation nodes are isolated.

4-2-4 Reliability assessment

Power system reliability consists of providing specific services under defined conditions and period [95]. Several approaches are possible to assess the reliability of the power systems, from analytical to Monte Carlo probabilistic models. Monte Carlo is a more flexible methodology in comparison with analytical approaches but increases the computation burden, especially when complex operating conditions and system states are considered. In Monte Carlo simulations, two main techniques are usually employed: time-sequential and non-sequential. In non-sequential techniques (system state sampling) each time step or system state is considered independently while sequential techniques can be used realistically to simulate the actual chronological process and random behavior of system [336]. This accurate flexible approach requires a large computation capacity compared to non-sequential techniques [336]. For this study, accuracy and flexibility are fundamental, thus leading to employ the sequential approach [337]. It consists of the following steps [338] as illustrated in Figure 4-3.

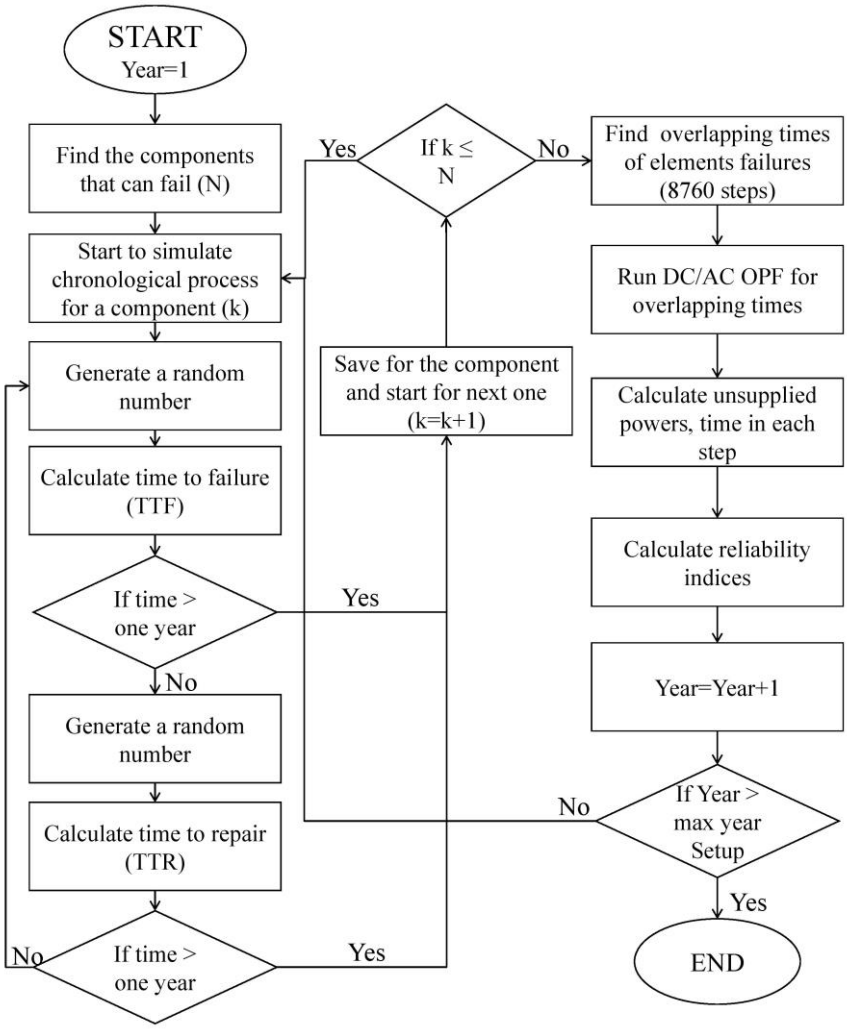

Figure 4-3. The flowchart of reliability analysis.

Step 1: Specify the initial state and number of components that can fail. It is assumed that all components are in a normal state and have only two states (normal and failure).

Step 2: For a specific component *k*, the time to failure (TTF_k) is determined accordingly to equation (4-12) [338]:

$$TTF_k = -\frac{\ln(r_k)}{\lambda_k} \tag{4-12}$$

Where, r_k denotes a random number uniformly distributed in (0 1), and λ_k is the annual failure rate [#/year]. Then, the time to repair (TTR_k) is computed accordingly to equation (4-13) [338]:

$$TTR_k = -\ln(r_k) \times MTTR_k \tag{4-13}$$

Where, $MTTR$ denotes the mean TTR [hours].

Step 3: When the states of all components are known for a specific year, the model computes the overlapping times of elements failures, i.e., when various components are simultaneously out of service.

Step 4: Power flow calculation of new topology by considering the element failures. Optimal DC/AC power flow (OPF) is employed to specify the effects of failed element removal on energy supply and normal operation of the system. The open-source MATLAB based simulation package, MATPOWER [313], is used for OPF calculations.

Step 5: Calculate the reliability indices using the results provided from the previous step. The reliability indices are described in Section 3-2-2.

Step 6: This whole cycle is repeated until the coefficient of variation (COV) for expected energy not supplied (EENS) index meets the tolerance error, here 6%. Different reliability indices have different convergence speeds. The EENS index with the lowest rate of convergence is used to ensure that others are well converged [336].

4-3 Test systems and assumptions

In this chapter, the IEEE reliability test system (RTS-96) [240] is used as a test system (see Figure 4-4). Data availability makes it an ideal test case for bulk power system reliability evaluation. It consists of three interconnected mirrored sub-areas. It has three areas that are

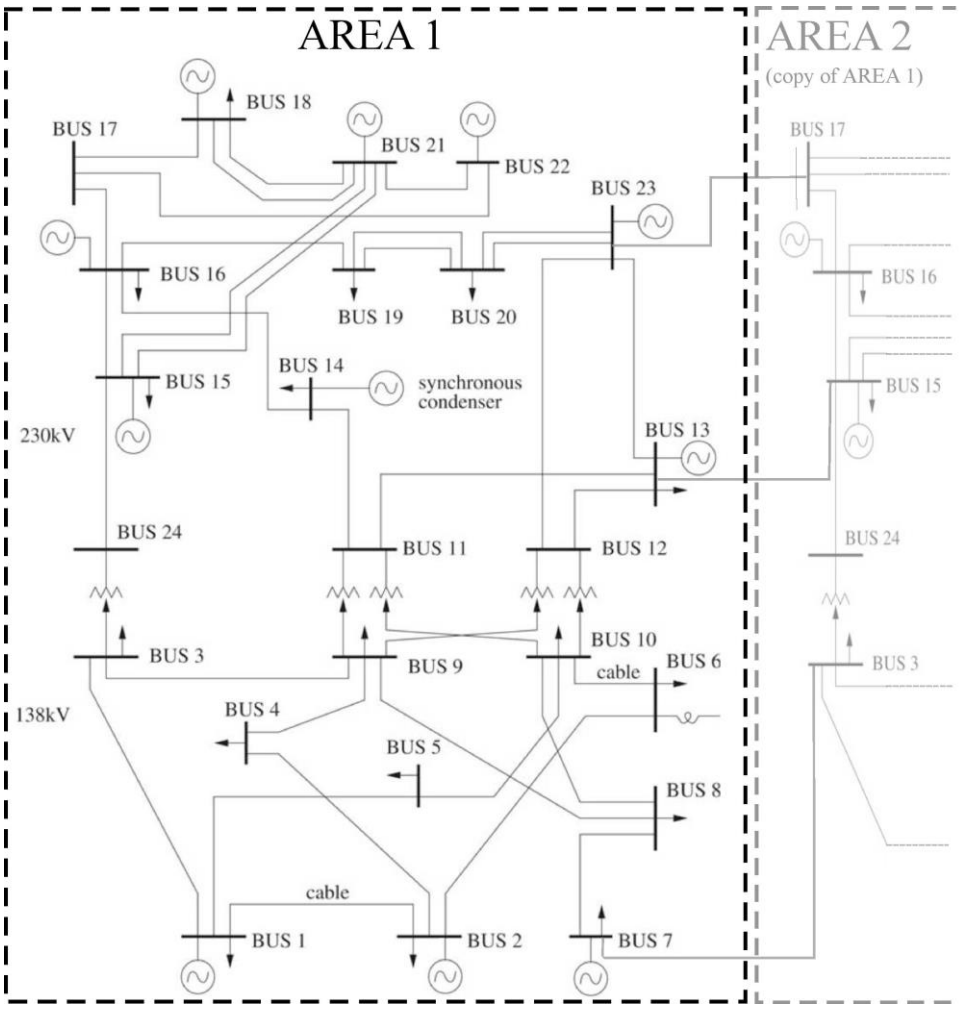

Figure 4-4. Two interconnected copies of the IEEE RTS 24-bus.

mirrored copies of Figure 4-4 (area 1). These areas are interconnected with different components. For example, area 1 is connected with three lines to area 2 (Figure 4-4) and so on [240]. In this chapter, two different combinations of three areas are used for reliability evaluation i.e., area 1 and area 1&2. In each area, 94 components can fail i.e., 24 buses, 32 generators and 38 branches and transformers. In addition to data that are available in [240], failure rate and MTTR of buses are considered 0.001(#/year) and 24 hours, respectively [95]. It is assumed that the annualized peak power demand for each area is 2850 MW [240].

Second, we consider the IEEE modified reliability test system (MRTS) [328]. It only multiplies the peak generation and loads of the first case by 2 and 1.8, respectively. The goal of introducing MRTS is to better consider the effects of removing the transmission lines in power system reliability analysis. The contribution of the transmission lines on reliability analysis can be ignored in RTS [328] because the line capacity limits are much higher than the loading level.

It should be noted that for all simulations, $V^{\min}$ and $V^{\max}$ are usually assumed 0.95 and 1.05, respectively in MATPOWER. However, they are based on the allowed voltage fluctuations. Finally, the used $S^{\max}$ is available in RATE_A column of the branch matrix in IEEE test cases [313].

4-4 Simulation results

4-4-1 Vulnerability analysis

Increasing total load: This criterion consists of increasing the load up to reach the point where the network shows different behavior in both modeling approaches. In this scenario, loads of RTS are equally increased by 5%. The topology of the network changed after a 35% increase in loads using ACM and DCM. Line loading of four lines exceeds 100% in ACM while only three lines are overloaded in DCM. The results show that for about 30% of the cases, the line loading difference is more than 10% and more specifically, for about 10% of the cases, the difference is more than 40%. In the next section, the sources of these errors are investigated in detail.

Number of overloading (NOL): The second analysis is to calculate the number of overloading (NOL) using N-k ($k \leq 3$) contingency analysis. Figure 4-5 shows NOL for each transmission line (i.e., the line between buses X and Y). It proves that the used method for power flow calculations can affect the results of vulnerability assessments in a power system. For instance,

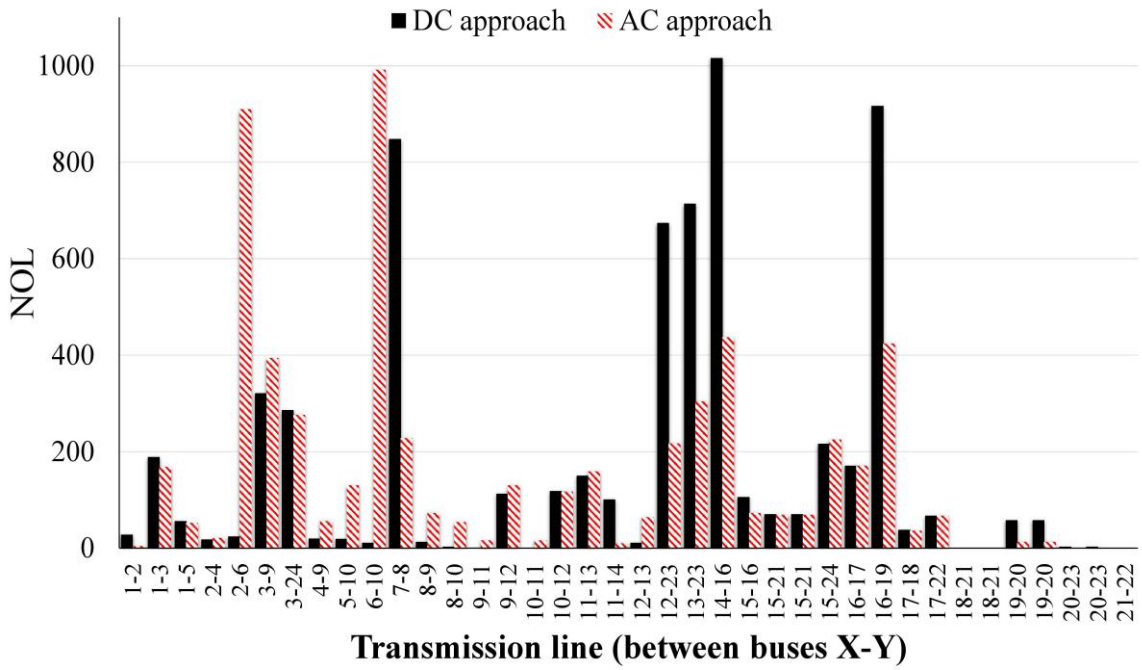

Figure 4-5. Number of overloading (NOL) using DCM and ACM.

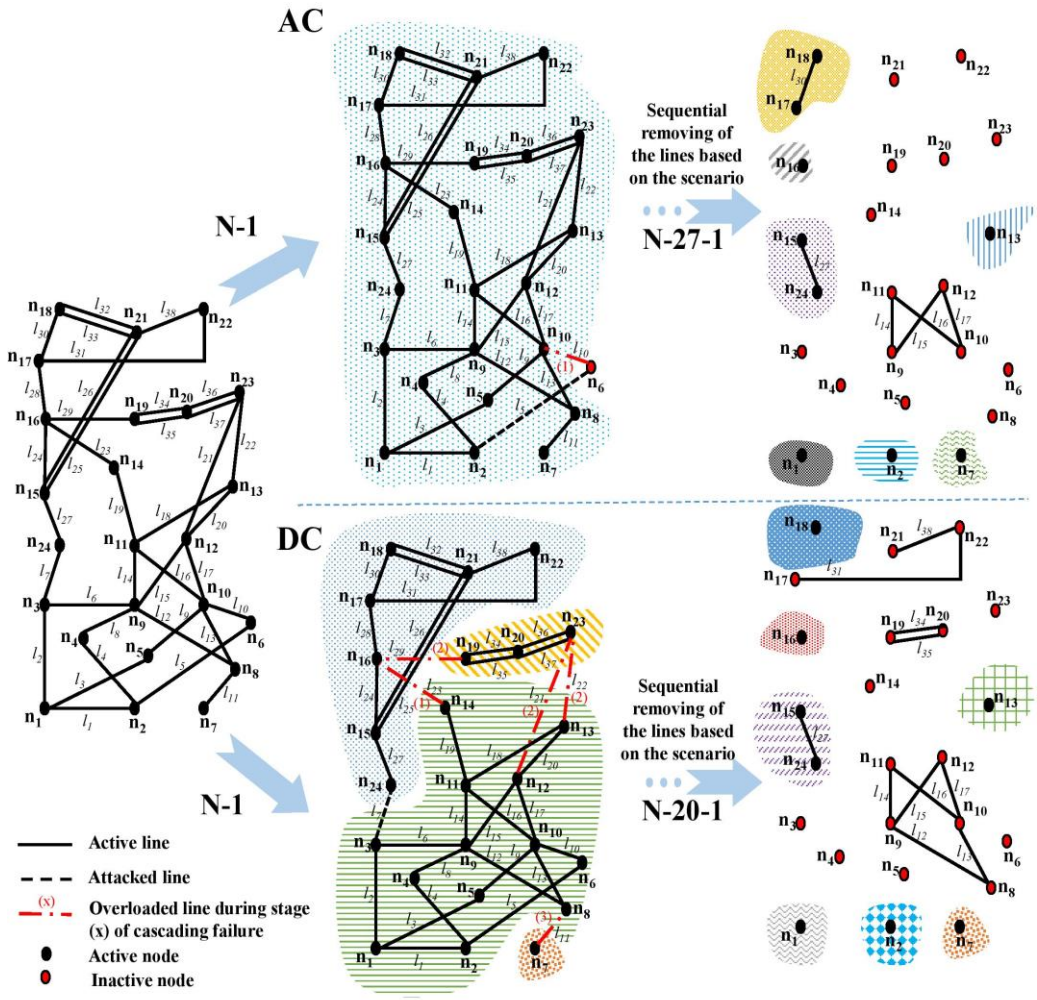

Figure 4-6. Consecutive removing the critical lines based on N-k′-1 scenario using ACM and DCM (the active zones are highlighted).

ACM spots some new critical lines (e.g., 2-6, 6-10) in addition to the lines reported by DCM (e.g., 7-8, 12-23, 13-23, 14-16, 16-19). N-1 contingency analysis using DCM leads to a cascading failure when one line of 3-24 or 24-15 is removed (see Figure 4-6). This disruption overloads the 500 MVA line 16-19 with 502 MVA. In ACM, the line loading only reaches 486 MVA, therefore no cascading failure is triggered. ACM only observes an overloading problem in lines 6-10 and 2-6. Ignoring the reactive powers and losses in DCM can be the main reasons for these differences that are investigated in the next section.

4-4-2 Contingency analysis (the N-k′-1 scenario)

Figure 4-6 shows the initial, second and the last state of the system with the N-k′-1 scenario using both approaches. The lines l_5 and l_7 are reported as the critical lines for the first iteration using ACM and DCM, respectively. In both scenarios, removing the proposed critical lines leads to a cascading failure of one or five line(s) in different cascading stages. The cascading

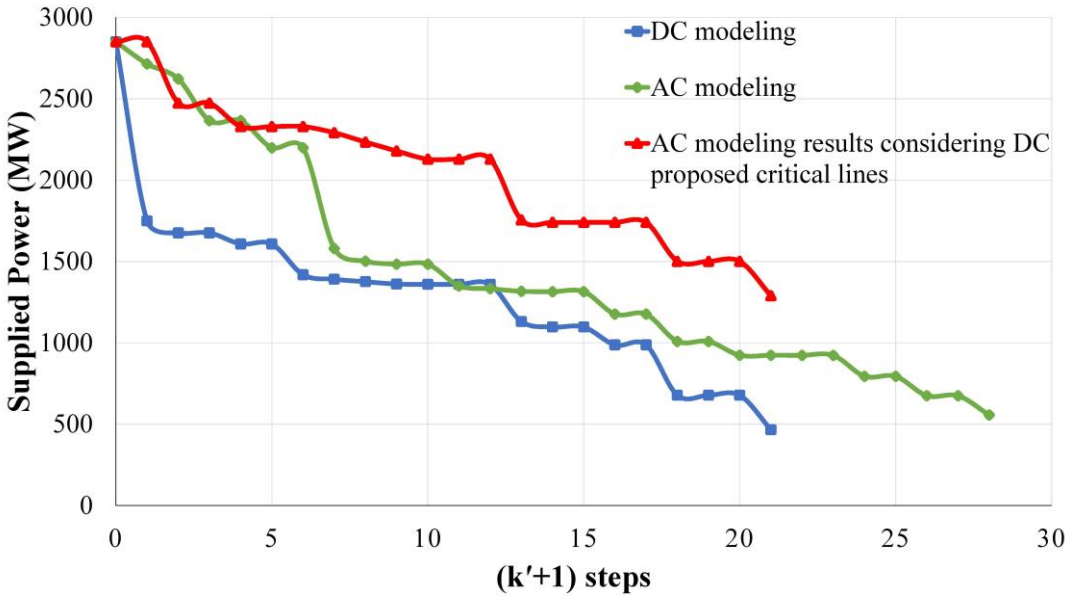

Figure 4-7. Supplied power of removing the critical lines in the N-k′-1 scenario.

failure process is introduced in Section 4-2. The final topology of the test system is depicted in Figure 4-6. It will be after 28 and 21 iterations in ACM and DCM, respectively. It should be noted that nodes 24 and 17 do not have any load or generation. Therefore, the simulation is stopped in these final topologies.

To find the effect of different line selection in the N-k′-1 scenario using both power flow models, the total supplied power is calculated in each (k′+1) steps. Figure 4-7 compares the supplied power in ACM and DCM. Indeed, the removed lines may differ between both approaches, as can be seen in Figure 4-6. The last simulation consists of selecting the proposed critical lines with DCM but modeling them by ACM. Therefore, it shows the actual impact of DCM on the supplied power.

The results of DCM are more pessimistic than of ACM. It contrasts with all the other assessments, where DCM was more optimistic [324]. Furthermore, Figure 4-8 presents the final topology of the proposed lines by DCM but calculated using ACM. One can see the difference compared to Figure 4-6. The main reason lies in the fact that some lines are overloaded with cascading failures during DCM. This means that they do not belong to the proposed lines that should be removed by ACM.

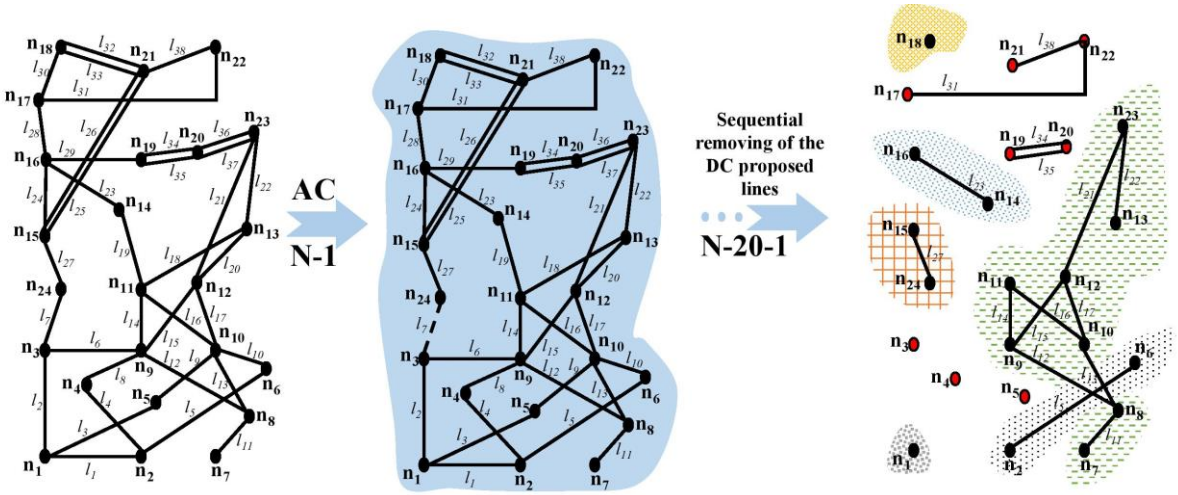

Figure 4-8. Final situation of IEEE RTS considering ACM with the proposed critical lines of DCM (the active zones are highlighted).

4-4-3 Reliability analysis

We tested two RTS topologies with the time-sequential Monte Carlo simulation approach. This simulation process stopped when the COV for EENS is less than 6% [336]. The result shows that 500-year period simulations lead to convergence for all reliability indices.

Table 4-1 reports the results and compares it with Billinton and Wangde [315]. The results reported by ACM based reliability indices diverge from the results of DCM by about 20% in all indices except the ADLC index. This last index consists of the division of the EDLC and EFLC, both underestimated in DCM. Therefore, the error in an index discards the error in the other one, which means that ADLC is irrelevant for comparing ACM and DCM.

To compare the reliability of various networks, we introduced RTS area 1&2 in Section 4-3. Table 4-1 shows that it is possible to use the results of DCM for comparing two or more different networks together. The modeling approach becomes more critical when investigating the reliability of the MRTS as a stressed network. According to Table 4-1, the reliability indices are underestimated by up to 20% for the RTS case and up to 91% for the MRTS case. These results confirm those obtained in Benidris and Mitra [328].

4-5 Sources of inaccuracy

This section examines the main reasons for the differences in both power flow models. We focus on the reliability indices, because of the similarity of reasons for the inaccuracy of results in different assessments. The following subsections are based on the inherent assumptions of DCM previously introduced.

Table 4-1. Annualized system indices for both case studies.

Reliability index	IEEE-RTS Area 1				IEEE-RTS Area 1&2			IEEE-MRTS Area 1		
	DCM Billinton and Wangde [315]	This work	ACM This work	Dif.+ (%)	DCM This work	ACM This work	Dif.+ (%)	DCM This work	ACM This work	Dif.+ (%)
EENS (MWh/year)	134590	130510	154040	-15	118910	144810	-18	92120	439230	-79
EDNS (MW)	15.4* (134590/8760)	14.9	17.6	-15	13.6	16.5	-18	10.5	50.1	-79
EFLC, LOLF (outages/year)	18.6	19.1	23.2	-18	26.3	30.9	-15	16.9	59.3	-72
EDLC, LOLE (hours/year)	740.2* (0.0845×8760)	744.7	940.5	-21	901.2	1042.2	-14	622.2	6707.5	-91
PLC, LOLP (%)	8.5	8.5	10.7	-21	10.0	11.9	-14	7.1	76.6	-91
ADLC, LOLD (hour/disturbance)	39.9* (740.2/18.6)	39.0	40.5	-4	34.2	33.7	+1	36.8	113.1	-67

* These are calculated using available data in reference [315]
+ Note that the results obtained by ACM is taken as the benchmark for comparisons (Dif. =Difference)

4-5-1 Reactive power and power losses

Reliability indices are calculated in two 100-year simulations to examine the main reasons for differences between ACM and DCM. Both use the same initial "seed" for the random number generator. The method includes a pseudo-random number generator that produces a string of pseudo-random numbers. The random numbers depend on the "seed" that is used to start the

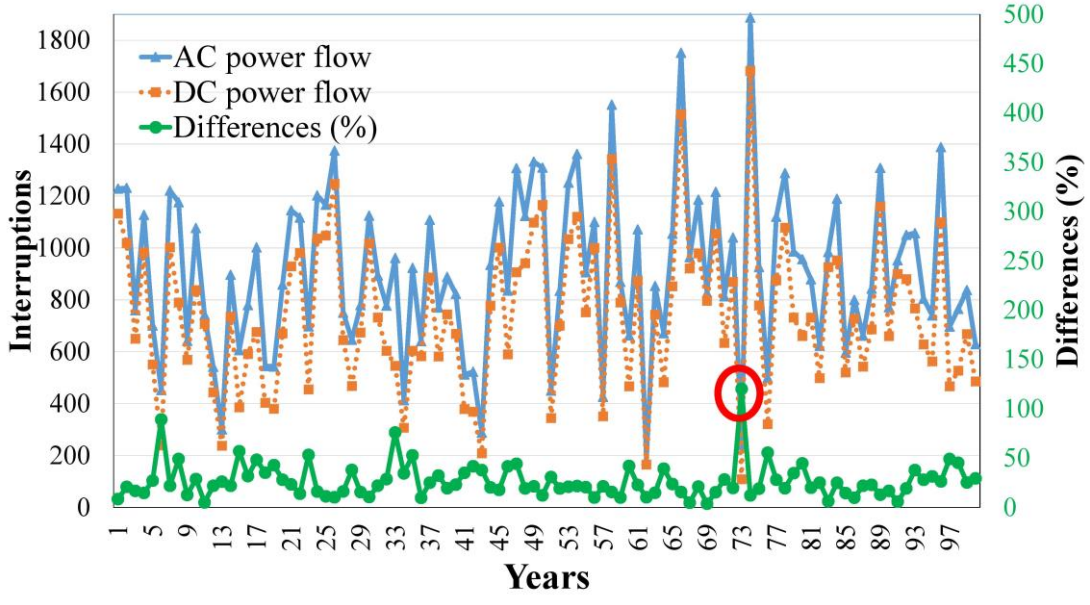

Figure 4-9. Interruptions using DCM and ACM for IEEE RTS.

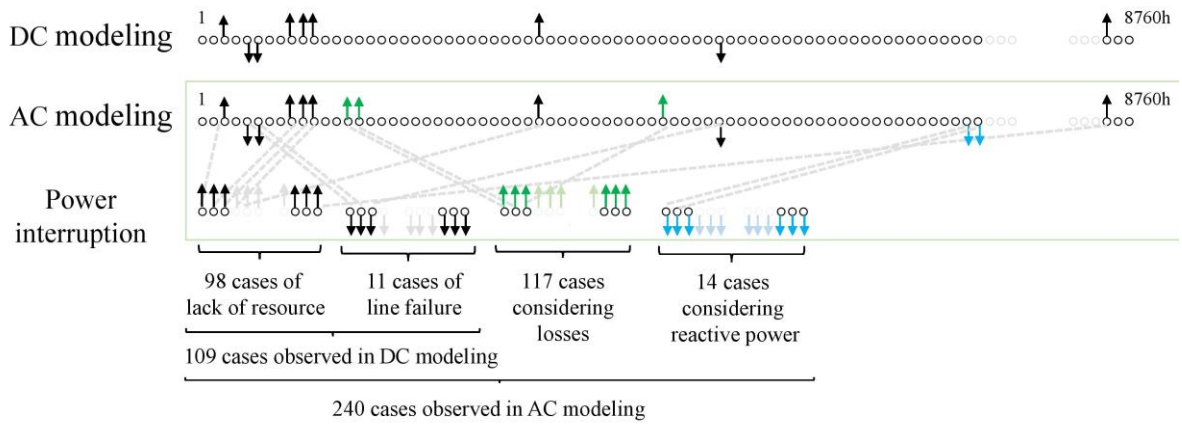

Figure 4-10. Interruptions of ACM and DCM for year 73 (8760 hours in total).

sequence. Hence, the seed is fixed to duplicate the results obtained in the example. Figure 4-9 compares the results of ACM and DCM for the RTS case. DCM always underestimates the number of interruptions. The error generally is below 50% in the RTS case with a mean error of 27%. The year 73 only observes a difference higher than 100%, as the number of interruption drops from 240 to 109.

The situation worsens with the MRTS case (not presented in Figure 4-9). DCM becomes completely inaccurate. The mean number of interruptions is 6655 in ACM, while only 570 in DCM. Again, year 73 records a large miscalculation from DCM. Therefore, we analyzed this specific year further to understand the main reasons.

In this year, ACM reports 240 interruptions, as shown in Figure 4-10. DCM only spots 109 of these interruptions. Analyzing the 131 remaining interruptions shows that in some hours, only losses cause that supplied power is less than the total load (interruption) and in some hours, considering reactive power flow leads to overloaded lines. The limits developed so far are based on apparent power (“MVA”) (refer to Section 4-2-1). The apparent power is the combination of active and reactive powers. So, considering reactive transfers between the lines decreases the limit of transferring active power. Hence, some lines will be overloaded only by considering reactive power flow. Accordingly, the losses and reactive power flow play an important role to cause the differences between the results.

4-5-2 Small-angle approximation

DCM uses small-angle approximation [324] for sine and cosine functions. It assumes that the phase angle difference between the buses is small enough and approximates the cosine and sine

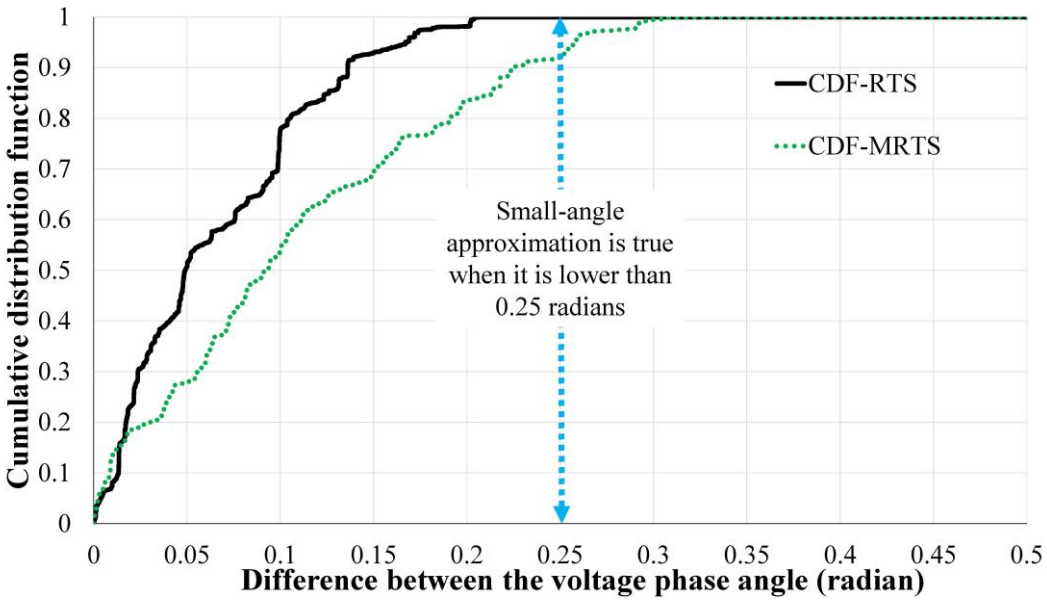

Figure 4-11. The absolute difference between the voltage phase angles, radian.

functions with $\sin(\theta_{ij}) \approx \theta_{ij}$ and $\cos(\theta_{ij}) \approx 1$, respectively. It is true as far as the angle is lower than 0.25 radians. Figure 4-11 provides the cumulative distribution functions (CDFs) for the absolute difference between the voltage phase angles of the 100-year simulations which are used to calculate reliability indices. This figure shows that RTS has no voltage phase angle difference larger than 0.25 radian, while MRTS observes it with about 8% of the nodes. This point contributes to understanding why DCM becomes less accurate with the MRTS case than the RTS.

4-5-3 Constant voltage magnitude

Finally, DCM ignores the variations of voltage magnitude and assumes 1 p.u for all nodes. In the previous sections, the default constraints of voltage in MATPOWER are used. It should be noted that it is not practically possible to freely relax voltage magnitude because of voltage stability. In this section, the goal is to investigate the impacts of voltage limits on reliability indices. So, we relax voltage up to 20% to figure out its effect. Table 4-2 presents the sensitivity of reliability indices to the relaxation of voltage limits. This table demonstrates the impact of relaxation on power flow results using ACM and hence, on reliability indices. This impact is very impressive in the stressed network (i.e., MRTS).

Table 4-2. Sensitivity of the reliability indices to relax voltage limits of IEEE RTS and MRTS.

Reliability index	Voltage limits of IEEE RTS (p.u.)				Voltage limits of IEEE MRTS (p.u.)			
	0.8-1.2	0.85-1.15	0.9-1.1	0.95-1.05	0.8-1.2	0.85-1.15	0.9-1.1	0.95-1.05
EENS*	0.97	0.97	0.99	1.00	0.32	0.34	0.37	1.00
EDNS*	0.97	0.97	0.99	1.00	0.32	0.34	0.37	1.00
EFLC, LOLF*	0.96	0.96	0.96	1.00	0.57	0.60	0.77	1.00
EDLC, LOLE*	0.99	0.99	0.99	1.00	0.20	0.20	0.25	1.00
PLC, LOLP*	0.99	0.99	0.99	1.00	0.20	0.20	0.25	1.00
ADLC, LOLD*	1.00	1.00	1.00	0.97	0.34	0.34	0.33	1.00

* The indices are relative number and calculated by dividing with the maximum magnitude for each index

4-6 Conclusion

In this chapter, we thoroughly investigate the effects of assumptions in DCM, especially when it is used for line capacity-based assessments such as reliability, vulnerability and contingency analyses. The reliability results show that the related indices are very sensitive to line capacity limits. Hence, DCM can lead to optimistic and inaccurate predictions in reliability. Furthermore, the assumptions' effects are very important in a more stressed network (i.e., IEEE MRTS), although it is possible to use the results of DCM for comparing two or more different networks. The results of contingency and vulnerability analyses show that DCM can lead to pessimistic predictions. Although the difference between line loadings is mostly very small in both models (approximately 3%), it leads to exceeding the line limit as well as cascading failures. In addition, in our test cases where reactive power flows predominate on some lines, such as cables (i.e., lines 6-10 and 1-2), overloads cannot be adequately shown only by the active power flows. Therefore, the results indicate that special care should be taken whenever DCM is used for the planning and operating of power systems.

Part Three

Multi-level optimization-based vulnerability analysis

This part has been published in:

Abedi, A., M.R. Hesamzadeh, and F. Romerio, *An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system.* International Journal of Electrical Power & Energy Systems, 2021. **125**: p. 106455.

Abedi, A. and F. Romerio, *Multi-period vulnerability analysis of power grids under multiple outages: An AC-based bilevel optimization approach.* International Journal of Critical Infrastructure Protection, 2020: p. 100365.

Abedi, A., M.R. Hesamzadeh, and F. Romerio, *Adaptive Robust Vulnerability Assessment of A Power System: A Trilevel OPF-based Optimization Approach* [Submitted].

Chapter 5

An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system

5-1 Introduction

A secure, competitive and decarbonized energy system is the main goal of the energy sector's decision-makers [320, 339]. The power network, which will undergo a major restructuring in the coming years, plays a key role as a critical infrastructure. Its security against various hazards and threats such as natural hazards (for example, high wind, flooding, or lightning), intentional attacks, and random failures [17] has become a growing concern. Deploying a robust and resilient power system improves security and accordingly, operators must detect the most vulnerable elements of their power system under a variety of attack scenarios. This vulnerability assessment helps them to design proper preventive and corrective schemes to reduce the vulnerability of their system to unpredictable events [33].

In the past, several innovative methods have been developed to determine critical components whose failures lead to the largest power-system loss [19]. These developed methods can range from analytical approaches (such as complex network, flow-based, logical, and functional methods) to Monte Carlo simulations. A detailed comparison of these methods and approaches

is recently conducted in [20]. Among these methods, optimization-based modeling has been shown to be successful and received attention in the relevant literature. The application of optimization techniques to the power-system vulnerability assessment is growing mainly due to the advancements in high-speed multiprocessors with large memory. The optimization models of the vulnerability assessment can be implemented using high-speed multiprocessors for realistic power systems as reported in [340].

The multilevel optimization framework has been used in [8] to model power system interdiction [341]. A multilevel optimization is a mathematical program where an optimization problem contains another optimization problem as a constraint [342]. These optimization problems are closely related to the hierarchical leader-follower or Stackelberg games [343]. Accordingly, the power-system vulnerability assessment can be modeled as a leader-follower game where the leader (or attacker) maximizes the damage to the system and the follower (or defender) responds to the action of the leader by minimizing the damage consequences for the power system [344, 345].

The relevant literature has focused on (a) attacker-defender (AD) [18, 341, 346-351] and (b) defender-attacker-defender (DAD) [352-358] models to improve the robustness of power systems exposed to natural hazards or intentional attacks. Salmerón et al. formulate an AD model [341] and apply the idea of global Benders decomposition [349] for interdiction problems in power systems. The Karush-Kuhn-Tucker (KKT) optimality conditions [346] and duality theory [347] are used to convert an AD model to a one-level problem. Arroyo [348] compares the KKT- and duality-based approaches by introducing minimum and maximum vulnerability models. A multi-start Benders decomposition technique is used to solve an AD model considering transmission line switching as a corrective action by the system operator (or defender) [350]. Yuan et al. formulate a DAD model and implement a Column-and-Constraint Generation (C&CG) algorithm to solve it [357]. Then, Yuan and Zeng [358] introduce the transmission line switching as a corrective action to reduce the attack consequences in a trilevel optimization model and solve it using the nested column-and-constraint generation (NC&CG) algorithm. Recently, Fang et al. [19] propose the AD model to assess the vulnerability of power systems exposed to natural hazards and then, develop a trilevel optimization model for improving the resilience of interdependent infrastructures under natural hazards using an adaptive robust framework [355]. Sayed et al. [356] use a trilevel optimization model and the NC&CG algorithm to assess vulnerability in the integrated electric-gas system (IEGS). The

metaheuristic techniques such as the genetic algorithm are also implemented to solve the AD problem [18, 351].

The above literature employs the DC optimal power flow (DCOPF) in the lower-level problem as the operator's (defender's) tool to mitigate the attack's adverse consequences. The DCOPF model has some drawbacks. Technically, it cannot provide correct information on a power system since it ignores reactive power, resistance, and losses, and it assumes a perfect voltage regulation at each bus (voltage magnitudes are fixed to 1 per unit). The DCOPF assumptions make the AD model solution less accurate and attractive [359], especially where the reactive power flows are of concern in the congested power systems [23]. The authors in [360] first used the AC power flow equations and they assumed that attackers are allowed to increase the impedance of transmission lines in the model. The topology of the power system does not change in their AD model and accordingly their model cannot predict the harmful consequences of the topology change following an attack. Furthermore, another drawback of the model is using a solver for evaluating the ACOPF in the lower level which cannot guarantee to find the global solution.

In this chapter, the main aim is to propose a new model for vulnerability analysis of a power system by employing the AC power flow equations. In doing so, the AC optimal power flow (ACOPF) is used in the lower-level defender problem which is a non-linear and non-convex optimization problem [340]. Considering the ACOPF in the lower-level defender problem converts the whole problem to a mixed-integer bilevel nonlinear program (MIBNLP) that is non-convex and NP-hard [361].

To solve the proposed MIBNLP model, we first develop a Linear Program (LP) approximation of the non-convex ACOPF model of the defender problem. The LP model is derived following some technically sound assumptions for well-designed transmission networks and a series of linearization techniques. The LP approximation of the ACOPF provides more accurate modeling of the power system as compared to the DCOPF and accordingly makes the results of our proposed AD model more practical and useful for system operators. Also, our approximation model is a convex LP which can be solved efficiently using state-of-the-art solvers such as Cplex solver.

Employing our LP model of ACOPF, the bilevel AD model is now a mixed-integer bilevel linear program (MIBLP). To solve the MIBLP model, we first take advantage of the LP model of the lower-level defender model. We replace the LP model by its dual program using the

duality theory. By replacing the LP by its dual program, the MIBLP is converted to a single-level mixed-integer nonlinear program (MINLP). The nonlinear terms in the MINLP model are then linearized using the Big-M technique [362]. This gives us the final mixed-integer linear program (MILP) which can be solved efficiently using state-of-the-art solvers such as the Cplex. Accordingly, the contributions of our work are as follows:

1. We first propose an LP for ACOPF where the technical details of AC networks such as resistance, reactance, shunt susceptance, active and reactive power are properly modeled. Due to AC power flow details in the LP model, our results are more practical and useful for the system operators as compared to the models where the naïve DCOPF approximation is used.
2. Our proposed bilevel optimization model for the AD game is converted to an easier-to-solve one-level MILP model. Our MILP model can be solved efficiently using state-of-the-art solvers such as Cplex to the desired precision level. Furthermore, the system operator by adding more linear terms can improve the accuracy of our proposed MILP model.

The remainder of this chapter is organized as follows. Section 5-2 introduces the attacker-defender ACOPF-based mixed-integer bilevel nonlinear program including the assumptions and formulations. Section 5-3 proposes the linearization approaches and the final transformation to a single-level MILP. Section 5-4 presents the numerical results by applying our proposed MILP to different case studies and comparing our results with some benchmark models. Finally, concluding remarks are provided in Section 5-5.

5-2 The attacker-defender mixed-integer bilevel nonlinear program (MIBNLP)

In this Section, the mathematical formulation of the ACOPF-based attacker-defender problem, also known as the interdiction model, is presented. This formulation is based on the following assumptions that are commonly used in the literature for vulnerability assessment of a power system [346-348, 352-354]:

1. The rational attacker has the intention to maximize the damage and disable multiple assets simultaneously and permanently or at least for several hours. As a result, if the attack is achieved, the power flow of other lines will be also affected.
2. We assume that the targeting assets are transmission lines and transformers, as they are usually reachable. For instance, transmission lines are out of the substation fences with low or no security to withstand. By removing the attacked transmission lines and their connected transformers, all loads which are only supplied by the attacked lines will be out of service.

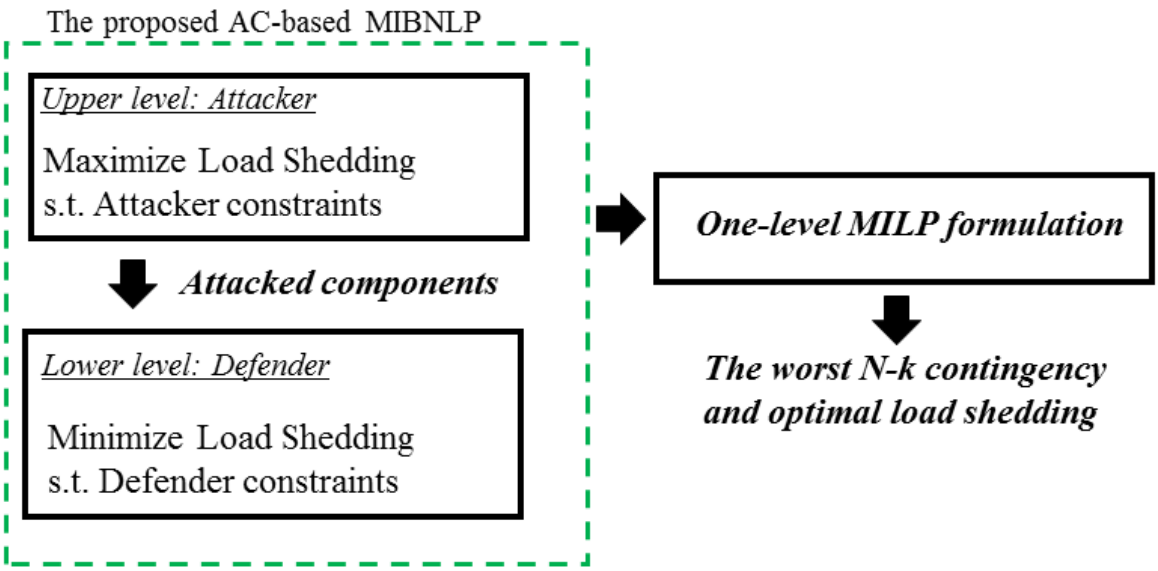

Figure 5-1. The attacker-defender model used in the current Chapter.

3. Because two parallel circuits between the buses are usually on the same tower, they are modeled as a single line with double capacity.
4. Our proposed MILP models the steady-state security constraints following the attack. Accordingly, the dynamic behavior of the power system from the time of attack to the steady-state situation is not considered (assuming the power system can withstand the dynamic changes). Modeling the dynamic response of the power system following the attack adds an extra level of complexity to our model and it is not within the scope of this chapter. However, this dynamic simulation is a good extension of our work.
5. In this chapter, the system damage is measured by the level of load shedding which is the amount of load that cannot be supplied due to the physical constraints of the power system. However, different objective functions of interest can be used in our MILP model to measure the system damage following an attack.

The attacker-defender model used in this chapter is illustrated in Figure 5-1.

As in Figure 5-1, the upper level models the attacker, and the lower level models the defender. The attacker as the leader starts the leader-follower game with limited disruptive resources. The defender as the follower reacts against the set of out-of-service assets to mitigate its adverse consequences. This leader-follower interaction between the attacker and the defender is modeled as the bilevel optimization problem (5-1)-(5-15). Dual variables associated with the constraints of the lower-level problem are shown inside parentheses.

$$\underset{Z}{Max} \sum_{i\in N} Ls_i^* \tag{5-1}$$

s.t. $$0.5\times \sum_{i,j\in N} (1-z_{ij}) = NPO; \quad z_{ij} \in \{0,1\} \quad \forall i, j \in N \tag{5-2}$$

$$z_{ij} = z_{ji}; \quad z_{ij} \in \{0,1\} \quad \forall i, j \in N \tag{5-3}$$

where: $$\sum_{i\in N} Ls_i^* \in \arg\left\{ \underset{\substack{Pg,Qg,Ls,Lsq,\\ P,Q,V,\theta}}{Min} \sum_{i\in N} Ls_i \right\} \tag{5-4}$$

s.t. $$Pg_{i|i\in G} + Ls_{i|i\in D} - Pd_{i|i\in D} = \sum_{j\in N} P_{ij}; \quad \forall i, j \in N : (\alpha_i) \tag{5-5}$$

$$Qg_{i|i\in G} + Lsq_{i|i\in D} - Qd_{i|i\in D} = \sum_{j\in N} Q_{ij}; \quad \forall i, j \in N : (\beta_i) \tag{5-6}$$

$$P_{ij} = z_{ij}\left(V_i^2 G_{ij} - V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij})\right); \quad \forall i, j \in N : (\lambda_{ij}) \tag{5-7}$$

$$Q_{ij} = z_{ij}\left(-V_i^2 (B_{ij} + \frac{B_{ij}^{sh}}{2}) - V_i V_j (G_{ij}\sin\theta_{ij} - B_{ij}\cos\theta_{ij})\right); \quad \forall i, j \in N : (\mu_{ij}) \tag{5-8}$$

$$0 \le Pg_i \le Pg_i^{\max}; \quad \forall i \in G : (\overline{\delta}_i) \tag{5-9}$$

$$Qg_i^{\min} \le Qg_i \le Qg_i^{\max}; \quad \forall i \in G : (\underline{\sigma}_i, \overline{\sigma}_i) \tag{5-10}$$

$$\left(P_{ij}\right)^2 + \left(Q_{ij}\right)^2 \le \left(S_{ij}^{\max}\right)^2; \quad \forall i, j \in N \tag{5-11}$$

$$V_i^{\min} \le V_i \le V_i^{\max}; \quad \forall i \in N : (\underline{\upsilon}_i, \overline{\upsilon}_i) \tag{5-12}$$

$$\theta_{ij}^{\min} \le \theta_{ij} \le \theta_{ij}^{\max}; \quad \forall i, j \in N \tag{5-13}$$

$$0 \le Ls_i \le Pd_i; \quad \forall i \in D : (\overline{\omega}_i) \tag{5-14}$$

$$Lsq_i = Ls_i \tan\phi_i; \quad \forall i \in D \tag{5-15}$$

The optimization problem (5-1)-(5-15) is a mixed-integer bilevel nonlinear program (MIBNLP) which is non-convex and NP-hard. Equations (5-1)-(5-3) model the attacker optimization problem which maximizes the load shedding subject to the limited number of plausible outages considered in constraint (5-2). Since $z_{ij} = z_{ji}$, the factor 0.5 is multiplied by the total number of line outages to avoid double consideration in our formulation. If z_{ij} is 0, the line *ij* is under attack, otherwise it is safe. In the lower-level defender problem (5-4)-(5-15), unlike the previous approaches [346-348, 352-354], the ACOPF is used as the defender tool to mitigate the adverse consequences of the outages. Equation (5-4) is the objective function of the defender to minimize the damage. The asterisk in (5-1) and (5-4) emphasizes that Ls_i is decided in the

lower-level problem. Equations (5-5) and (5-6) are the nodal power balance equations for active and reactive powers, respectively. Equations (5-7) and (5-8) represent the line flows of active and reactive powers, respectively. Constraints (5-9)-(5-11) enforce the limits of active and reactive power generations and transmission line capacity, respectively. Voltage magnitude and voltage angle are limited using (5-12) and (5-13), respectively. Furthermore, active load shedding is limited to maximum active load at each bus in (5-14) and load shedding assumes constant power factor at load buses using (5-15). To solve our proposed MIBNLP model (5-1) -(5-15), in the next Section we transform the MIBNLP to a mixed-integer linear program (MILP) which is computationally more tractable than the original MIBNLP. We then solve our proposed MILP model using the off-the-shelf Cplex solver.

5-3 Solution methodology

In this Section, the proposed MIBNLP in the previous Section is transformed to a single-level MILP in two steps: First, the lower-level ACOPF model is approximated by an LP; then the whole bilevel model is transformed to a single-level MILP using the duality theory and several proposed linearization techniques.

5-3-1 Linearizing lower-level ACOPF model

We assume the phase differences between the bus voltages are small enough and the voltage magnitude is close to 1 p.u. for all buses. These assumptions are practically acceptable under the normal steady-state operating condition of a power system to maintain the system far from instability [340]. Based on these assumptions, we can use the first-order approximation of Taylor's series with respect to the variables $\{V_i, V_j, c_{ij}, n_{ij}\}$ for nonlinear terms of (5-7)-(5-8) (z_{ij} is the upper-level decision variable and considered as a given parameter in the lower-level problem). These first-order approximations are derived in (5-16) and (5-17) below:

$$P_{ij} = z_{ij}\left(G_{ij}\left(2V_i - 1\right) - G_{ij}\left(V_i + V_j + c_{ij} - 2\right) - B_{ij}n_{ij}\right) \tag{5-16}$$

$$Q_{ij} = z_{ij}\left(-(B_{ij} + \frac{B_{ij}^{sh}}{2})\left(2V_i - 1\right) + B_{ij}\left(V_i + V_j + c_{ij} - 2\right) - G_{ij}n_{ij}\right) \tag{5-17}$$

where, $c_{ij} = \cos\theta_{ij} \approx 1 - \frac{(\theta_i - \theta_j)^2}{2}$, and $n_{ij} = \sin\theta_{ij} \approx \theta_i - \theta_j$. Then, the quadratic function can be linearized based on the proposed method in [363] by using 2*M* piecewise linear (PWL) blocks as expressed below:

$$c_{ij} \approx 1-\frac{(\theta_i-\theta_j)^2}{2}=1-\frac{\sum_{m=1}^{M}((2m-1)\Delta\theta_{ij})\theta_{ijm}}{2};\quad m=1\cdots M,\forall i,j\in N:(\chi_{ij}) \tag{5-18}$$

$$\left|\theta_i-\theta_j\right|=\sum_{m=1}^{M}\theta_{ijm}=\delta_{ij}^{+}+\delta_{ij}^{-};\quad m=1\cdots M,\forall i,j\in N:(\varphi_{ij}) \tag{5-19}$$

$$n_{ij}\approx\theta_i-\theta_j=\delta_{ij}^{+}-\delta_{ij}^{-};\quad \forall i,j\in N:(\xi_{ij}) \tag{5-20}$$

$$0\le\theta_{ijm}\le\Delta\theta_{ij};\quad m=1\cdots M,\forall i,j\in N:(o_{ijm}) \tag{5-21}$$

$$\theta_{ijm}=\theta_{jim};\quad m=1\cdots M,\forall i,j\in N:(\kappa_{ijm}) \tag{5-22}$$

$$n_{ij}=-n_{ji};\quad \forall i,j\in N:(\varepsilon_{ij}) \tag{5-23}$$

where $(2m-1)\Delta\theta_{ij}$ and θ_{ijm} are the slope and the value of m^{th} block of the voltage phase difference of transmission line ij (see Figure 5-2 for its illustration). The appropriate value for $\Delta\theta_{ij}$ can be 2π divided by $2M$. The absolute function in (5-19) is linearized by introducing two positive variables δ_{ij}^{+} and δ_{ij}^{-}. Note that this linearization technique for the quadratic function does not need any binary variables given small voltage angles [363] which makes it much more tractable as compared to linearization techniques which use either binary variables in their formulations [364], or the special ordered set of type 2 (SOS2) [365]. Nevertheless, our piece-

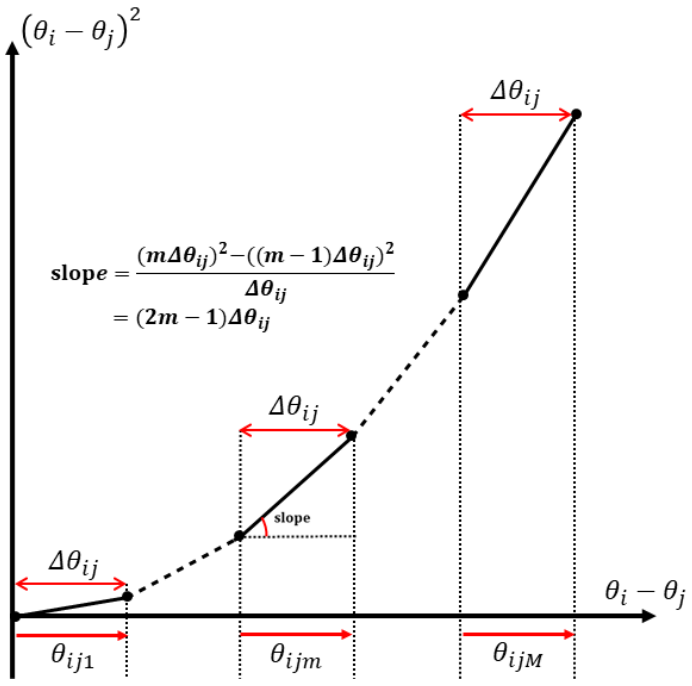

Figure 5-2. The piecewise linear approximation of a nonlinear function.

wise linear approximation adds three sets of continuous variables to the problem (*M* piecewise linearization blocks plus 2 auxiliary variables (δ_{ij}^{+} and δ_{ij}^{-}) for each line).

The nonlinear constraint (5-11) presents a circle with the radius of $S_{ij}^{\max}$. This circle is linearized by an *n*-sided convex regular polygon using following *n* equations [366]:

$$\left(\sin\left(\frac{2\pi k}{n}\right)-\sin\left(\frac{2\pi(k-1)}{n}\right)\right)P_{ij}-\left(\cos\left(\frac{2\pi k}{n}\right)-\cos\left(\frac{2\pi(k-1)}{n}\right)\right)Q_{ij} \\ -S_{ij}^{\max}\sin\left(\frac{2\pi}{n}\right)\le 0;\quad k=1\cdots n,\forall i,j\in N:(\eta_{k,ij}) \tag{5-24}$$

Linearizing the constraint (5-11) as suggested above, adds *n* constraints for each line. A small *n* enforces more restrictions on transmission line capacity and might lead to the problem infeasibility while a large *n* increases the number of equations and accordingly the computational burden. Hence, the appropriate value for *n* should be carefully decided. We set it at *n* = 64 following the recommendations in [340, 365]. At this stage, the initial MIBNLP model is formulated as a mixed-integer bilevel linear program (MIBLP). This MIBLP is transformed into a single-level MILP in the next Section using duality theory.

5-3-2 Transforming MIBLP to an equivalent single-level MILP model

In this step, the proposed MIBLP in the previous subsection is transformed to a single-level MILP using the duality theory for linear programs. First, the lower-level minimization problem is replaced by its dual optimization problem. This converts the Max-Min optimization model to a Max-Max optimization model. Then, this Max-Max optimization model is reformulated as the following MILP maximization problem set out in (5-25)-(5-38).

$$\underset{\substack{z_{ij},\underline{\lambda}_{ij},\underline{\mu}_{ij},\underline{\alpha}_i,\underline{\omega}_i,\\ \underline{\beta}_i,\underline{\delta}_i,\underline{\sigma}_i,\underline{\upsilon}_i,\underline{\xi}_{ij},\\ \underline{\upsilon}_i,\eta_{1,ij}\cdots\eta_{n,ij},\chi_{ij},\\ o_{ijm},\varphi_{ij},\kappa_{ijm},\varepsilon_{ij}}}{Max}\left(\begin{array}{l}\sum_{i,j\in N}z_{ij}\lambda_{ij}G_{ij}+\sum_{i,j\in N}z_{ij}\mu_{ij}(\frac{B_{ij}^{sh}}{2}-B_{ij})+\sum_{i\in N}(\alpha_i+\overline{\omega}_i)Pd_{i|i\in D}+\sum_{i\in N}\beta_i Qd_{i|i\in D}\\ +\sum_{i\in G}\overline{\delta}_i Pg_i^{\max}+\sum_{i\in G}\overline{\sigma}_i Qg_i^{\max}+\sum_{i\in G}\underline{\sigma}_i Qg_i^{\min}+\sum_{i\in N}\overline{\upsilon}_i V_i^{\max}+\sum_{i\in N}\underline{\upsilon}_i V_i^{\min}\\ +\sum_{i,j\in N}S_{ij}^{\max}\sin\left(\frac{2\pi}{n}\right)(\eta_{1,ij}+\cdots+\eta_{n,ij})+\sum_{i,j\in N}\chi_{ij}+\sum_{i,j\in N}\sum_{m=1}^{M}o_{ijm}\Delta\theta_{ij}\end{array}\right) \tag{5-25}$$

$$\text{s.t.}\quad 0.5\times\sum_{i,j\in N}(1-z_{ij})=NPO;\quad z_{ij}\in\{0,1\}\quad\forall i,j\in N \tag{5-26}$$

$$z_{ij}=z_{ji};\quad z_{ij}\in\{0,1\}\quad\forall i,j\in N \tag{5-27}$$

$$\lambda_{ij} - \alpha_i + \sum_{k=1}^{n} \eta_{k,ij} \left(\sin\left(\frac{2\pi k}{n} \right) - \sin\left(\frac{2\pi (k-1)}{n} \right) \right) = 0 : (P_{ij}) \tag{5-28}$$

$$\mu_{ij} - \beta_i - \sum_{k=1}^{n} \eta_{k,ij} \left(\cos\left(\frac{2\pi k}{n} \right) - \cos\left(\frac{2\pi (k-1)}{n} \right) \right) = 0 : (Q_{ij}) \tag{5-29}$$

$$\begin{aligned} &- \sum_{\substack{i,j \in N \\ |S(ij)=i}} z_{ij} \lambda_{ij} G_{ij} + \sum_{\substack{i,j \in N \\ |R(ij)=i}} z_{ij} \lambda_{ij} G_{ij} + \sum_{\substack{i,j \in N \\ |S(ij)=i}} z_{ij} \mu_{ij} (B_{ij} + B_{ij}^{sh}) \\ &- \sum_{\substack{i,j \in N \\ |R(ij)=i}} z_{ij} \mu_{ij} (B_{ij} + B_{ij}^{sh}) + \bar{\upsilon}_i + \underline{\upsilon}_i = 0 : (V_i) \end{aligned} \tag{5-30}$$

$$z_{ij} \lambda_{ij} G_{ij} - z_{ij} \mu_{ij} B_{ij} + \chi_{ij} = 0 : (c_{ij}) \tag{5-31}$$

$$z_{ij} \lambda_{ij} B_{ij} + z_{ij} \mu_{ij} G_{ij} + \xi_{ij} + \varepsilon_{ij} + \varepsilon_{ji} = 0 : (n_{ij}) \tag{5-32}$$

$$\alpha_i + \bar{\delta}_i \le 0 : (Pg_{i|i \in G}) \tag{5-33}$$

$$\beta_i + \bar{\sigma}_i + \underline{\sigma}_i = 0 : (Qg_{i|i \in G}) \tag{5-34}$$

$$+\varphi_{ij} - \xi_{ij} \le 0 : (\delta_{ij}^{+}) \tag{5-35}$$

$$\varphi_{ij} + \xi_{ij} \le 0 : (\delta_{ij}^{-}) \tag{5-36}$$

$$\chi_{ij} (0.5(2m-1)\Delta\theta_{ij}) - \varphi_{ij} + o_{ijm} + \kappa_{ijm} - \kappa_{jim} \le 0 : (\theta_{ijm}) \tag{5-37}$$

$$\alpha_i + \beta_i \tan\phi + \bar{\omega}_i \le 1 : (Ls_{i|i \in D}) \tag{5-38}$$

Where the primal variables associated with the different constraints of the dual optimization problem are shown in parentheses. This transformation introduces a new nonlinearity in the model, which is the product of binary and continuous dual variables ($z_{ij}\lambda_{ij}$ and $z_{ij}\mu_{ij}$) in (5-25), (5-30)-(5-32). This product can be linearized using two auxiliary variables T_{ij} and H_{ij} [353, 367, 368]. For instance, $T_{ij} = z_{ij}\lambda_{ij}$ can be linearized as follows:

$$\begin{aligned} &T_{ij} = \lambda_{ij} - H_{ij} \\ &-Bz_{ij} \le T_{ij} \le Bz_{ij} \\ &-B(1 - z_{ij}) \le H_{ij} \le B(1 - z_{ij}) \end{aligned} \tag{5-39}$$

Where, B is a suitable large constant. The final proposed MILP model can be solved using the high performance, efficient, and reliable off-the-shelf solvers such as Cplex [369]. These solvers can efficiently solve our MILP model to the desired level of accuracy. They can also provide the certificate of optimality of the solution. This is while the original MIBNLP model is an NP-hard optimization problem with no guarantee of finding the global solution [340].

5-4 Numerical result

The proposed model has been successfully applied to three different power systems; IEEE 24-bus reliability test systems (RTS) [240], IEEE 57-bus [370] and Iran's 400-kV network [371]. In all numerical studies, the minimum and maximum of the voltage magnitude of buses are assumed to be 0.95 and 1.05 p.u., respectively. The problems are solved on a laptop running with an Intel Core i7, 2.2 GHz processor, and 8 GB RAM. The Cplex solver in the GAMS (General Algebraic Modeling System) platform is used to solve our proposed MILP model [372]. Furthermore, the ACOPF function of MATPOWER in MATLAB environment [313] is also used for comparing the results. Table 5-1 reports statistics regarding the size and complexity of the examined cases in this chapter.

Table 5-1. The size and complexity of the examined cases measured by the number of equations, variables and the simulation time

Model statistics	**IEEE 24-bus**		**IEEE 57-bus**		**Iranian 400-kV network (AC-based)**	
	DCOPF-based	ACOPF-based	DCOPF-based	ACOPF-based	Existing network	Candidate network
Blocks of equations	12	24	12	24	24	24
Blocks of variables	12	86	12	86	86	86
Nonzero elements	1993	49266	4476	112697	105825	143281
Single equations	533	6667	1200	15247	14316	19364
Single variables	512	16136	1157	36952	34635	46871
Binary variables	68	68	156	156	146	198
Average elapsed time/simulation (min)	<1	~3	~4	~25	~27	~40

5-4-1 IEEE 24-bus reliability test systems (RTS)

In this subsection, the proposed ACOPF-based MILP model is applied to the IEEE 24-bus network. This case study has 24 buses, 32 generators, and 38 branches and transformers as shown in Figure 5-3. Detailed data of the IEEE RTS can be found in [240]. Before proceeding to solve the proposed MILP model for the IEEE RTS network, the accuracy of the linearized ACOPF model in this chapter and its dual optimization problem is investigated. In doing so, the exact nonlinear ACOPF is solved using MATPOWER package and the results are compared with those obtained from our proposed linearized ACOPF model. The objective function for

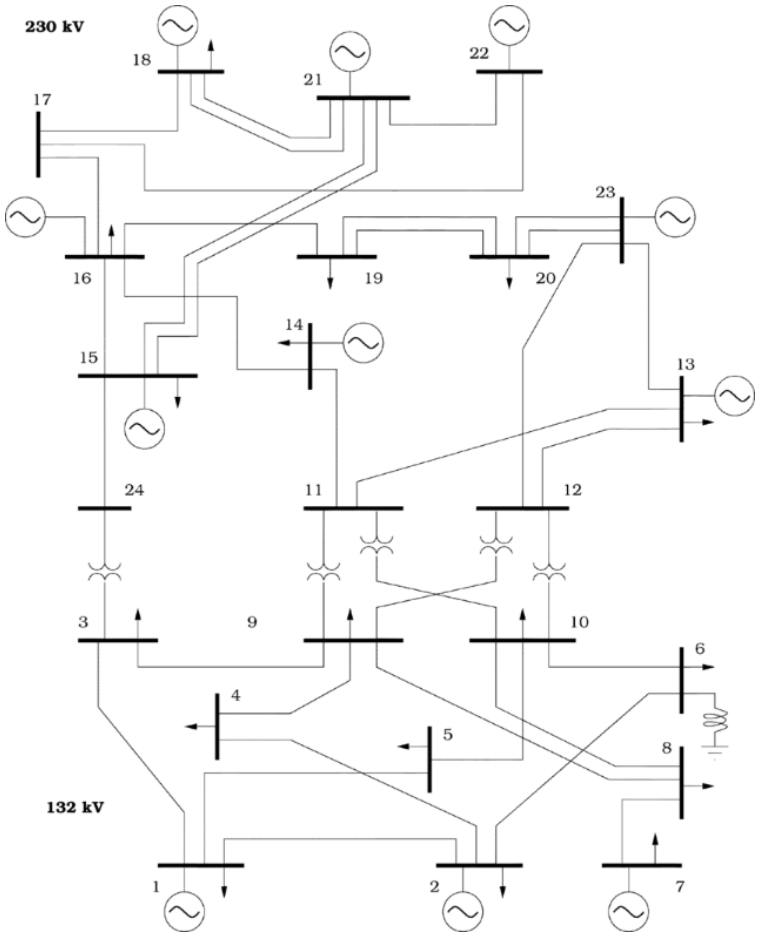

Figure 5-3. The single-line diagram of the IEEE RTS 24-bus system.

this comparison is chosen to be the total operation cost of the generators ($/h) in the form of $\sum_{i \in G} C_i Pg_i$, where C_i is cost coefficients of generators [313].

For the exact ACOPF and DCOPF models solved using MATPOWER package, the objective functions are 44196 $/h and 41904 $/h, respectively, whereas the objective function is found to be 44483 $/h using our linearized ACOPF model. The results show an error of 5.2% as compared to the DCOPF model and a small error of 0.6% as compared to the exact ACOPF. Furthermore, the objective function is found to be 44483 $/h using the dual optimization problem of the linearized ACOPF model (illustrating the strong-duality property of the LP model) [367].

The proposed one-level MILP problem is applied to the IEEE RTS. Figure 5-4 shows the load shedding of the IEEE 24-bus system as a function of NPO (interdiction resources). As can be seen in this figure, the optimal solutions or total load sheddings are approximately the same in some cases. However, Table 5-2 shows small differences in some NPOs, which in turn lead to

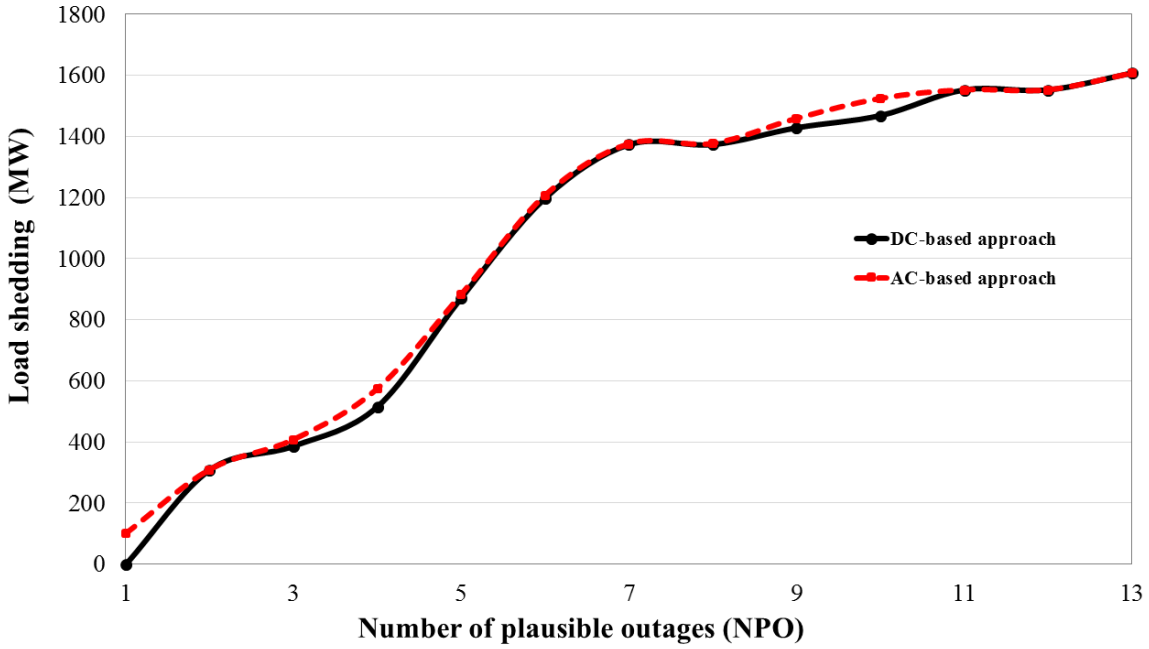

Figure 5-4. The optimal load shedding for IEEE 24-bus system as a function of number of plausible outages (NPO).

proposing different critical lines. For instance, when NPO is 3, our proposed ACOPF-based approach and the previously reported approach [346-348, 352-354] find similar critical lines (i.e. 7-8). This is while our approach and the DCOPF-based approach propose different lines (16-19, 20-23) and (15-21, 16-17), respectively as the 2nd and 3rd critical lines. In other words, the Jaccard Similarity Index (JSI) for these two sets of lines is 0.2 and the average JSI is 0.52 for this test case.

We have compared the results of our ACOPF-based model (reported in columns 6 and 7 of Table 5-2) with the ones from the DCOPF-based model used in [346, 348] (reported in columns 2 and 3 of Table 5-2). For those cases where we could not find the DCOPF-based results from the existing literature (indicated by n/a in Table 5-2) we have used the results from our own DCOPF-based model (reported in columns 4 and 5 of Table 5-2).

Using our proposed approach the calculated load shedding is more accurate as compared to the one from the DCOPF model. Based on the simulation results for the IEEE 24-bus system, the potential critical lines are radial lines (e.g. 7-8), parallel lines (e.g. 15-21, 20-23), and the lines connecting the generation to demand zones (e.g. 11-13, 12-13). It should be noted that when all lines are out of service, the system operator is forced to shed 1607 MW which is 56% of total demand [348]. The remaining loads are directly connected to the generators' buses. Our proposed MILP model shows that this total possible system load is shed with only 13

simultaneous outages. In the next sections, a larger network and a real power network are studied.

Table 5-2. The six worst-case load shedding scenarios and their related lines for the IEEE 24-bus system

NPO	DCOPF-based approach used in [346, 348]*		Our DCOPF-based approach***		Proposed ACOPF-based approach		
	Critical lines	LS (MW)	Critical lines	LS (MW)	Critical lines	LS (MW)	JSI
1	n/a	n/a	-	0	7-8	99	0
2	16-19, 20-23**	309	16-19, 20-23	309	16-19, 20-23	309	1
3	n/a	n/a	7-8, 15-21, 16-17	387	7-8, 16-19, 20-23	407	0.2
4	3-24, 12-23, 13-23, 14-16	516	3-24, 12-23, 13-23, 14-16	516	7-8, 15-21, 16-17, 20-23	574	0
5	n/a	n/a	12-23, 13-23, 15-21, 16-17, 20-23	872	12-23, 13-23, 15-21, 16-17, 20-23	883	1
6	11-13, 12-13, 12-23, 15-21**, 16-17, 20-23**	1198	11-13, 12-13, 12-23, 15-21, 16-17, 20-23	1198	1-5, 11-13, 15-21, 15-24, 16-17, 20-23	1207	0.5

*This approach is also used with different objective functions and case studies in [347, 352-354].

** Two parallel circuits are considered as two independent lines in [346, 348].

*** Our DCOPF-based model for cases where we do not have the benchmark results from the existing literature (see rows 1, 3 and 5).

5-4-2 The IEEE 57-bus system

The second test system is IEEE 57-bus example that has 57 buses, 7 generators, and 80 branches and transformers as shown in Figure 5-5. In this case, when all lines are out of service, the system operator is forced to shed 449.8 MW and 509.2 MW with DCOPF-based and our ACOPF-based approaches, respectively. This difference stems from considering constant power factor at load buses modeled in constraint (5-15). For instance, the total reactive load is less than the total capacity of reactive power of generators in buses 2 and 9. Hence, it causes more total active load shedding in these buses. Furthermore, the results show that this total possible system load is shed with only 14 and 13 simultaneous outages using DCOPF-based and our ACOPF-based approaches, respectively. Figure 5-5 also shows five worst-case load shedding and their related lines based on the proposed MILP problem. Moreover, these results are compared with the previous DCOPF-based approaches in Table 5-3. Figure 5-6 shows that the objective function (i.e. *LS*) reported based on the previous methods is lower than the one

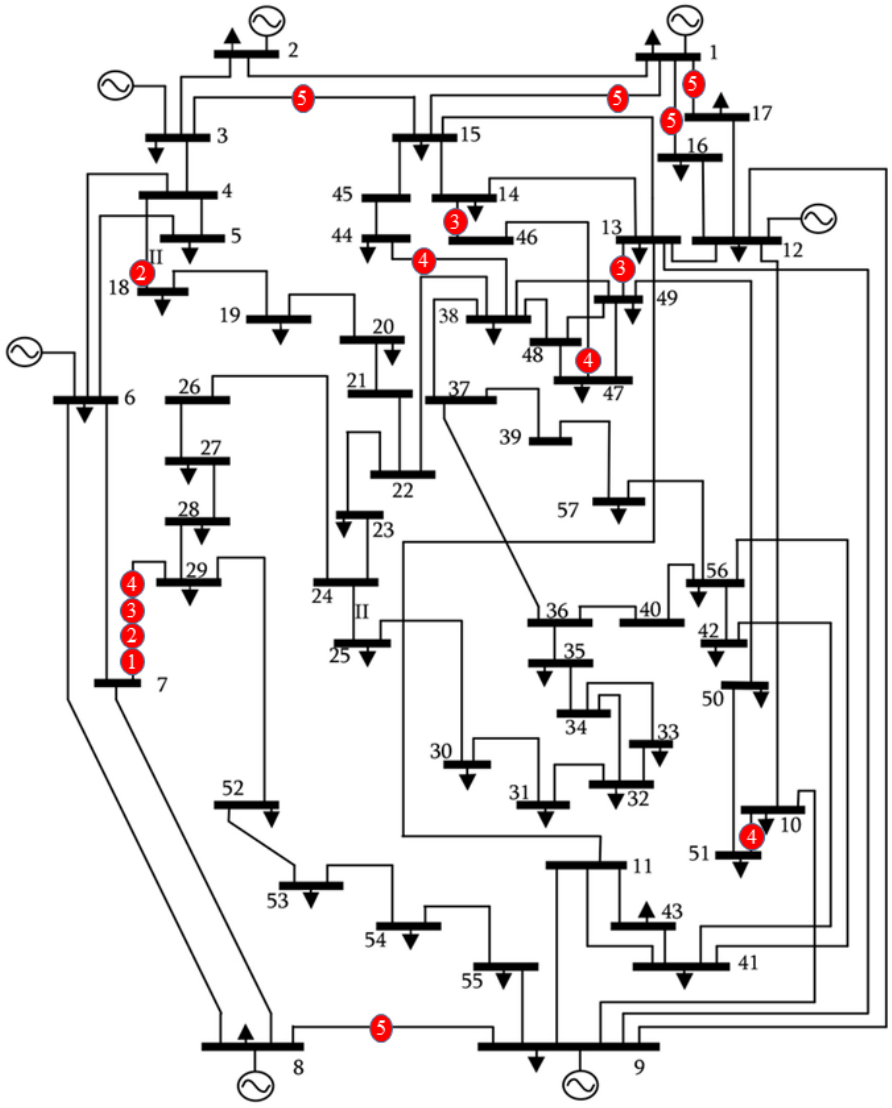

Figure 5-5. The IEEE 57-bus system and optimal solutions for NPO=1 to 5 using our proposed MILP model.

found using our proposed ACOPF-based approach. In addition, Table 5-3 is useful to analyze the effects of DCOPF approximations on the results. As can be seen, the DCOPF approximations affect not only the optimal load shedding value but also the proposed critical lines that must be hardened by the system planner. This fact is reported in the average of JSI for the sets of critical lines which is 0.5. In this network, similar to the previous one, the potential critical lines are parallel lines (e.g. 4-18) and the lines connecting the generation to demand zones (e.g. 7-29, 1-16, etc.).

Table 5-3. The five worst-case load shedding scenarios and their related lines for the IEEE 57-bus system calculated using our MILP model

NPO	DCOPF-based approach*	LS (MW)	ACOPF-based approach	LS (MW)	JSI
1	25-30	6	7-29	64	0
2	1-16, 12-16	43	4-18, 7-29	95	0
3	7-29, 9-55, 21-22	78	7-29, 13-49, 14-46	118	0.2
4	7-29, 8-9, 12-17, 21-22	105	7-29, 10-51, 38-44, 46-47	132	0.1
5	1-16, 7-29, 8-9, 12-17, 21-22	186	1-15, 1-16, 1-17, 3-15, 8-9	245	0.3

* This approach is also used with different objective functions and case studies in **[347, 352-354]**.

5-4-3 The Iran's 400-kV network

As the last test system, the proposed MILP model is implemented in a realistic power system. A modified Iran's 400-kV transmission network is used in this subsection. Iran's transmission network has voltage levels of 400 kV and 230 kV. It is operated by the Iran Grid Management Company (IGMC) which is established in 2003 as an independent system operator (ISO) [371]. The system is comprised of 52 buses, 28 generators, and 99 lines as shown in Figure 5-7. In this figure, the solid lines/circles are existing lines/substations and the dashed lines/circles are candidate 400-kV lines/substations which are planned to be added to the existing system as reported in [371]. The detailed data of this network can be found in [366, 371].

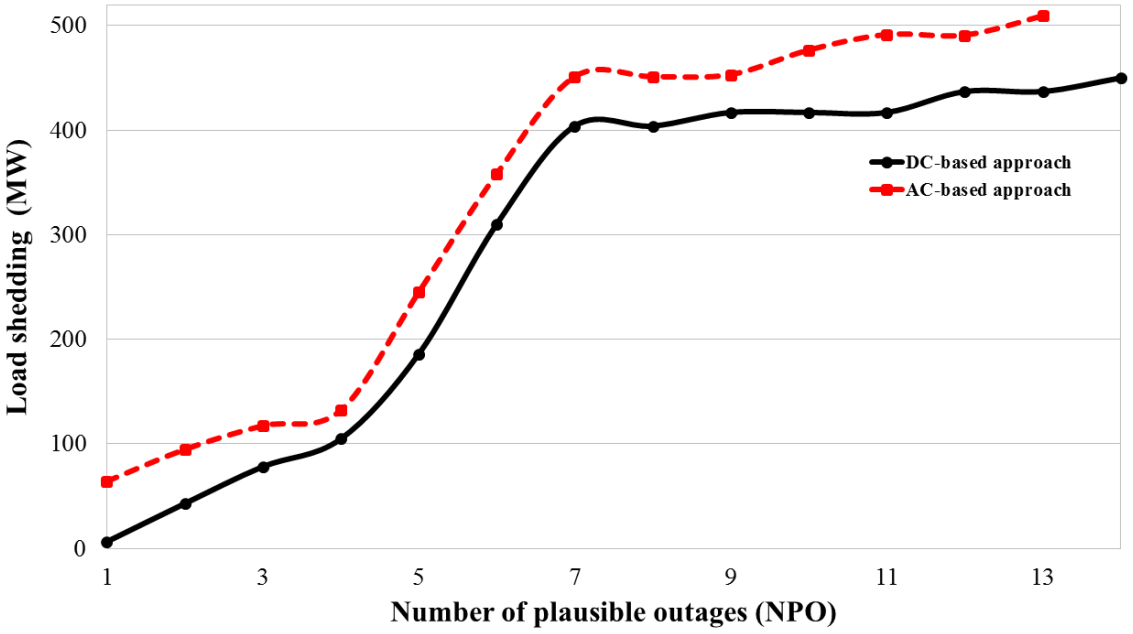

Figure 5-6. The load shedding for IEEE 57-bus system as a function of the number of plausible outages (NPO).

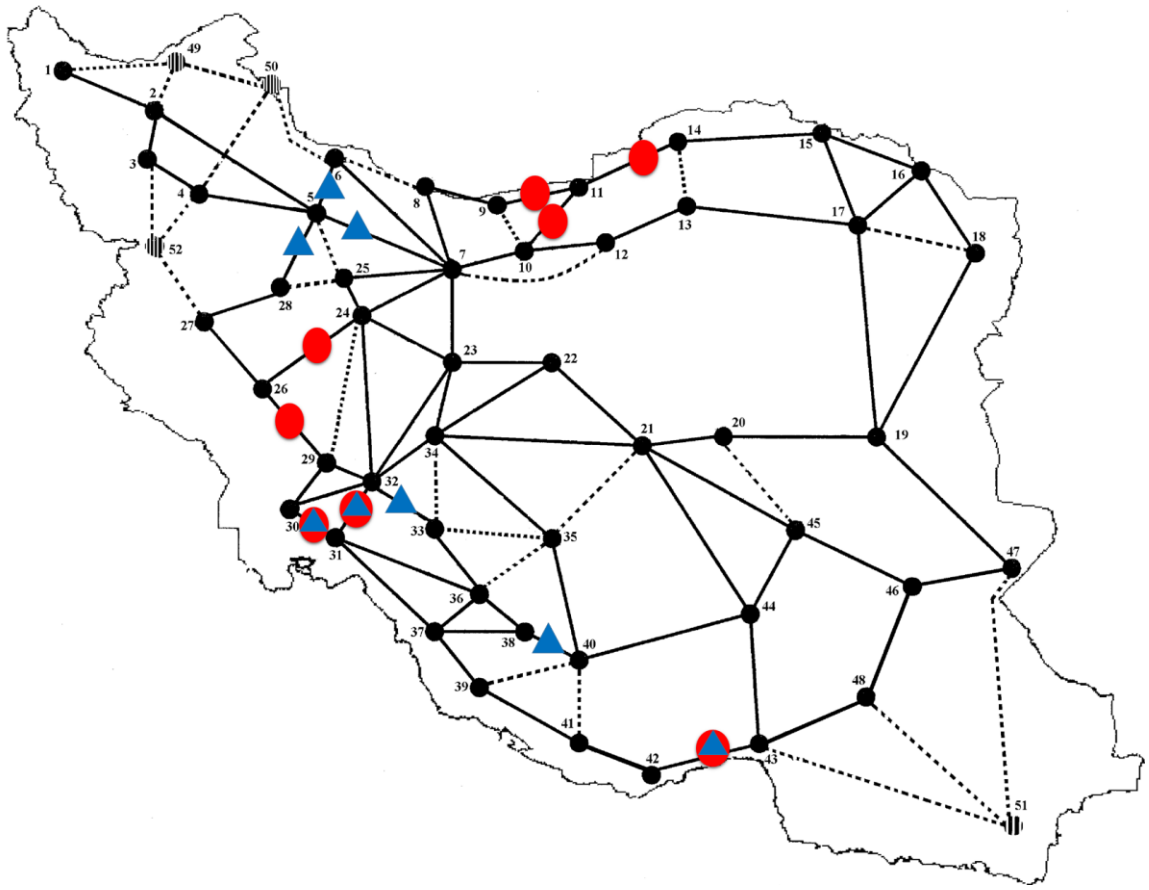

Figure 5-7. Modified Iran's 400-kV transmission network, existing lines/substations are black solid lines/ nodes and the candidate lines/ substations are black dash lines/nodes. The critical lines for the existing network are indicated by blue triangles and the ones for the expanded network are indicated by the red circles (NPO=8).

Figure 5-8 compares the imposed load shedding as a function of NPO in two topologies. According to this figure, the total possible load shedding of 10390 MW will occur after removing 46 and 61 simultaneous lines (i.e. NPO) in the existing and new grids, respectively. The figure also highlights that the new grid is more robust than the existing one (on average, the load shedding is decreased by 40% for a given NPO). Finally, as an example, the proposed set of critical lines that need to be hardened is presented in Figure 5-8, when NPO=8.

5-5 Conclusion

This chapter proposes a MILP for power system vulnerability assessment. An attacker-defender Stackelberg game is introduced to model the interaction between the attacker and the defender. This attacker-defender game is modeled as a bilevel optimization problem. The upper level represents the attacker and the lower level represents the defender. Employing the ACOPF for the defender model, the whole attacked-defender game is a mixed-integer bilevel nonlinear program (MIBNLP). The original MIBNLP is NP-hard and hard to solve. Accordingly, we first

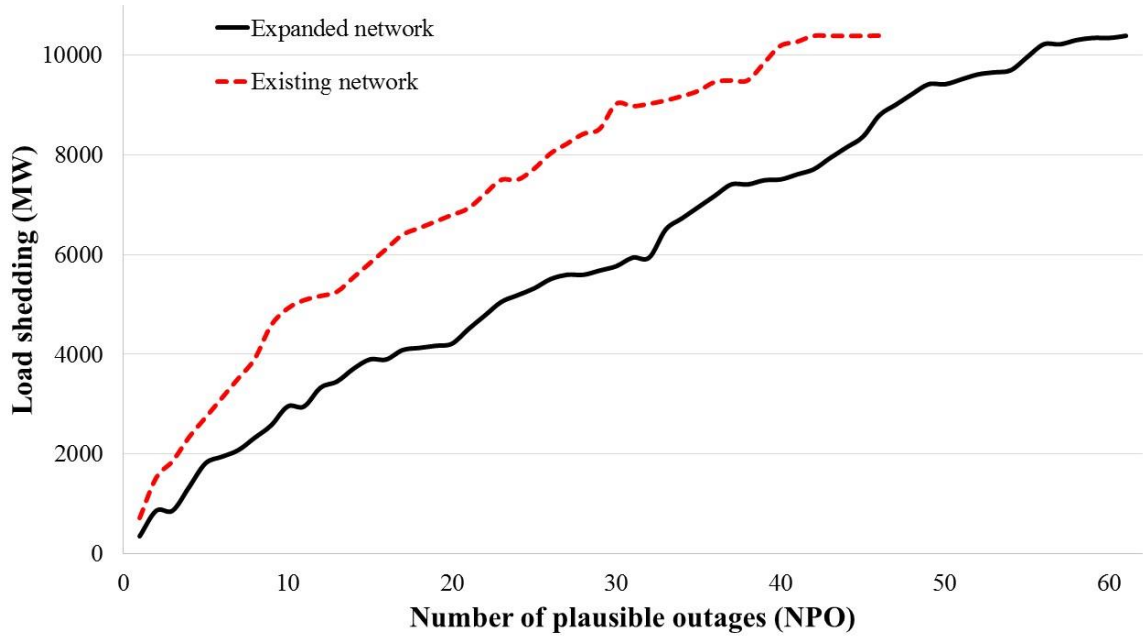

Figure 5-8. The load shedding for modified Iran's 400-kV transmission network as a function of number of plausible outages (NPO).

approximate the ACOPF as a linear program though some practically sound approximations for well-behaved transmission networks and some linearization techniques. Replacing the nonlinear program of the lower-level ACOPF model converts the original MIBNLP problem to a mixed-integer bilevel linear program (MIBLP). We then employ the duality theory for linear programs and replace the lower level with its dual program. The duality theory along with some linearization techniques transforms the problem to a single level MILP model. Our proposed MILP model can be solved efficiently to global optimum using state-of-the-art solvers such as Cplex. Our proposed MILP model has been applied to several case studies to show its performance and utility. In particular, using an approximate ACOPF model in our vulnerability assessment makes our results more trustable as compared to the vulnerability assessment models based on DCOPF used in the previous literature. Our work can be extended in several aspects. First, our deterministic model can be extended to a stochastic one where the uncertain parameters are modeled by a set of scenarios. Second, the dynamic response of the power system to an attack can also be incorporated in our MILP assessment model.

Chapter appendix: Nomenclature

Indices

i,j	Indices of buses
k	Index of regular polygon for linearizing the circle
l	Index of lines
m	Index of blocks used for piecewise linearization

Sets

D	Set of all buses with demand
G	Set of all buses with generation
L	Set of all lines
N	Set of all buses

Constants

B	Big-*M* parameter
B_{ij}^{sh}	Total line charging susceptance of line *ij* (p.u.)
C_i	Cost coefficients of generators ($/MWh)
$\mathrm{Cos}\,\phi_i$	Power factor at bus *i*
M	Number of blocks used for piecewise linearization
n	Number of sides of a regular polygon to formulate a circle
NPO	Number of plausible outages (interdiction resources)
$Pg_i^{\max}$	Maximum of active-power magnitude for a generator at bus *i* (MW)
$Qg_i^{\max}$	Maximum of reactive-power magnitude for a generator at bus *i* (MVAR)
$Qg_i^{\min}$	Minimum of reactive-power magnitude for a generator at bus *i* (MVAR)
$R(ij)$	Receiving bus of line *ij*
$S(ij)$	Sending bus of line *ij*
$S_{ij}^{\max}$	Maximum of apparent-power magnitude for line *ij* (MVA)
Y_{ij}	Admittance of line *ij* (p.u.) $(Y_{ij} = G_{ij} + jB_{ij})$
$V_i^{\max}$	Maximum of voltage magnitude at bus *i* (V)
$V_i^{\min}$	Minimum of voltage magnitude at bus *i* (V)
$\theta_{ij}^{\max}$	Maximum of voltage-angle difference between bus i and j (Rad)
$\theta_{ij}^{\min}$	Minimum of voltage-angle difference between bus i and j (Rad)
$\Delta\theta_{ij}$	Maximum of each block width for line *ij*

Variables

Ls_i	Active-power load shedding at bus i (MW)
Lsq_i	Reactive-power load shedding at bus *i* (MVAR)
P_{ij}	Active power-flow of line *ij* (MW)
Pg_i	Active power of generator at bus *i* (MW)
Pd_i	Active power demand at bus *i* (MW)
Q_{ij}	Reactive power-flow of line *ij* (MVAR)
Qg_i	Reactive power of generators at bus *i* (MVAR)
Qd_i	Reactive power demand at bus *i* (MVAR)
V_i	Voltage magnitude at bus *i* (V)
Z / z_{ij}	Upper-level decision variable: binary variable that is equal to 0 if line *ij* is out of service and otherwise, is equal to 1
θ_{ijm}	Width of the mth angle block of line *ij* (Rad)
θ_{ij}	Voltage-angle difference between bus i and j (Rad)
$\delta_{ij}^{+}, \delta_{ij}^{-}$	Positive variables used to reformulate the absolute function
T_{ij}, H_{ij}	Auxiliary variables to linearize the product of binary and continuous variables
$\lambda_{ij}, \mu_{ij}, \alpha_i, \overline{\omega}_i, \beta_i, \overline{\delta}_i, \overline{\sigma}_i, \overline{\upsilon}_i, \xi_{ij}, \underline{\upsilon}_i, \eta_{1,ij} \cdots \eta_{n,ij}, \chi_{ij}, o_{ijm}, \varphi_{ij}, \kappa_{ijm}, \varepsilon_{ij}$	Dual variables associated with their corresponding constraints

Chapter 6

Multi-period vulnerability analysis of power grids under multiple outages: An AC-based bilevel optimization approach

6-1 Introduction

Energy is a vital commodity in modern societies and power systems play a crucial role in providing secure and reliable energy. Protection of the power system as a critical infrastructure against different hazards and threats i.e., natural hazards, intentional attacks, and random failures [17] has become a growing concern. Furthermore, the interdependencies between power systems and communication networks in smart grids are introducing new challenges i.e., cyber threats. So, the operators and planners must protect the most vulnerable elements of a system under a variety of attack scenarios in order to improve the system security and deploying a robust and resilient power system [33].

In this context, a key question is which components are critical and must be protected or fortified when the protective and financial resources are limited [373]. To this end, it is fundamental to develop robust methodologies and tools to assess the vulnerability of a power system against external attacks [374]. Hence, the vulnerability analysis and, in particular,

prioritizing the vulnerable components result in an effective power system protection with limited resources [375].

Contingency analysis or *N-k* contingency assessment is a methodology looking for a set of *k* critical components of the power system whose simultaneous failure would maximize the damage, in terms of the amount of involuntary load shedding in the power system. *N-k* ($k \geq 2$) contingencies are low-probability events but inherently more severe than *N*-1 contingencies in triggering cascading failures and even blackouts [376]. Therefore, the North American Reliability Council (NERC) suggests power system planners and operators considering *N-k* contingency analysis in their planning and operation [377]. The difficulty of *N-k* contingency selection is that it follows the combination formula. It means that for a very modest size power system with *N*=1000, there are 1000 '*N*-1' contingencies, 499500 '*N*-2' contingencies, over 160 million '*N*-3' contingencies, over 40 billion '*N*-4' contingencies and so on. So, the number of possible *N-k* contingencies, even for small values of *k*, makes total enumeration approaches computationally impractical in a large-scale interconnected power network [378].

Scientists have been developing innovative methods to determine critical components whose failures lead to the largest system loss. Generally, there are two different lines of work in the literature. Some literature work on the low-order contingencies including single or a small number of component failures that have a very high occurrence probability. For instance, the *N*-1 security constraint that all of the regulatory agencies in the world enforce the system operators to satisfy it by strict security standards. Within this constraint, the system should normally continue to work after any single failure [379]. Analyzing the loss of two elements consecutively or *N*-1-1 contingency analysis is another example of this category [335, 380, 381]. It should be noted that the reliability concept that defines the ability of the electric power system to meet the demand with continuity and an acceptable level of quality, comes under the low-order contingencies [22].

The second line of works presents not only the low-order but also the high-order contingencies. The high-order contingencies include a relatively large number of component failures that have a very low occurrence probability but high consequences. The focus of this chapter is on this type of assessment i.e. the vulnerability analysis of power systems. The vulnerability can be social, organizational, economic, environmental, territorial, physical, and systemic [86, 87]. Most studies focus on physical and systemic vulnerabilities. Physical vulnerability represents the degree of loss of an element due to external pressure such as natural hazards [88]. In

contrast, systemic vulnerability considers the degree of redundancy, functionality, and dependency of a system due to the failure of a specific element or an interconnected system [89]. This chapter aims to investigate the behavior of the power system i.e. systemic vulnerability to identify the critical components under a worst-case scenario such as an intentional attack.

The works can range from analytical approaches (complex network, flow-based, logical, and functional methods) to Monte Carlo simulations. A detailed comparison of these approaches is recently conducted in [20] (and the references therein). Among them, the optimization-based problem can directly lead to promising results without the need to rank the sets of critical assets. The application of these approaches is considerably increasing in the complex problems thanks to the advent of advanced high-speed multiprocessors with large memory. It makes the problem tractable for a realistic power system [340].

The interdiction model is at the forefront of the models used to identify the worst *N-k* contingency. It has been developed based on a multilevel optimization problem to assess the vulnerability of power systems [341]. A multilevel optimization is a mathematical program where an optimization problem contains another optimization problem as a constraint [342]. These problems are also known as the hierarchical leader-follower problem or the Stackelberg game [343]. The interdiction model basically includes an upper level whose objective is to identify exactly *k* components to maximize the damage (load shedding) in the system and a lower level whose objective is mitigating the impacts of attacks and minimizing the damage consequences.

Later, the interdiction model is developed based on two models i.e., bilevel and trilevel interdiction models. For instance, Karush-Kuhn-Tucker (KKT) optimality conditions [346] and duality theory [347] are used to convert a bilevel attacker-defender model to a one-level problem. Arroyo J.M. [348] compared the KKT- and duality-based approaches by introducing minimum and maximum vulnerability models. Brown et al. [352] extended the classical bilevel interdiction model to a general trilevel defender-attacker-defender model to assign limited defensive resources in power systems. Alguacil et al. [353] proposed an approach to allocate the defensive resources in a power system to mitigate the vulnerability. Wu et al [354] decomposed a planner-attacker-operator model to a master problem and a subproblem using a Benders primal decomposition method. Recently, Fang et al. [19, 355] and Che et al. [372] used this approach to identify the vulnerability of power grids exposed to natural hazards and the

hidden *N-k* contingencies, respectively and finally, Nemati et al. [382, 383] proposed tri-level transmission expansion planning (TTEP) under physical intentional attacks.

The above-surveyed literature uses the simplified formulation of nonlinear AC optimal power flow (ACOPF) i.e., the DC optimal power flow (DCOPF) as the lower level. The DCOPF has some drawbacks. Technically, it cannot provide precise information on the power system since it ignores reactive power, resistance and losses and fixes the voltage values for the buses. Mathematically, restricting the available degrees of freedom (e.g., fixed voltages in DC-based method) makes the solution non-optimal and less accurate [359].

To the best of our knowledge, a few studies considered a real picture of the power grid parameters i.e. both active and reactive powers, losses, and voltage profile to assess the vulnerability of the power system. Kim et al. [360] used the AC power flow equations and the Frank Wolfe algorithm to compute an optimal solution of the problem. However, they assumed that attackers are allowed to increase the impedance of transmission lines in the model. Modeling component removal needs to introduce binary variables that require different and more complicated solution techniques. Recently, a probabilistic *N-k* model is introduced to analyze a probabilistic generalization of the interdiction model using the cutting-plane algorithm [378]. They use convex relaxations instead of the DC power flow approximation.

Generally speaking, the ACOPF is a non-linear and non-convex optimization problem [340] which is used as the lower level in this chapter. Considering the ACOPF for each time period (t) as the lower level converts the problem to a bilevel mixed-integer nonlinear programming (MINLP) problem that is very complicated and challenging to solve. It should be emphasized that employing metaheuristic algorithms or non-linear solvers does not guarantee to have a global optimum solution [365]. The aim of this chapter is to tackle the new problem and avoid the probable local solution for each time period (t). The contributions of the proposed model in this chapter are threefold:

(1) A novel deterministic multi-period AC-based one-level MILP formulation of a bilevel MINLP problem is introduced so as to assess the *N-k* contingency analysis.

(2) The model considers a real picture of the power grid parameters i.e., both active and reactive powers, losses, and voltage profile.

(3) The planners can decide the level of accuracy by setting the predefined parameters (i.e., n and M) that are introduced in the linearization process for each time period (t).

The remainder of this chapter is organized as follows. Section 6-2 introduces the multi-period AC-based bilevel MINLP problem. Section 6-3 proposes the solution approaches to linearize and then, transforming to a one-level MILP problem. Sections 6-4 and 6-5 present the test case and the numerical results, respectively. Concluding remarks are finally provided in Section 6-6.

6-2 The multi-period AC-based bilevel MINLP problem

In this section, the mathematical formulation of multi-period AC-based bilevel MINLP problem is introduced. The model provides the worst-case scenario under multiple outages that is of interest in *N-k* security assessment. This formulation is based on the following assumptions that are commonly used for vulnerability and contingency assessment of a power system [346-348, 352-354, 384, 385]:

1. The rational attacker (the worst-case scenario) is considered trying to maximize the damage and can disable multiple assets simultaneously and permanently or at least for several hours. As a result, the power flow of other lines will be affected.
2. The power system has two main components i.e., substations or transmissions and transformers. Herein, the targeting assets are transmission lines and transformers, because they are usually reachable with low or no security to withstand. However, by removing the connected lines and transformers of a load bus, it will be spontaneously out of service.
3. Because two parallel circuits between the buses are usually on the same tower, they are modeled as a single line with double capacity. Furthermore, the shunt susceptances of the lines are ignored.
4. A steady-state security model and multi-period scenario are considered where typically, the highest load demand forecast is used in each time period (i.e., daily, hourly, etc.).
5. Herein, the system damage is load shedding, that is, the amount of involuntarily decreasing the load demand. In the lower level, we assumed the active and reactive loads are shed independently [386]. Admittedly, different objective functions as the system damage can be defined based on the interest.
6. The ratings of transmission lines are not only limited by the power flowing in that line but also they are dependent on the conductor material and radius and the weather such as solar irradiance, ambient temperature, wind speed, and wind direction. In the following formulation, a static thermal rating is used. However, applying the dynamic thermal rating in the model is also straightforward.

According to the multi-period interdiction (attacker-defender) model in Figure 6-1, the attacker as a leader or upper-level problem starts the game with the limited disruptive resources. The system operator as a follower or lower-level problem reacts against the set of out-of-service assets to mitigate its adverse consequences based on the following formulations whose dual variables are shown on top of the corresponding equalities or inequalities:

$$\underset{Z}{Max} \sum_{i \in NB} Ls_i^{t^*} \tag{6-1}$$

Subject to:

$$0.5 \times \sum_{i,j \in N} (1 - z_{ij}{}^t) = k; \quad z_{ij}{}^t \in \{0,1\} \quad \forall i, j \in N \tag{6-2}$$

$$\sum_{i \in NB} Ls_i^{t^*} \in \arg \left\{ \underset{\substack{Pg,Qg,Ls,Lsq, \\ P,Q,V,\theta}}{Min} \sum_{i \in NB} Ls_i^t \right\} \tag{6-3}$$

Subject to:

$$Pg_{i|i \in D}^t + Ls_{i|i \in D}^t - Pd_{i|i \in D}^t \overset{\alpha_i}{=} \sum_{j \in NB} P_{ij}^t; \quad \forall i, j \in NB, \forall t \in T \tag{6-4}$$

$$Qg_{i|i \in G}^t + Lsq_{i|i \in D}^t - Qd_{i|i \in D}^t \overset{\beta_i}{=} \sum_{j \in NB} Q_{ij}^t; \quad \forall i, j \in NB, \forall t \in T \tag{6-5}$$

$$P_{ij}^t = z_l{}^t \left(V_{it}{}^2 G_{ij} - V_{it} V_{jt} (G_{ij} \cos \theta_{ijt} + B_{ij} \sin \theta_{ijt}) \right); \quad \forall l \in L, \forall t \in T \tag{6-6}$$

$$Q_{ij}^t = z_l{}^t \left(-V_{it}{}^2 B_{ij} - V_{it} V_{jt} (G_{ij} \sin \theta_{ijt} - B_{ij} \cos \theta_{ijt}) \right); \quad \forall l \in L, \forall t \in T \tag{6-7}$$

$$0 \le Pg_i^t \overset{\bar{\delta}_i}{\le} Pg_i^{\max}; \quad \forall i \in G, \forall t \in T \tag{6-8}$$

$$Qg_i^{\min} \overset{\underline{\sigma}_i}{\le} Qg_i^t \overset{\bar{\sigma}_i}{\le} Qg_i^{\max}; \quad \forall i \in G, \forall t \in T \tag{6-9}$$

$$\left(P_{ij}^t\right)^2 + \left(Q_{ij}^t\right)^2 \le \left(S_{ij}{}^{\max}\right)^2; \quad \forall l \in L, \forall t \in T \tag{6-10}$$

$$V_i^{\min} \overset{\underline{\upsilon}_i}{\le} V_{it} \overset{\bar{\upsilon}_i}{\le} V_i^{\max}; \quad \forall i \in NB, \forall t \in T \tag{6-11}$$

$$\theta_{ij}{}^{\min} \le \theta_{ijt} \le \theta_{ij}{}^{\max}; \quad \forall i, j \in NB, \forall t \in T \tag{6-12}$$

$$0 \le Ls_i^t \le \bar{\omega}_i Pd_i^t; \quad \forall i \in D, \forall t \in T \tag{6-13}$$

$$0 \le Lsq_i^t \le \bar{\psi}_i Qd_i^t; \quad \forall i \in D, \forall t \in T \tag{6-14}$$

Equation (6-1) shows the objective function that the attacker is trying to maximize with the constraint sets (6-2)-(6-14). Equation (6-2) is the upper-level constraint that shows the maximum number of outages (k) is fixed. If z_l is 0, the line l is under attack. Otherwise, it is safe. Moreover, note that factor 0.5 is multiplied by the total number of line outages because $z_l = z_{ij} = z_{ji}$ and the line ij is considered twice in the formulation. In the lower-level problem (6-3)-(6-14), unlike the previous approaches [346-348, 352-354], the ACOPF is used as the operator tool to mitigate the adverse consequences of the outages. Equation (6-3) is the objective of the system operator to minimize the damage. The asterisk in (6-1) and (6-3) emphasizes that Ls_i are decision variables of the lower level problem. Equations (6-4) and (6-5) are the nodal power balance equations for active and reactive powers, respectively. Equations (4-3) and (4-4) represent the line flows of active and reactive powers, respectively. Constraints (6-8)-(6-14) enforce the limits of active and reactive power generations, transmission line capacity, voltage, and voltage angle, active and reactive load shedding, respectively. The above-formulated problem is a bilevel MINLP problem due to the

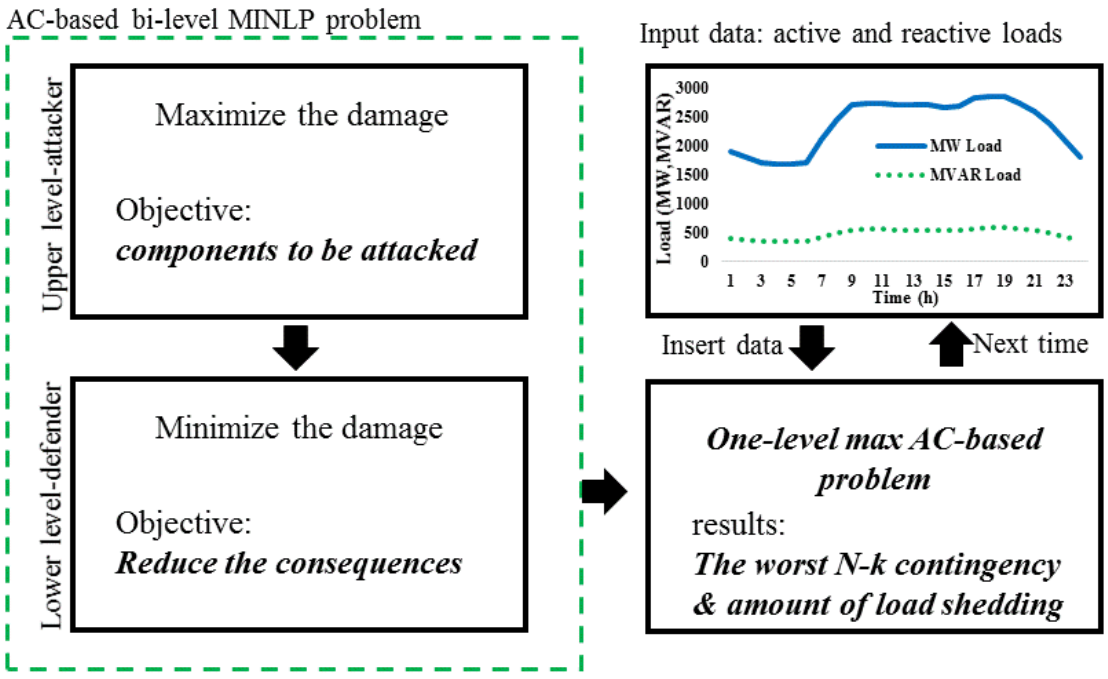

Figure 6-1. The multi-period AC-based bilevel MINLP problem.

nonlinearities in equations (4-3), (4-4) and (4-7). In the following sections, just for the sake of simplicity, the superscript "*t*" has been dropped.

6-3 Solution methodology

It should be noted that there will be no guarantee to obtain the global solution due to the non-convexity non-linearity nature of the proposed approach [387] with a non-linear solver or evolutionary approaches [340]. Therefore, we transformed it to one-level MILP problem in two steps. First, the lower-level problem is transformed to a MILP problem to avoid any local solution. Then, the duality theory [388] is used to have a one-level MILP problem in the second step.

6-3-1 Linearizing lower-level NLP problem

To linearize the lower-level NLP problem, the phase differences between the bus voltages are assumed small enough and the voltage magnitude is close to 1 p.u. for all buses. These assumptions are practically acceptable under the normal operating condition to maintain the system far from instability [340]. Based on the aforementioned assumptions, the first-order approximation of Taylor's series with respect to the variables $\{V_i, V_j, \cos\theta_{ij}, \sin\theta_{ij}\}$ is used for nonlinear terms of equations (4-3)-(4-4) (z_l is a constant at this level). Then, the quadratic function is linearized based on the proposed method in [363] by using 2M piecewise linear (PWL) blocks as below:

$$P_{ij} \overset{\lambda_l}{=} z_l \left(G_{ij}\left(2V_i - 1\right) - G_{ij} \left(V_i + V_j + (1 - \frac{\sum_{m=1}^{M}((2m-1)\Delta\theta_{ij})\theta_{ijm}}{2}) - 2 \right) - B_{ij}(\delta_{ij}^{+} - \delta_{ij}^{-}) \right) \tag{6-15}$$

$$Q_{ij} \overset{\mu_l}{=} z_l \left(-B_{ij}\left(2V_i - 1\right) + B_{ij} \left(V_i + V_j + (1 - \frac{\sum_{m=1}^{M}((2m-1)\Delta\theta_{ij})\theta_{ijm}}{2}) - 2 \right) - G_{ij}(\delta_{ij}^{+} - \delta_{ij}^{-}) \right) \tag{6-16}$$

$$\left|\theta_i - \theta_j\right| = \sum_{m=1}^{M} \theta_{ijm} \overset{\varphi_{ij}}{=} \delta_{ij}^{+} + \delta_{ij}^{-}; \quad m = 1 \cdots M, \forall i, j \in NB \tag{6-17}$$

$$0 \le \theta_{ijm} \overset{o_{ijm}}{\le} \Delta\theta_{ij}; \quad m = 1 \cdots M, \forall i, j \in NB \tag{6-18}$$

$$\theta_{ijm} \overset{\kappa_{ijm}}{=} \theta_{jim}; \quad m = 1 \cdots M, \forall i, j \in NB \tag{6-19}$$

Where, $(2m-1)\Delta\theta_{ij}$ and θ_{ijm} are the slope and the value of the m[th] block of the voltage phase difference of transmission line ij (see Figure 6-2). Derivation of equations (6-15) and (6-16) are described in the appendix. The appropriate value for $\Delta\theta_{ij}$ can be $\frac{\pi}{M}$. The absolute function in (5-19) is modeled by introducing two positive variables i.e., δ_{ij}^{+} and δ_{ij}^{-}. This linearization technique of the quadratic function doesn't need to have binary variables compared to other linearization techniques such as the binary expansion theory [364], the special ordered set of type 2 (SOS2) [365]. Nevertheless, this technique adds three sets of continuous variables to the problem (M+2 variables for each line). Adding binary variables changes the lower-level problem to a MILP problem that is impossible to use the duality theory in the next step to have a one-level MILP problem [353].

As can be seen, the last nonlinear constraint of the lower-level problem (i.e., equation (4-7)) presents a circle with the radius of $S_{ij}^{\max}$. This circle is linearized by an n-sided convex regular polygon using the following n equations [366]:

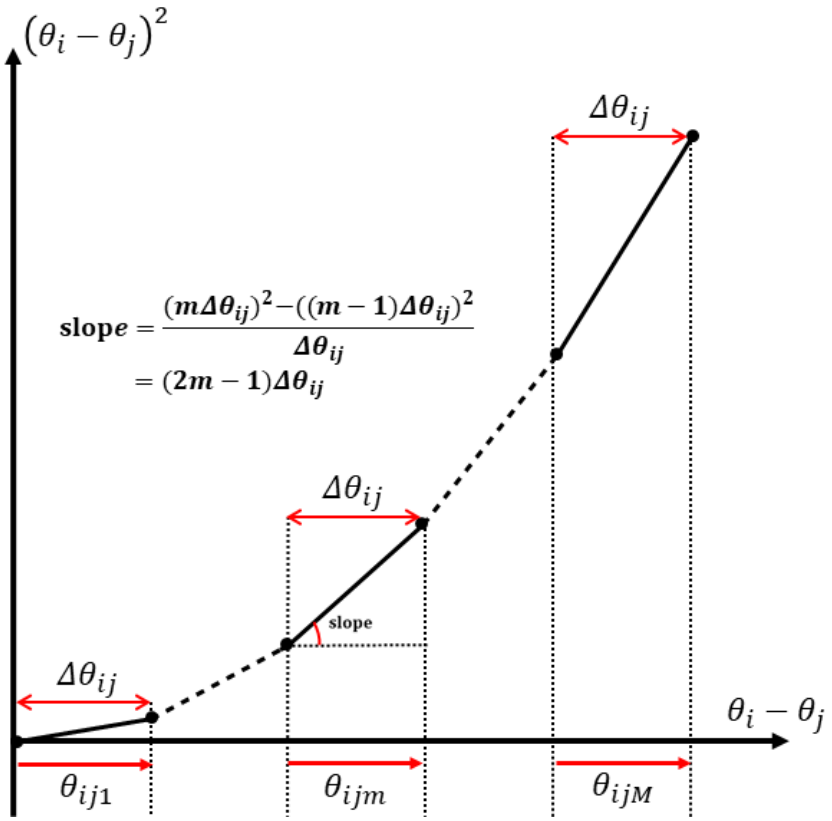

Figure 6-2. Piecewise linear approximation of a nonlinear function.

$$\left(\sin\left(\frac{2\pi kc}{n}\right)-\sin\left(\frac{2\pi(kc-1)}{n}\right)\right)P_{ij}-\left(\cos\left(\frac{2\pi kc}{n}\right)-\cos\left(\frac{2\pi(kc-1)}{n}\right)\right)Q_{ij}$$
$$-S_{ij}^{\max}\sin\left(\frac{2\pi}{n}\right)^{\eta_{k,l}}\le 0;\quad kc=1\cdots n,\forall i,\ j\in NB \tag{6-20}$$

In fact, the linearization of (4-7) adds "*n*" equations for each line. A small *n* forces more restrictions on transmission line capacity and probably leads to the infeasible problem while a big *n* increases the number of equations and simulation time. The appropriate value for *n* can be 64 [340, 365]. Thereafter, the problem is completely a bilevel MILP which can be transformed into one-level MILP in the next section using the duality theory [388].

6-3-2 Transforming to an equivalent one-level MILP problem

The duality theory states that every linear programming (LP) problem (the primal problem) has another LP problem (the dual problem) that can be derived from it. The dual problem will be a maximization problem when the primal problem is a minimization problem and vice versa. Furthermore, each variable (constraint) in the primal problem becomes a constraint (variable) in the dual problem [388]. So, in order to transform the bilevel max-min problem to a max-max problem, the duality theory is used below. Then, the max-max problem is reformulated to a one-level max problem as follows.

$$\underset{\substack{z_{ij},\underline{\lambda}_{ij},\underline{\mu}_{ij},\underline{\alpha}_i,\overline{\omega}_i,\\ \overline{\beta}_i,\overline{\delta}_i,\overline{\sigma}_i,\overline{\upsilon}_i,\overline{\xi}_{ij},\\ \underline{\upsilon}_i,\eta_{1,ij}\cdots\eta_{n,ij},\chi_{ij},\\ o_{ijm},\varphi_{ij},\kappa_{ijm},\varepsilon_{ij}}}{Max}\left(\begin{array}{l}\sum_{l\in L}z_l\lambda_l G_{ij}-\sum_{l\in L}z_l\mu_l B_{ij}+\sum_{i\in NB}(\alpha_i+\overline{\omega}_i)Pd_{i|i\in D}+\sum_{i\in NB}(\beta_i+\overline{\psi}_i)Qd_{i|i\in D}\\ +\sum_{i\in G}\overline{\delta}_i Pg_i^{\max}+\sum_{i\in G}\overline{\sigma}_i Qg_i^{\max}+\sum_{i\in G}\underline{\sigma}_i Qg_i^{\min}+\sum_{i\in NB}\overline{\upsilon}_i V_i^{\max}+\sum_{i\in NB}\underline{\upsilon}_i V_i^{\min}\\ +\sum_{l\in L}S_{ij}^{\max}\sin\left(\frac{2\pi}{n}\right)(\eta_{1,l}+\cdots+\eta_{n,l})+\sum_{l\in L}\chi_{ij}+\sum_{l\in L}\sum_{m=1}^{M}o_{ijm}\Delta\theta_{ij}\end{array}\right) \tag{6-21}$$

Subject to:

$$0.5\times\sum_{i,j\in N}(1-z_{ij})=k;\quad z_{ij}\in\{0,1\}\quad\forall i,j\in N \tag{6-22}$$

$$\lambda_l-\alpha_i+\sum_{kc=1}^{n}\eta_{kc,l}\left(\sin\left(\frac{2\pi kc}{n}\right)-\sin\left(\frac{2\pi(kc-1)}{n}\right)\right)^{P_{ij}}=0 \tag{6-23}$$

$$\mu_l-\beta_i-\sum_{kc=1}^{n}\eta_{kc,l}\left(\cos\left(\frac{2\pi kc}{n}\right)-\cos\left(\frac{2\pi(kc-1)}{n}\right)\right)^{Q_{ij}}=0 \tag{6-24}$$

$$-\sum_{l|S(l)=i} z_l\lambda_l G_{ij} + \sum_{l|R(l)=i} z_l\lambda_l G_{ij} + \sum_{l|S(l)=i} z_l\mu_l B_{ij} - \sum_{l|R(l)=i} z_l\mu_l B_{ij} + \overline{\upsilon}_i + \underline{\upsilon}_i \overset{V_i}{=} 0 \tag{6-25}$$

$$z_l\lambda_l G_{ij} - z_l\mu_l B_{ij} + \chi_{ij} \overset{c_{ij}}{=} 0 \tag{6-26}$$

$$z_l\lambda_l B_{ij} + z_l\mu_l G_{ij} + \xi_{ij} + \varepsilon_{ij} + \varepsilon_{ji} \overset{n_{ij}}{=} 0 \tag{6-27}$$

$$\alpha_i + \overline{\delta}_i \overset{Pg_{i|i\in G}}{\leq} 0 \tag{6-28}$$

$$\beta_i + \overline{\sigma}_i + \underline{\sigma}_i \overset{Qg_{i|i\in G}}{=} 0 \tag{6-29}$$

$$+\varphi_{ij} - \xi_{ij} \overset{\delta_{ij}^{+}}{\leq} 0 \tag{6-30}$$

$$\varphi_{ij} + \xi_{ij} \overset{\delta_{ij}^{-}}{\leq} 0 \tag{6-31}$$

$$\chi_{ij}(0.5(2m-1)\Delta\theta_{ij}) - \varphi_{ij} + o_{ijm} + \kappa_{ijm} - \kappa_{jim} \overset{\theta_{ijm}}{\leq} 0 \tag{6-32}$$

$$\alpha_i + \overline{\omega}_i \overset{Ls_{i|i\in D}}{\leq} 1 \tag{6-33}$$

$$\beta_i + \overline{\psi}_i \overset{Lsq_{i|i\in D}}{\leq} 0 \tag{6-34}$$

Where the primal variables are shown on top of the corresponding equalities or inequalities. This transformation introduces a new nonlinearity to the model i.e., the product of binary and continuous dual variables ($z_l\lambda_l$ and $z_l\mu_l$) in equations (6-21), (6-25)-(6-27). This product can be easily linearized using two sets of continuous variables T_l and H_l [353, 367] that are introduced in the previous chapter.

6-4 Test system

The IEEE Reliability Test System (RTS) and IEEE 57-bus are used in this chapter. The IEEE 57-bus test case is only used for comparison. It represents a portion of the American Electric Power system (in the U.S. Midwest) and has 57 buses, 7 generators, and 42 loads [389]. Data availability makes the IEEE RTS an ideal test case for multi-period bulk power system vulnerability analysis. It contains 24 buses, 32 generators, and 38 branches (lines plus

transformers) as shown in Figure 6-3. The transmission lines operate at two different voltage levels, 132 kV and 230 kV. The system working at 230 kV and 132 kV are represented in the upper half and the lower half of Figure 6-3, respectively. Detailed data of the systems can be found in [240, 389]. Furthermore, the annual load profile of the IEEE RTS is shown in Figure 6-4. This profile can be adapted to seasonal patterns. If the first week is assumed the first week of the calendar year, then the profile shows the annual peak occurring in the week prior to Christmas (winter). If the week number one is assumed to be the first week of August, then the annual peak will occur in the month of July (summer) [240].

6-5 Numerical results

The proposed model has been successfully applied to the test systems. In this numerical study, the minimum and maximum of the voltage magnitude of buses are assumed to be 0.95 and 1.05 p.u., respectively [313]. The problems are solved on a laptop running with an Intel Core i7, 2.2 GHz processor, and 8 GB RAM. The CPLEX solver which uses the branch and cut algorithm is employed under GAMS (General Algebraic Modeling System) [390]. Furthermore, the

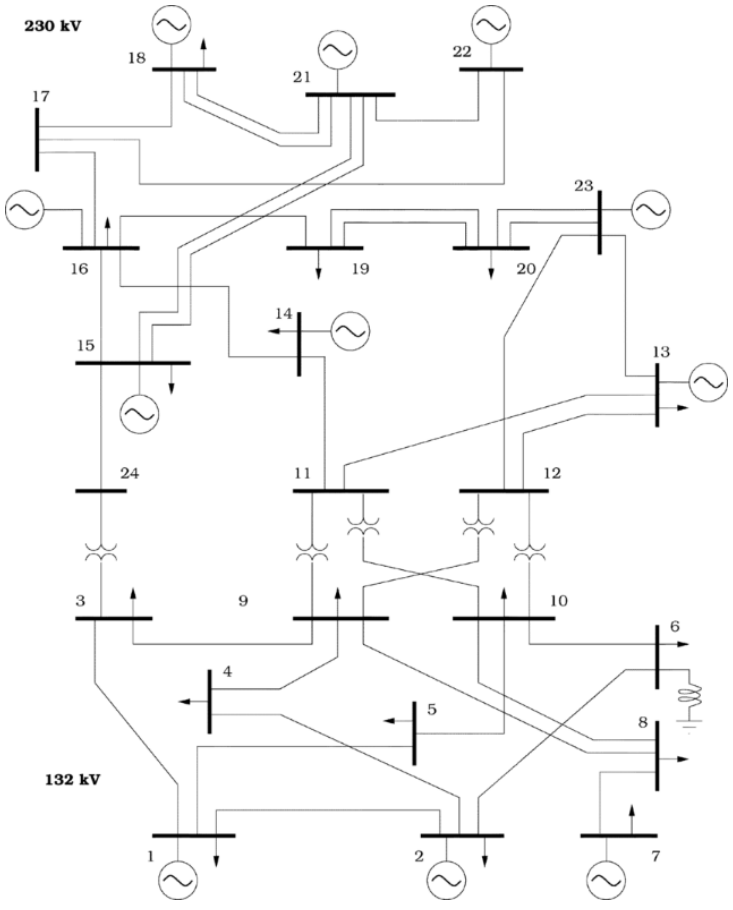

Figure 6-3. Topology of IEEE 24-bus reliability test systems (RTS).

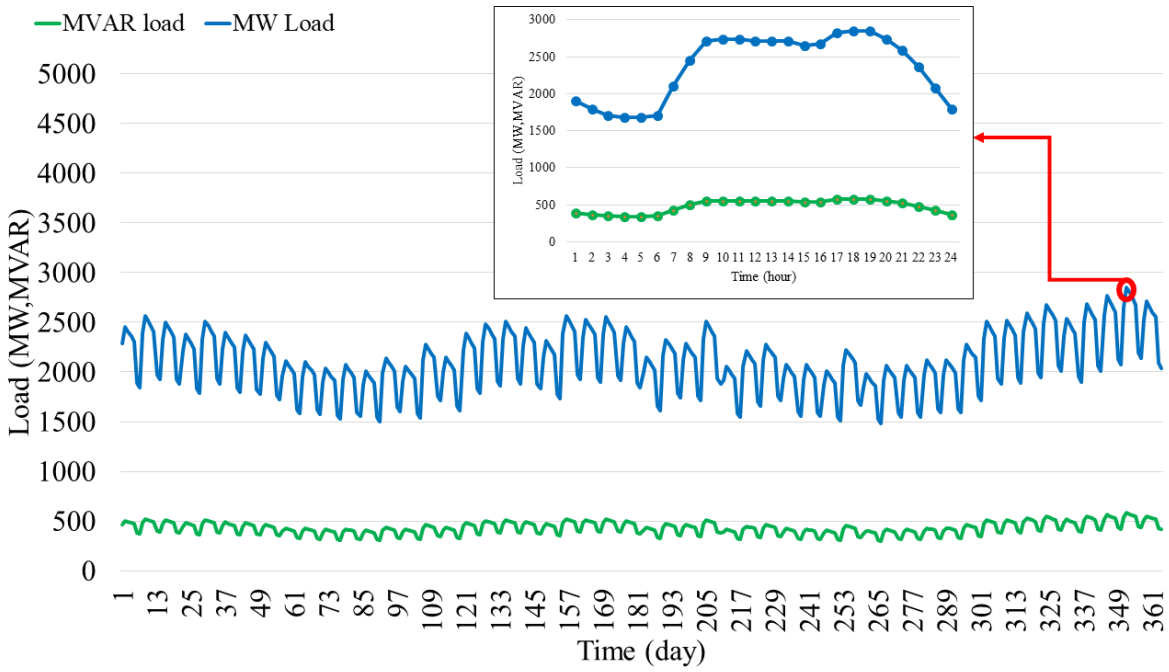

Figure 6-4. System daily peak loads in one year with highlighted annual peak load.

ACOPF function of MATPOWER in MATLAB environment [313] is also used for comparing the results. In linearization, it is assumed M=80 and n=64. Larger values for these parameters do not change the results [340, 365]. With these assumptions, Table 6-1 shows the comparison of statistic data for different test cases. It compares the average elapsed time of the models with the different numbers of nonzero elements, single equations, single variables, and binary variables. As discussed before, the difficulty of *N-k* contingency selection is that it follows the combination formula. Trendline of the simulation time shows that in the low-order contingencies and the orders that the objective function does not change afterward (e.g., *k*=13 in the IEEE RTS network), the simulation time is the minimum value while the number of samples is increasing (Figure 6-5).

Table 6-1. Comparison of statistic data of different test cases

Model statistics	**IEEE 24-bus**		**IEEE 57-bus**	
	DC-based	AC-based	DC-based	AC-based
Blocks of equations	12	25	12	25
Blocks of variables	12	87	12	87
Nonzero elements	1993	49300	4476	112781
Single equations	533	6684	1200	15289
Single variables	512	16153	1157	36994
Binary variables	68	68	156	156
Average elapsed time/simulation (min)	<1	~2	~4	~23

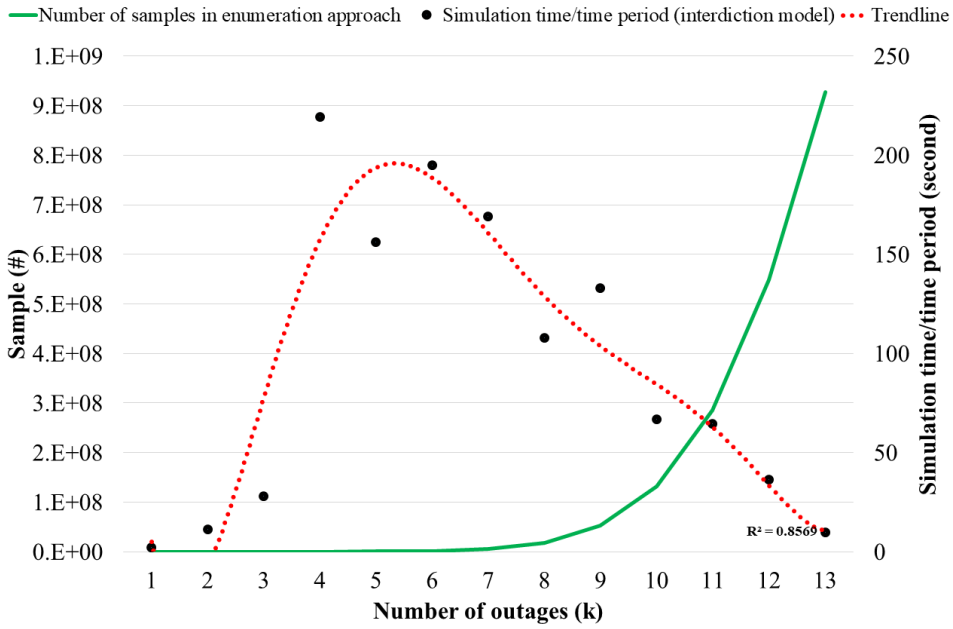

Figure 6-5. Comparing enumeration-based approach and this approach in the case of simulation time for the IEEE RTS network.

6-5-1 Accuracy of the lower-level problem and its strong duality

Before proceeding to implement the proposed method on the IEEE RTS network, the accuracy of the linearized ACOPF problem in the lower level and its dual problem are investigated. In doing so, the exact nonlinear ACOPF using MATPOWER package and proposed linearized ACOPF method are compared. The objective function for the ACOPF problem is introduced as the total operation cost of the generators in the form of $\sum_{i\in G} c_i Pg_i$ [313].

For the exact ACOPF and DCOPF models using MATPOWER package, the objective functions are 44196 \$/h and 41904 \$/h, respectively, whereas the objective function is found to be 44322 \$/h using the lower-level problem in this chapter. The results show an error of 5.2 % for the exact DC-OPF method and a very small error of 0.3 % for the linearized ACOPF in the lower-level problem. Furthermore, the objective function is found to be 44322 \$/h using its dual problem. This result demonstrates the strong duality in the problem where the optimal values of the primal and dual problems are equal [367].

6-5-2 Comparison between the proposed approach and the previous literature

The previous literature uses the DCOPF as the operator tool in the lower level problem whose objective is minimizing the damage consequences [346-348, 352-354]. It means that the

reactive power, variation of voltage magnitude, power losses, and the line resistance are ignored [331]. It also approximated the small angle. It considers that the differences of the voltage angle between the neighboring buses *i* and *j* are insignificant, that is, $\sin(\theta_{ij})\approx\theta_{ij}$ and $\cos(\theta_{ij})\approx1$ [324]. Hence, to derive the DC-based approach [346-348, 352-354] for a fair comparison, the equations (6-1)-(6-14) are revised based on the above assumptions. So, equations (6-5), (4-4), (6-9), (6-11) and (6-14) are ignored and equations (4-3) and (4-7) are reformulated based on the assumptions.

Then, both models are applied to the test cases. The results show that small differences in total load sheddings, lead to proposing different critical lines in the IEEE RTS network. For instance, when *k* is 8, the proposed approach and the previous approach [346-348, 352-354] find 6 similar critical lines (i.e., 7-8(l_{11}), 11-13(l_{18}), 12-13(l_{20}), 15-21(l_{25}, l_{26}), 16-17(l_{28}), 20-23(l_{36}, l_{37})) while they propose different lines (1-5(l_3), 12-23(l_{21})) and (9-12(l_{15}), 10-12(l_{17})), respectively as the 7th and 8th critical lines. In other words, the Jaccard similarity index (JSI) for these two sets of lines is 0.6 and the average JSI is 0.9 for this test case.

The effects of reactive power, losses, etc. are more highlighted in a network under stress (not in IEEE 24-bus [391]). So, IEEE 57-bus is selected as the second test case to compare both models. Figure 6-6 shows that the objective function (LS) of the previous method in all simulations are lower/equal and so, optimistic compared to the proposed AC-based approach. It presents the fact that restricting the available degrees of freedom (e.g., fixing voltages in DC-

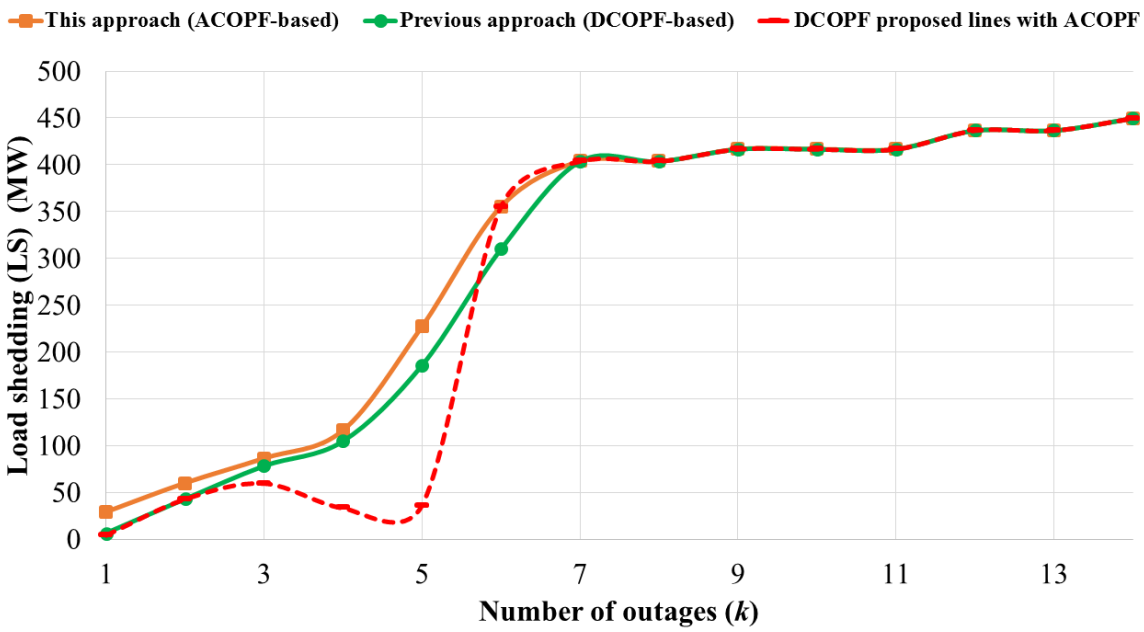

Figure 6-6. Load shedding for IEEE 57-bus as a function of number of outages (k).

based method) makes the solution less optimal and accurate [359]. Furthermore, the DC-proposed critical lines are tested with ACOPF. The results show that the critical lines are not the real critical lines. This phenomenon has clearly happened when *k* is 4 and 5. Figure 6-7 also shows five worst-case load shedding scenarios (*k*=1 to 5) and their related lines based on both models. In this network, the average JSI is about 0.6. Note that thanks to the proposed approach the calculated load shedding is more accurate (with the same *k* presents more damage) and also, it provides more precise information about the critical lines that is vital for planning and remedial actions.

6-5-3 Multi-period contingency analysis with daily peak loads

The system daily peak load of the IEEE RTS network (Figure 6-4) is used in the model to find out the effects of contingencies over a range of system demand levels (Figure 6-8). It should be noted when all lines are out of service, the system operator is forced to shed 1607 MW which

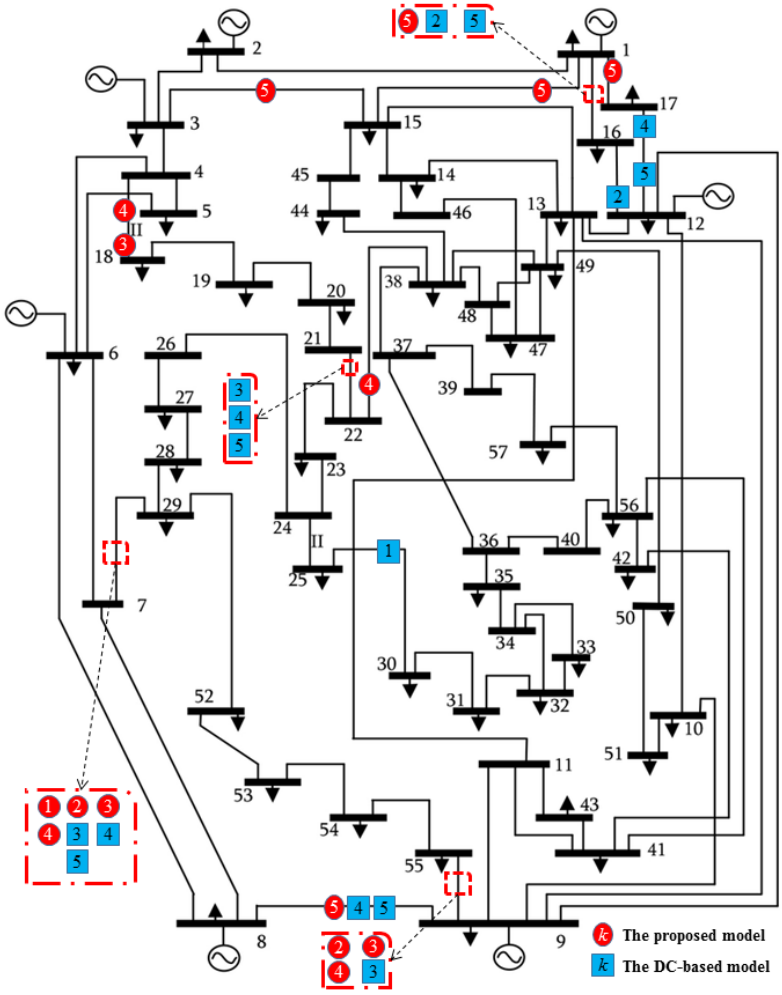

Figure 6-7. The IEEE 57-bus and optimal solutions for *k*=1 to 5 using both models.

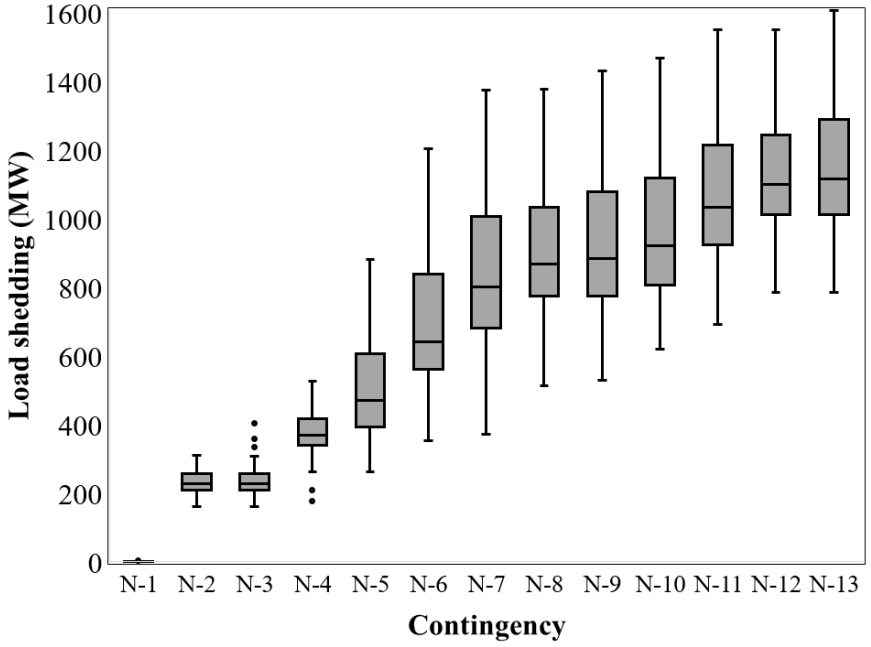

Figure 6-8. Effects of the contingencies with daily peak loads.

is 56% of total demands. The remainders are directly connected to the generators' buses. The method determined that this total possible system load is shed with only 13 simultaneous outages. In addition, the results show that the maximum damage is in midweek of the high-demand season while the minimum load shedding is on weekends of the low-demand season. The maximum damages sometimes don't change significantly with the increase of the outages e.g., maximum load shedding of *N*-7 comparing with *N*-8 or change significantly e.g., maximum load shedding of *N*-4 comparing with *N*-5 (68% increase). This point is very important in the intentional attack-based studies where the interdiction resources are limited. Last but not least, this network is not *N*-1 secure. However, it occurs only on the 352nd day of the year (see Figure 6-4). This is a hidden *N*-1 contingency using the previous approaches [23, 346] because the main reason is the dominant flow of reactive power in that area (lines connected to bus 6). Hence, the proposed approach helps the decision makers of the energy sector for long-term operation planning in the power system.

6-5-4 Multi-period contingency analysis with hourly peak loads

In the next step, this analysis is conducted similarly for the hourly peak loads of the 352nd day when the demands are the daily peak load of the year. Figure 6-9 shows the distribution of load shedding for the hourly peak loads of the 352nd day. The results show that the maximum damage is at around 5 to 7 p.m. while the minimum load shedding is at around 3 to 5 a.m. during the night. It is interesting to note that based on the used hourly peak loads, this network is not *N*-1

secure for hours between 4-7 p.m. when the hourly load profile (see Figure 6-4) has a peak. This information is essential for the decision makers of power system security sectors and operators making a robust and fast remedial action to protect the power system. Furthermore, operators can use this approach for a day-ahead steady-state security assessment.

The model allows having critical lines for each contingency and time. Table 6-2. Outcomes of the proposed model when the demand of the buses is the annual peak load. presents the critical lines and the consequences when the demand for the buses is the annual peak load. In this topology, the critical lines are the lines removing them leads isolating load buses in low-order contingencies (e.g., Figure 6-10(a)). With increasing k, the model tries to separate the generation zone from the load zone. The generation zone of this topology is in 230 kV area where the generation capacity is much more than the required demands. Figure 6-10 (b) shows that the lines l_7, l_{21}, l_{22}, and l_{23} are the critical lines where removing them separates two zones. In the higher order of contingency, the model suggests removing all of the efficacious lines between generation buses and demands. The efficacious lines are the lines that removing them increases the load shedding. For instance, line 27 in Figure 6-10(c) is not effective because the demand is much more than the generation capacity in bus n_{15}. On the contrary, bus n_{18} has much more generation capacity than the demand in the generation zone of Figure 6-10 (c). Therefore,

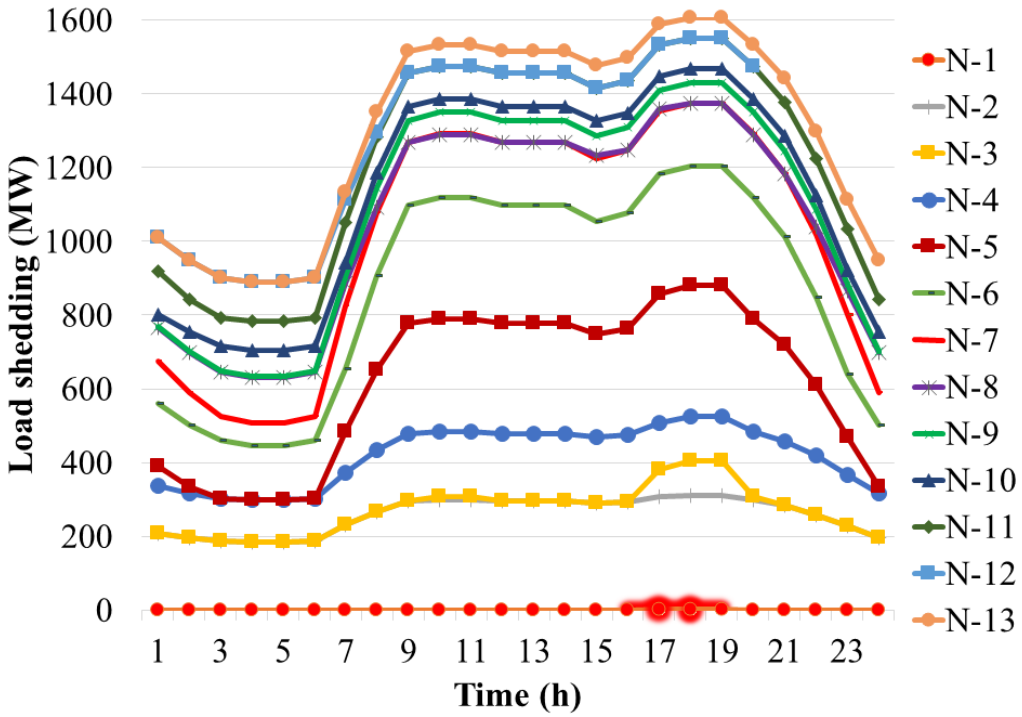

Figure 6-9. Effects of the contingencies with hourly peak loads.

removing lines in that zone is not effective. To summarize the results, according to the simulation results, the potential critical lines are radial lines (e.g., l_{11}), parallel lines (e.g., l_{25} and l_{26}, l_{36}, and l_{37}) and the lines connecting the generation to demand zones in a nearly centralized generation such as IEEE RTS.

Table 6-2. Outcomes of the proposed model when the demand of the buses is the annual peak load.

k	**Critical lines**	**Load shedding (MW)**	**Simulation time (Min)**
1	l_{10}	2	0.03
2	l_{29}, $(l_{36}, l_{37})^*$	309	0.19
3	l_{11}, $(l_{25}, l_{26})^*$, l_{28}	405	0.47
4	l_7, l_{21}, l_{22}, l_{23}	526	3.66
5	l_{21}, l_{22}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	883	2.60
6	l_{18}, l_{20}, l_{21}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	1204	3.25
7	l_{11}, l_{18}, l_{20}, l_{21}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	1374	2.82
8	l_3, l_{11}, l_{18}, l_{20}, l_{21}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	1377	1.80
9	l_{11}, l_{18}, l_{20}, l_{21}, l_{23}, l_{24}, $(l_{25}, l_{26})^*$, l_{29}, $(l_{36}, l_{37})^*$	1430	2.22
10	l_1, l_4, l_5, l_{11}, l_{15}, l_{17}, l_{18}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	1469	1.11
11	l_2, l_3, l_4, l_5, l_{11}, l_{15}, l_{17}, l_{18}, $(l_{25}, l_{26})^*$, l_{28}, $(l_{36}, l_{37})^*$	1552	1.07
12	l_2, l_3, l_4, l_5, l_{11}, l_{18}, l_{20}, l_{21}, $(l_{25}, l_{26})^*$, l_{28}, l_{29}, $(l_{36}, l_{37})^*$	1552	0.60
13	l_2, l_3, l_4, l_5, l_{11}, l_{15}, l_{17}, l_{18}, l_{23}, l_{24}, $(l_{25}, l_{26})^*$, l_{29}, $(l_{36}, l_{37})^*$	1607	0.16

* The lines in the parentheses are the parallel lines between two nodes.

6-6 Conclusion

A novel multi-period AC-based approach is presented to analyze *N-k* contingencies in order to enhance the resilience of a bulk power system under multiple outages. This method is based on the Stackelberg game theory which includes an upper level whose objective is to identify exactly *k* components to maximize the damage (load shedding) in the system and a lower level whose objective is mitigating the impacts of attacks and minimizing the damage consequences. Unlike the literature, in order to provide a more precise and real picture of the reactive power flow, losses as well as voltage profile, ACOPF is used in the lower-level problem as the operator's (defender's) tool. The resulting formulated problem is an AC-based bilevel MINLP problem in each time. To guarantee a globally optimal solution, The formulated problem is linearized and recast to the one-level MILP problem using the linearization techniques and the duality theory. The linearized ACOPF shows a very small error of 0.3% by assuming the predefined linearization parameters i.e., M=80 and n=64. The multi-period analysis is

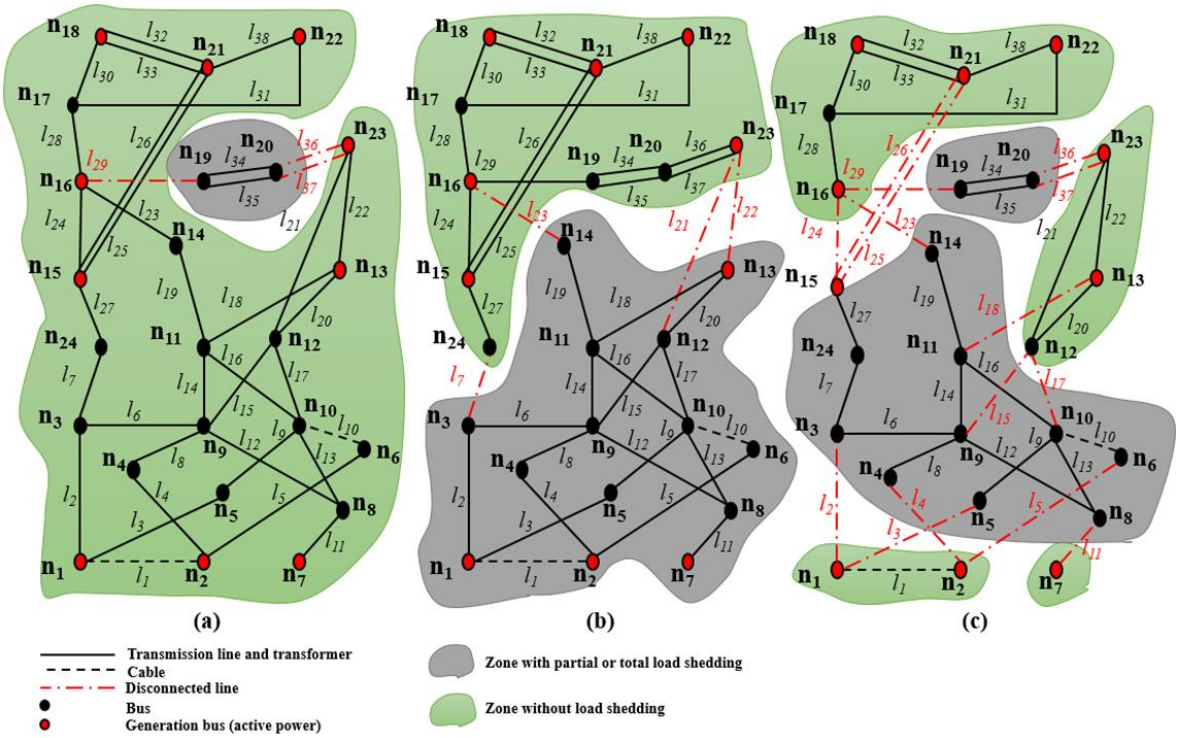

Figure 6-10. Topology of IEEE RTS under different contingencies, (a) *N*-2 (b) *N*-4 (c) *N*-13.

conducted with hourly and daily peak loads of the IEEE RTS. The method presents load shedding and the critical lines for each contingency over a range of system demand levels of this test system. Furthermore, the results show that in the congested systems especially where the reactive power flows predominate on some lines or buses such as cables or bus 6 in this case, the assessment cannot be adequately conducted only by the active power flows.

Chapter appendix: Nomenclature

Indices

i,j	Indices of buses
kc	Index of regular polygon for linearizing the circle
l	Index of lines
m	Index of blocks used for piecewise linearization

Sets

D	Set of all buses with a demand
G	Set of all buses with a generation
L	Set of all lines
NB	Set of all buses
T	Set of time (days or hours)

Constants

B	Big *M* parameter
C_i	cost coefficients of generators ($/MWh)
k	Number of outages (interdiction resources)
M	Number of blocks used for piecewise linearization
n	Number of sides of a regular polygon to formulate a circle
N	Number of assets
$Pg_i^{\max}$	Maximum magnitude of active power of generators at bus *i* (MW)
$Qg_i^{\max}$	Maximum magnitude of reactive power of generators at bus *i* (MVAR)
$Qg_i^{\min}$	Minimum magnitude of reactive power of generators at bus *i* (MVAR)
R(l)	Receiving bus of line *l*
S(l)	Sending bus of line *l*
$S_{ij}^{\max}$	Maximum magnitude of apparent power of line *ij* (MVA)
$V_i^{\max}$	Maximum magnitude of voltage magnitude at bus *i* (V)
$V_i^{\min}$	Minimum magnitude of voltage magnitude at bus *i* (V)
Y_{ij}	Admittance of line *ij* $(Y_{ij} = G_{ij} + jB_{ij})$
$\theta_{ij}^{\max}$	Maximum of voltage angle difference between bus *i* and *j* (Rad)
$\theta_{ij}^{\min}$	Minimum of voltage angle difference between bus *i* and *j* (Rad)
$\Delta\theta_{ij}$	Maximum of each block width for line *ij*

Variables

H_l, T_l	Two sets of continuous variables to linearize the product of binary and continuous dual variables
Ls_i^t	Active power load shedding at bus *i* (MW) in time *t*
Lsq_i^t	Reactive power load shedding at bus *i* (MVAR) in time *t*
P_{ij}^t	Active power flow of line *ij* (MW) in time *t*
Pg_i^t	Active power of generators at bus *i* (MW) in time *t*
Pd_i^t	Active power demand at bus *i* (MW) in time *t*
V_{it}	Voltage magnitude at bus *i* (V) in time *t*
Q_{ij}^t	Reactive power flow of line *ij* (MVAR) in time *t*
Qg_i^t	Reactive power of generators at bus *i* (MVAR) in time *t*
Qd_i^t	Reactive power demand at bus *i* (MVAR) in time *t*
Z / z_l^t	Upper level decision variable / Binary variable in time t that is equal to 0 if line *l* is out of service and otherwise, is equal to *1*
θ_{ijt}	Voltage angle difference between bus *i* and *j* (Rad) in time *t*
θ_{ijm}	Width of the mth angle block of line *ij* (Rad)
$\delta_{ij}^+, \delta_{ij}^-$	Positive variables used to eliminate the absolute function
$\lambda_{ij}, \mu_{ij}, \alpha_i, \overline{\omega}_i,$ $\beta_i, \overline{\delta}_i, \overline{\sigma}_i, \overline{\upsilon}_i, \xi_{ij},$ $\underline{\upsilon}_i, \eta_{1,ij} \cdots \eta_{n,ij}, \chi_{ij},$ $o_{ijm}, \varphi_{ij}, \kappa_{ijm}, \varepsilon_{ij}$	Dual variables that are shown on top of the corresponding equalities or inequalities

Chapter 7

Adaptive Robust Vulnerability Assessment of A Power System: A Trilevel OPF-based Optimization Approach

7-1 Introduction

Nowadays, more than ever, electricity has become a key commodity for any growing society. Any failure or destruction of its infrastructure has a considerable impact on safety, security, economy, health, and the well-being of a community [2]. For instance, three independent events in Iran, North America, and Italy hit a total of 128 million people in 2003. More recently, 670 million Indian people and 70 million Turkish people were temporarily deprived of electricity in 2012 and 2015, respectively [3-6]. In the USA, the annual cost of weather-related blackouts ranges from $20 to $55 billion [319]. Hence, the vulnerabilities of these power systems should be minimized to cope with several sources of disruption such as natural hazards, intentional attacks, and random failures [20].

Scientists have been developing innovative methods to assess the system vulnerability i.e. to determine critical components whose failures lead to the largest system loss [322]. These works can range from analytical approaches (such as complex network, flow-based, logical, and functional methods) to Monte Carlo simulations. Complex network analysis (CNA) [110] has

been developed recently for vulnerability analysis of several human-made infrastructures such as power systems and natural gas networks. In the pure CNA for a power system, each node represents a power-system bus and each edge represents a transmission line. The pure CNA neglects weight and direction and all the nodes and edges are identical [137]. In this context, several centralities are introduced such as flow betweenness centralities [138], delta centrality (or Δ centrality) [139], and combined degree–betweenness centrality [140]. The pure CNA also ignores the physical properties, electrical characteristics, and operational limits of power systems which limits the scope of the analysis [137, 147, 149]. Researchers have updated the "pure" centralities to the "extended" centralities in which some of the power system characteristics are taken into account. Some studies consider the physical resistance and impedance of lines and cables as the weight on the edges [17, 151]. Others introduce the reliability characteristics of transmission networks [152]. The P-Q network decomposition employs active power flow, the capacity of the generator, and the load [2, 137, 153]. The CNA originally ignores the physics of the power system operation, an issue that was partially overcome with extended CNA. Moreover, different power flow-based methods are developed for vulnerability analysis which can intrinsically and completely consider physical features of the power system [15, 194]. A detailed comparison of power-flow based methods and other novel approaches are recently conducted in [20, 23] (and the references therein).

Among the state-of-the-art approaches for the vulnerability assessment, the optimization-based approaches lead to promising results without the need to rank the sets of critical assets. The application of optimization-based approaches to the power system operation problems is considerably increasing, especially with the advent of advanced high-speed multiprocessors with large memory [340]. The interdiction model as a multilevel optimization problem is at the forefront of the models used to assess vulnerabilities [392, 393]. The interdiction model basically includes an upper-level problem whose objective is to identify critical components so as to maximize the damage (load shedding) in the system and a lower-level problem whose objective is mitigating the impacts of attacks and minimizing the damage consequences. The interdiction model is developed based on bilevel and trilevel programs. For instance, Karush-Kuhn-Tucker (KKT) optimality conditions [346] and duality theory [347] are used to convert a bilevel attacker-defender optimization problem to an equivalent one-level optimization problem. Arroyo J.M. [348] compared the KKT- and duality-based approaches by introducing minimum and maximum vulnerability models. Brown et al. [352] extended the classical bilevel interdiction model to a general trilevel defender-attacker-defender model to assign limited

defensive resources in power systems. Alguacil et al. [353] proposed an approach to allocate the defensive resources in a power system for mitigating the vulnerability. Wu et al [354] decomposed a planner-attacker-operator model into a master problem and a subproblem using a primal Benders decomposition method. Recently, Fang et al. [19, 394] and Che et al. [372] used this approach to identify the vulnerability of power systems exposed to natural hazards and the hidden *N-k* contingencies, respectively. Sayed et al. [356] use a trilevel optimization model and the nested column and constraint generation (NC&CG) algorithm to assess vulnerability in the integrated electric-gas system (IEGS). Also, an ACOPF-based bilevel optimization approach for vulnerability assessment of a power system and the multi-period vulnerability analysis of power systems under multiple outages are conducted in [25] and [24], respectively.

The above-surveyed literature ignored the uncertainty of parameters. Due to the increasing uncertainty caused by the dramatic increase of intermittent renewable energy sources (RESs) such as wind power [395], together with the load forecast errors, and price-responsive demands [396], the traditional security assessment may not provide a holistic and optimal solution for the power system operation under uncertainty [397]. However, such uncertainties may jeopardize the operational security of power systems. In order to guarantee the operational security of power systems with such uncertainties, developing security models and tools for immunizing the system against worst uncertainty realizations has attracted growing attention in recent years [398].

In the literature, there are essentially two approaches to tackle uncertainty in an optimization problem, namely, stochastic programming (SP) and robust optimization (RO) [399, 400] approaches. By employing SP and scenario-based approaches, we explore a few representative scenarios using the probability distributions. So, to obtain a high-quality solution, a large set of discrete scenarios is needed which may cause computational intractability if large systems are considered [401]. In contrast, the RO approach only defines the uncertainty in terms of bounded intervals using an uncertainty set, rather than a hard-to-obtain probability distribution of the uncertain data, and hence, the problem maintains at a moderate size [397, 402]. The RO approach immunizes the solution against all realizations of the uncertain data within a deterministic uncertainty set and hence that might be conservative in comparing with the SP approach. As the main aim of vulnerability analysis is to guarantee the supply of demands in all situations, a conservative solution is suitable for this type of problem [403].

The RO-based analysis has been attracting considerable attention for various applications in the power-system operation area. For instance, the RO-based analysis is used for expansion planning problems such as transmission network expansion planning under uncertainties of renewable generation and load [400, 404], coordinated investment in transmission and storage systems [402], the generation and transmission expansion planning [399]. It is also employed in finding the optimal unit commitment decision taking into account uncertainty (see these references as good examples: contingency-constrained unit commitment in [405], robust unit commitment with wind power and pumped hydro storage proposed in [406], an adaptive robust optimization (ARO) approach for unit commitment with recourse developed in [397], and finally an adaptive robust AC-based unit commitment model in [407]). Recently, a defender–attacker–defender model is proposed to deal with the power grid protection problem under uncertain attacks using the analytic hierarchy process [9]. Moreover, authors in [408] introduce several application areas where the ARO concepts are used.

Accordingly, in the current chapter, we propose a two-stage ARO model for the vulnerability analysis of power systems, where the first-stage, or the here-and-now decision, is the leader decision subject to a number of plausible outages (NPOs) and the second-stage, or the wait-and-see decision, is the dispatch decision which is robust against the worst case of all possible uncertainty realizations [409]. In doing so, the DC optimal power flow (DCOPF) is used in the lower-level defender problem. The uncertainty realization and the attacker model are modeled as the middle-level and the upper-level problems, respectively. The proposed trilevel model is a mixed-integer trilevel nonlinear program (MITNLP) that is non-convex and NP-hard [361]. To solve the proposed MITNLP model, we first replace the lower-level defender problem with its dual program using the duality theory. By replacing the lower-level problem with its dual program, the MITNLP is converted to a single-level mixed-integer nonlinear program (MINLP). The nonlinear terms in the MINLP model are then linearized using the Big-M technique [362]. We also prove a lemma which improves the computational tractability of our proposed final MILP model. This gives us the final mixed-integer linear program (MILP) which can be solved efficiently using state-of-the-art solvers such as the Cplex. The main contributions of the current chapter are summarized below:

1. An adaptive robust trilevel optimization model is introduced to assess the vulnerability of power systems. The proposed optimization model is robust against all possible realizations of uncertain power generations and load demands. Moreover, the level of robustness is controlled using physically-based budget constraints.

2. Since the proposed model is a MITNLP that is non-convex and NP-hard, an alternative MILP model is developed using the Big-M technique. We also prove a lemma which can be used to improve the computational tractability of our proposed final MILP model. The proposed final MILP model can be solved efficiently using off-the-shelf solvers such as Cplex. Numerical results using the IEEE 24-bus system and the modified model of Iran's transmission network show the promising performance of our proposed MILP model.

The remainder of this chapter is organized as follows. Section 7-2 introduces assumptions, the two-stage adaptive robust vulnerability assessment, and the uncertainty set. The formulation of the proposed trilevel optimization model will be presented in Section 7-3. Section 7-4 proposes the mathematical techniques to transform the original MITNLP model to an equivalent MILP model. We also prove a lemma which improves the computational tractability of our proposed final MILP model. Sections 7-5 presents the test cases and the numerical results. Concluding remarks are finally provided in Section 7-6.

7-2 Problem Description

7-2-1 Assumptions

For the sake of clarity, the main modeling assumptions in this chapter are summarized below [346-348, 352-354, 407]:

1. The uncertain parameters are the maximum power of generation units and bus loads. Furthermore, minimum up/down time constraints are not considered for simplicity.
2. The rational attacker has the intention to maximize the damage and disable multiple assets simultaneously and permanently or at least for several hours. As a result, if the attack is achieved, the power flow of other lines will be also affected.
3. We assume that the targeting assets are transmission lines and transformers, as they are usually reachable. For instance, transmission lines are out of the substation fences with low or no security to withstand. By removing the attacked transmission lines and their connected transformers, all loads which are only supplied by the attacked lines will be out of service.
4. Because two parallel circuits between the buses are usually on the same tower, they are modeled as a single line with double capacity.
5. Our proposed MILP models the steady-state security constraints following the attack. This chapter employs the DC optimal power flow (DCOPF) in the lower-level problem as the operator's (defender's) tool to mitigate the attack's adverse consequences.

6. The system damage is measured by the level of load shedding which is the amount of load that cannot be supplied due to the physical constraints of the power system. However, different objective functions of interest can be used in our MILP model to measure the system damage following an attack.

7-2-2 Uncertainty Characterization

A pivotal component of an ARO model is the definition of uncertainty set, which determines how much uncertainty is considered in the model [410]. In this chapter, we employ the most commonly used static uncertainty sets, i.e., the budget-based uncertainty set [397]. It is a polyhedral uncertainty set which assigns an interval for each uncertain parameter. Such uncertainty set is introduced by the following constraint [397, 407]:

$$\sum_{k=1}^{K}\left|\frac{\tilde{d}_k-\bar{d}_k}{\hat{d}_k}\right|\le\Delta;\ \ \tilde{d}_k\in[\bar{d}_k-\hat{d}_k,\bar{d}_k+\hat{d}_k] \tag{7-1}$$

Where $\tilde{d}_k$ is the k^{th} component of the uncertain-parameter vectors (the maximum power of generation units and bus loads) and K is the total number of buses that have uncertain power generation or load. The $\bar{d}$ is the expected value of the uncertain parameter, $\hat{d}$ is the variation from the expected value and Δ is the "budget of uncertainty". This inequality restricts the total variation of the uncertainty realization from the expected value [410]. When $\Delta=0$, for all nodes $\tilde{d}=\bar{d}$, which means no uncertainty is considered. With increasing the budget of uncertainty, the size of the uncertainty set enlarges. This means that the resulting robust solutions are more conservative considering a larger total deviation from the expected values and accordingly, the power system will be immunized against a higher degree of uncertainty [397]. When $\Delta=K$, the uncertainty set will be the entire hypercube defined by the intervals for each $\tilde{d}_k$. In this chapter, to model the uncertainty of both loads and power generations, two independent uncertainty sets are employed.

7-2-3 The Two-Stage Adaptive Robust Vulnerability Assessment

This chapter aims to assess the vulnerability of power systems capturing uncertainty in (renewable) power availability at generation units and in power consumption at load buses. From the safety point of view, the results of a model must be reliable in all circumstances, especially, with respect to uncertainties [409]. To ensure a robust and reliable result, an approach based on the RO is proposed for vulnerability analysis of power systems. The robust optimization approach determines a feasible solution to an optimization problem which is

optimal for the worse-case realization of the uncertain parameters within the uncertainty set [401, 409]. Figure 7-1 shows the two-stage nature of the decisions in our proposed model. In this model, a set of first-stage decisions are made before the realization of uncertainty (attacker's decisions) and a set of second-stage decisions are made once the uncertain parameters are revealed (defender's decision). Accordingly, our proposed model is *fully adaptive* to the specific realization of uncertainties. This two-stage model comprises three levels:

1. The upper level models the attacker as the leader prior to the uncertainty realization. The attacker maximizes the load shedding subject to the limited number of plausible outages.
2. The middle level represents the uncertainty realization in the worst possible manner within an uncertainty set, and thus it seeks to maximize the load shedding.
3. The lower level models the defender as the follower and reacts against the set of out-of-service assets to mitigate the attacker's adverse consequences considering the worse-case realization of uncertain parameters from the middle-level problem.

The proposed ARO-based vulnerability assessment for power systems is illustrated in Figure 7-1. In Section 7-3, the mathematical formulation of the proposed model as a mixed-integer trilevel nonlinear program (MITNLP) is presented. This formulation is based on the assumptions in Subsection 7-2-1. Then, this MITNLP is transformed into a single-level MILP in Section 7-4 using a series of proposed mathematical techniques [367].

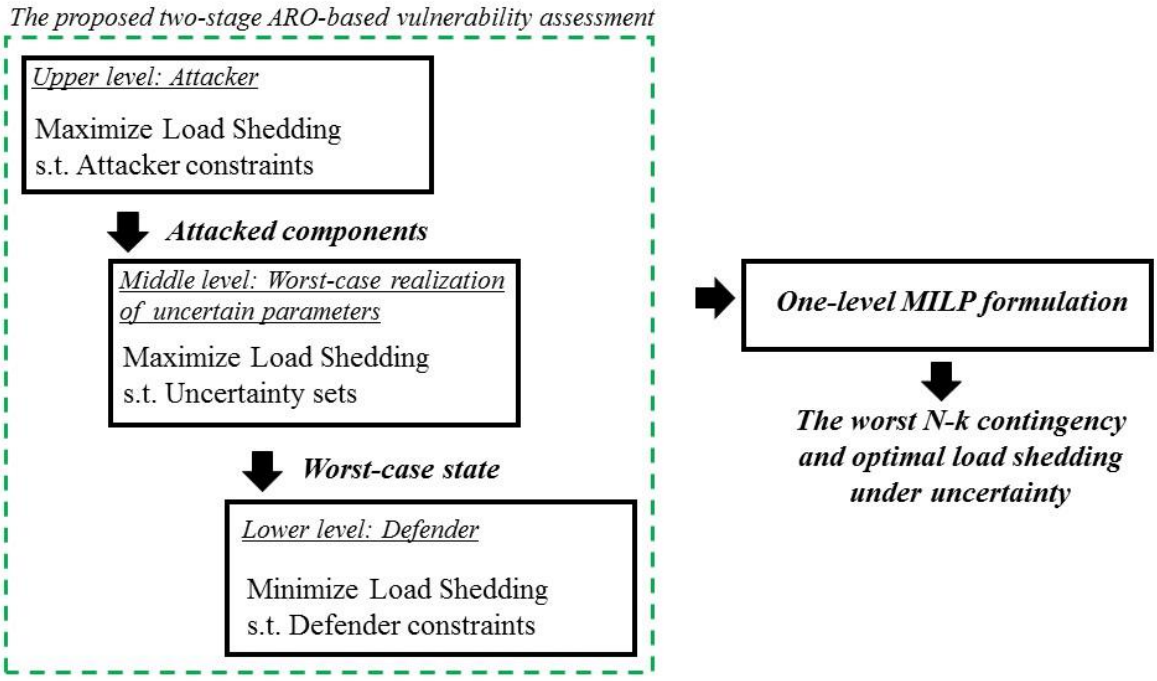

Figure 7-1. The proposed ARO-based vulnerability assessment for power systems in the current chapter.

7-3 The Adaptive Robust Attacker-Defender Problem

In this section, the mathematical formulation of the proposed adaptive robust attacker-defender problem is presented. This leader-follower interaction between the attacker and the defender considering the worse-case realization of uncertain parameters is modeled as the trilevel optimization problem (7-2)-(7-16). Dual variables associated with the constraints of the lower-level problem are shown inside parentheses.

$$\underset{Z}{Maximize} \sum_{i\in N} Ls_i^{**} \tag{7-2}$$

subject to: $$0.5\times \sum_{i,j\in N}(1-z_{ij}) = NPO; \quad z_{ij}\in\{0,1\} \quad \forall i,j\in N \tag{7-3}$$

$$z_{ij} = z_{ji}; \quad z_{ij}\in\{0,1\} \quad \forall i,j\in N \tag{7-4}$$

where: $$\sum_{i\in N} Ls_i^{**} \in \arg\left\{ \underset{\tilde{P}g,\tilde{P}d}{Maximize} \sum_{i\in N} Ls_i^{*} \right\} \tag{7-5}$$

subject to: $$\bar{P}g_i - \hat{P}g_i \le \tilde{P}g_i \le \bar{P}g_i + \hat{P}g_i; \quad \forall i\in G \tag{7-6}$$

$$\sum_{i\in G}\left|\frac{\tilde{P}g_i - \bar{P}g_i}{\hat{P}g_i}\right| \le DR^g; \quad \forall i\in G \tag{7-7}$$

$$\bar{P}d_i - \hat{P}d_i \le \tilde{P}d_i \le \bar{P}d_i + \hat{P}d_i; \quad \forall i\in D \tag{7-8}$$

$$\sum_{i\in D}\left|\frac{\tilde{P}d_i - \bar{P}d_i}{\hat{P}d_i}\right| \le DR^d; \quad \forall i\in D \tag{7-9}$$

where: $$\sum_{i\in N} Ls_i^{*} \in \arg\left\{ \underset{\substack{Pg,Ls,\\ P,\theta}}{Minimize} \sum_{i\in N} Ls_i \right\} \tag{7-10}$$

subject to: $$Pg_{i|i\in G} + Ls_{i|i\in D} - \tilde{P}d_{i|i\in D} = \sum_{j\in N} P_{ij}; \quad \forall i\in N:(\lambda_i) \tag{7-11}$$

$$P_{ij} = z_{ij}B_{ij}\theta_{ij}, \theta_{ij} = \theta_i - \theta_j; \quad \forall i,j\in N:(\mu_{ij}) \tag{7-12}$$

$$0 \le Pg_i \le \tilde{P}g_i; \quad \forall i\in G:(\bar{\gamma}_i) \tag{7-13}$$

$$-S_{ij}^{\max} \le P_{ij} \le S_{ij}^{\max}; \quad \forall i,j\in N:(\underline{\varphi}_{ij},\bar{\varphi}_{ij}) \tag{7-14}$$

$$-\theta_i^{\max} \le \theta_i \le \theta_i^{\max}; \quad \forall i\in N:(\underline{\omega}_i,\bar{\omega}_i) \tag{7-15}$$

$$0 \le Ls_i \le \tilde{P}d_i; \quad \forall i\in D:(\bar{\alpha}_i) \tag{7-16}$$

The optimization problem (7-2)-(7-16) comprises three optimization levels: (*i*) the upper level (7-2)-(7-4), which is associated with the attacker; (*ii*) the middle level (7-5)-(7-9), which

characterizes the worse-case realization of the uncertainties to maximize the damage; and (*iii*) the lower level (7-10)-(7-16), which models the system operator (i.e. defender) to mitigate the damage consequences. This problem is a mixed-integer trilevel nonlinear program (MITNLP) which is non-convex and NP-hard. Equations (7-3)-(7-4) models the limited number of plausible outages by the attacker. Since $z_{ij} = z_{ji}$, factor 0.5 is multiplied by the total number of line outages to avoid double consideration in our formulation. If z_{ij} is 0, the line *ij* is under attack, otherwise, it is safe.

As previously mentioned, two sources of uncertainty are considered in this chapter:

(*i*) The available generation capacity modeled as $\tilde{P}g_i$: The level of availability of power generation varies based on several conditions such as equipment failures or the weather conditions for renewable units [407]. Constraint (7-6) ensures that this level will be in an interval. The total deviations of the available capacities with respect to the expected ones are bounded in constraint (7-7) by the uncertainty budget for generation units DR^g;

(*ii*) The level of loads for the load buses modeled as $\tilde{P}d_i$: Constraints (7-8) and (7-9) introduce an interval and the total deviations of the available loads, respectively. To adjust the budget of uncertainty, we employ integer values which are the number of generation units and load buses for DR^g and DR^d, respectively.

In the lower-level defender problem (7-10)-(7-16), the DCOPF is used as the defender tool to mitigate the adverse consequences of the outages. Equation (7-10) is the objective function of the defender to minimize the damage. The asterisk in (7-2), (7-5), and (7-10) emphasizes that Ls_i is decided in the lower-level problem. Equation (7-11) is the nodal power-balance equation for active power. Equation (7-12) represents the line flow calculation. Constraints (7-13)-(7-14) enforce the limits of active power generation and transmission line capacity, respectively. The voltage angles are limited using (7-15). Furthermore, active load shedding is limited to the maximum available active load at each bus in (7-16). To solve our proposed MITNLP model (7-2)-(7-16), in the next section we transform the MITNLP to a MILP which is computationally more tractable than the original MITNLP. We then prove a lemma which improves the computational tractability of our proposed final MILP model. This final proposed MILP model is then solved using the off-the-shelf Cplex solver.

7-4 Solution methodology

In this section, the proposed MITNLP in the previous section is transformed to a single-level MILP using the "dualize-and-combine" technique in two steps: First, the lower-level min problem is recast to a max problem by the duality theory [411]; then the whole trilevel model is transformed to a single-level MILP using several proposed linearization techniques. We also prove a lemma which improves the computational tractability of our proposed final MILP model.

7-4-1 The lower-level problem and the duality theory

The duality theory states that every linear programming (LP) problem (the primal problem) has another LP problem (the dual problem) that can be derived from it. The dual problem will be a maximization problem when the primal problem is a minimization problem and vice versa. Furthermore, each variable (constraint) in the primal problem becomes a constraint (variable) in the dual problem [411]. The dual optimization problem of the LP problem (7-10)-(7-16) is derived below.

$$\underset{\substack{\lambda_i,\underline{\mu}_{ij},\alpha_i,\underline{\omega}_i,\\ \underline{\omega}_i,\gamma_i,\underline{\varphi}_{ij},\overline{\varphi}_{ij}}}{\underline{Maximize}}\left(\sum_{i\in N}(\lambda_i+\overline{\alpha}_i)\tilde{P}d_{i|i\in D}+\sum_{i\in G}\overline{\gamma}_i\tilde{P}g_i+\sum_{i,j\in N}(\overline{\varphi}_{ij}-\underline{\varphi}_{ij})S_{ij}^{\max}+\sum_{i\in N}(\overline{\omega}_i-\underline{\omega}_i)\theta_i^{\max}\right) \quad (7\text{-}17)$$

subject to:

$$-\lambda_i+\mu_{ij}+\underline{\varphi}_{ij}+\overline{\varphi}_{ij}=0;\quad \forall i,j\in N:(P_{ij}) \quad (7\text{-}18)$$

$$\lambda_i+\overline{\gamma}_i\le 0;\quad \forall i\in G:(Pg_i) \quad (7\text{-}19)$$

$$\sum_{\substack{i,j\in N\\ |S(ij)=i}} z_{ij}\mu_{ij}B_{ij}-\sum_{\substack{i,j\in N\\ |R(ij)=i}} z_{ij}\mu_{ij}B_{ij}+\underline{\omega}_i+\overline{\omega}_i=0;\quad \forall i,j\in N:(\theta_i) \quad (7\text{-}20)$$

$$\overline{\alpha}_i+\lambda_i\le 1;\quad \forall i\in D:(Ls_i) \quad (7\text{-}21)$$

$$\lambda_{ij}\ free,\mu_{ij}\ free,\overline{\gamma}_i\le 0,\overline{\varphi}_{ij}\le 0,\overline{\alpha}_i\le 0,\overline{\omega}_i\le 0,\underline{\omega}_i\ge 0,\underline{\varphi}_{ij}\ge 0;\quad \forall i,j\in N \quad (7\text{-}22)$$

Where the primal variables associated with the different constraints of the dual optimization problem are shown in parentheses.

7-4-2 Transforming the MITNLP to a single-level MILP

We first replace the LP problem (7-10)-(7-16) with its dual optimization problem derived in (7-17)-(7-22). Then, the optimization problem (7-2)-(7-16) is converted to a trilevel max-max-max problem. This trilevel max-max-max problem can be written equivalently as the single-level MINLP model in (7-23)-(7-34).

$$\underset{\substack{Z,\tilde{P}g,\tilde{P}d,\\ \lambda_i,\underline{\mu}_{ij},\overline{\alpha}_i,\overline{\omega}_i,\\ \underline{\omega}_i,\overline{\gamma}_i,\underline{\varphi}_{ij},\overline{\varphi}_{ij}}}{Maximize}\left(\sum_{i\in N}(\lambda_i+\overline{\alpha}_i)\tilde{P}d_{i|i\in D}+\sum_{i\in G}\overline{\gamma}_i\tilde{P}g_i+\sum_{i,j\in N}(\overline{\varphi}_{ij}-\underline{\varphi}_{ij})S_{ij}^{\max}+\sum_{i\in N}(\overline{\omega}_i-\underline{\omega}_i)\theta_i^{\max}\right) \quad (7\text{-}23)$$

subject to:

$$0.5\times\sum_{i,j\in N}(1-z_{ij})=NPO;\quad z_{ij}\in\{0,1\}\quad \forall i,j\in N \quad (7\text{-}24)$$

$$z_{ij}=z_{ji};\quad z_{ij}\in\{0,1\}\quad \forall i,j\in N \quad (7\text{-}25)$$

$$\bar{P}g_i-\hat{P}g_i\le\tilde{P}g_i\le\bar{P}g_i+\hat{P}g_i;\ \forall i\in G \quad (7\text{-}26)$$

$$\sum_{i\in G}\left|\frac{\tilde{P}g_i-\bar{P}g_i}{\hat{P}g_i}\right|\le DR^g;\quad \forall i\in G \quad (7\text{-}27)$$

$$\bar{P}d_i-\hat{P}d_i\le\tilde{P}d_i\le\bar{P}d_i+\hat{P}d_i;\quad \forall i\in D \quad (7\text{-}28)$$

$$\sum_{i\in D}\left|\frac{\tilde{P}d_i-\bar{P}d_i}{\hat{P}d_i}\right|\le DR^d;\quad \forall i\in D \quad (7\text{-}29)$$

$$-\lambda_i+\mu_{ij}+\underline{\varphi}_{ij}+\overline{\varphi}_{ij}=0;\quad \forall i,j\in N:(P_{ij}) \quad (7\text{-}30)$$

$$\lambda_i+\overline{\gamma}_i\le 0;\quad \forall i\in G:(Pg_i) \quad (7\text{-}31)$$

$$\sum_{\substack{i,j\in N\\ |S(ij)=i}}z_{ij}\mu_{ij}B_{ij}-\sum_{\substack{i,j\in N\\ |R(ij)=i}}z_{ij}\mu_{ij}B_{ij}+\underline{\omega}_i+\overline{\omega}_i=0;\quad \forall i,j\in N:(\theta_i) \quad (7\text{-}32)$$

$$\overline{\alpha}_i+\lambda_i\le 1;\quad \forall i\in D:(Ls_i) \quad (7\text{-}33)$$

$$\lambda_{ij}\ free,\mu_{ij}\ free,\overline{\gamma}_i\le 0,\overline{\varphi}_{ij}\le 0,\overline{\alpha}_i\le 0,\overline{\omega}_i\le 0,\underline{\omega}_i\ge 0,\underline{\varphi}_{ij}\ge 0;\quad \forall i,j\in N \quad (7\text{-}34)$$

The nonlinear terms in the MINLP model are $\lambda_i\tilde{P}d_{i|i\in D}$, $\overline{\alpha}_i\tilde{P}d_{i|i\in D}$, and $\overline{\gamma}_i\tilde{P}g_i$ (products of two continuous variables in (7-23)), $z_{ij}\mu_{ij}$ (products of integer and continuous variables in (7-32)) and absolute values in (7-27) and (7-29). Below, we propose different linearization techniques to linearize these nonlinear terms:

The nonlinear terms $\lambda_i\tilde{P}d_{i|i\in D}$, $\overline{\alpha}_i\tilde{P}d_{i|i\in D}$, and $\overline{\gamma}_i\tilde{P}g_i$:

For linearizing the bilinear terms in the objective function, we observe the following properties of the LP problem (7-17)-(7-22).

Property 1: ***The feasibility set of the LP problem (7-17)-(7-22) is independent from the $\tilde{P}g_i$ and $\tilde{P}d_i$.***

Property 2: ***The LP problem (7-10)-(7-16) is an always-feasible optimization problem.***

Now we define the polyhedron $U=\{\lambda_i,\mu_{ij},\overline{\alpha}_i,\overline{\omega}_i,\underline{\omega}_i,\overline{\gamma}_i,\underline{\varphi}_{ij},\overline{\varphi}_{ij}\,|\,(7-18)-(7-22)\}$. Using Property 1 and Property 2, no matter what the values of $\tilde{P}g_i$ and $\tilde{P}d_i$, the maximum over U of the objective function (7-17) occurs at the extreme points of polyhedron U. On the other hand, we know that U has a finite number of extreme points. If we denote the extreme points of U as u^p $(p=1,\ldots,n_p)$, the value function of LP problem (7-17)-(7-22) can be written as the following piecewise linear function:

$$VF(\tilde{P}g_i,\tilde{P}d_i)=Max\{\sum_{i\in N}(\lambda_i^p+\overline{\alpha}_i^p)\tilde{P}d_{i|i\in D}+\sum_{i\in G}\overline{\gamma}_i^p\tilde{P}g_i+\sum_{i,j\in N}(\overline{\varphi}_{ij}^p-\underline{\varphi}_{ij}^p)S_{ij}^{\max}+\sum_{i\in N}(\overline{\omega}_i^p-\underline{\omega}_i^p)\theta_i^{\max},\ p=1,\cdots,n_p\} \quad (7\text{-}35)$$

This means that the *VF(* $\tilde{P}g_i$ *,* $\tilde{P}d_i$ *)* is the pointwise maximum of a set of affine functions as shown in (7-35). Now, in Lemma 1 below, we show that the *VF(* $\tilde{P}g_i$ *,* $\tilde{P}d_i$ *)* is a convex function in $\tilde{P}g_i$ and $\tilde{P}d_i$.

Lemma 1: ***The VF(*** $\tilde{P}g_i$ ***,*** $\tilde{P}d_i$ ***) is convex and its maximum with respect to*** $\tilde{P}g_i$ ***and*** $\tilde{P}d_i$ ***occurs at the extreme points of*** $\tilde{P}g_i$ ***and*** $\tilde{P}d_i$ ***variables.***

Proof: The VF is the pointwise maximum of a set of convex (or affine) functions. And it is straightforward to show that the pointwise maximum of a set of convex functions is a convex function. Since, VF($\tilde{P}g_i$ *,* $\tilde{P}d_i$ *) is a convex function in* $\tilde{P}g_i$ *and* $\tilde{P}d_i$ *, its maximum with respect to* $\tilde{P}g_i$ *and* $\tilde{P}d_i$ *occurs at the extreme points of* $\tilde{P}g_i$ *and* $\tilde{P}d_i$ *variables* [412].

■

Figure 7-2 below shows a simple illustration of function *VF(* $\tilde{P}g_i$ *,* $\tilde{P}d_i$ *)* in two-dimensional space. The x represents a general one-dimensional decision variable. The actual value function, VF($\tilde{P}g_i$, $\tilde{P}d_i$) is an extension of the function in Figure 7-2 in the multi-dimensional space. The black lines represent the affine functions in (7-35), and the red line represents the final convex piecewise function.

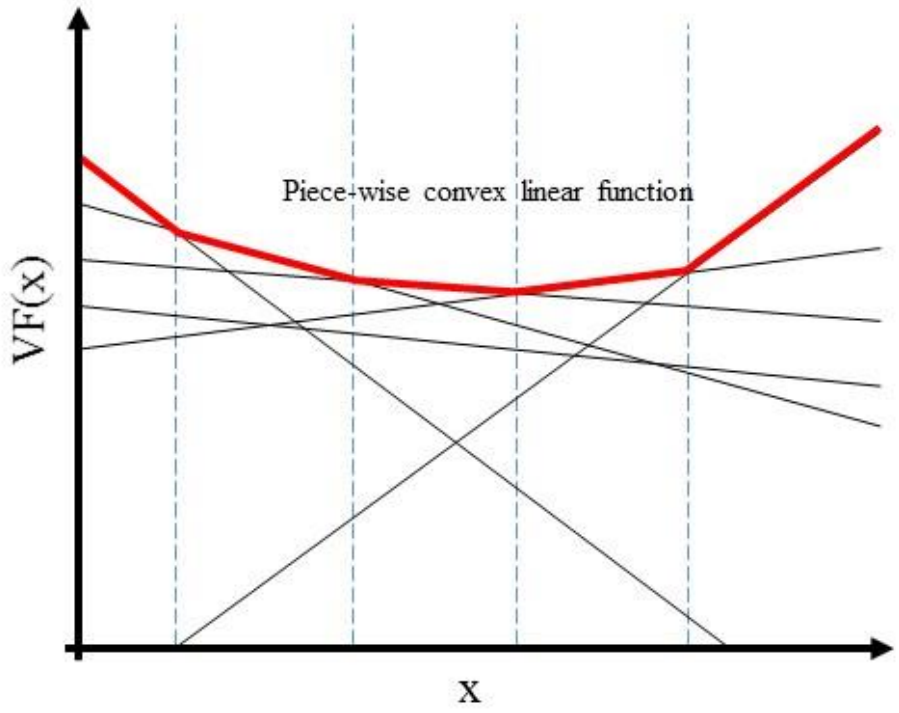

Figure 7-2. A simple illustration of value function $VF(\tilde{P}g_i, \tilde{P}d_i)$ in two-dimensional space.

By substituting (7-35) in our trilevel max-max-max problem, we have:

$$\underset{Z}{Maximize}\ \underset{\tilde{P}d,\tilde{P}g}{Maximize} VF(\tilde{P}d_i, \tilde{P}g_i) \tag{7-36}$$

As we can see in the lower-level optimization problem (7-36), we maximize a convex function $VF(\tilde{P}g_i, \tilde{P}d_i)$ over the box constraints $\bar{P}g_i - \hat{P}g_i \le \tilde{P}g_i \le \bar{P}g_i + \hat{P}g_i$ and $\bar{P}d_i - \hat{P}d_i \le \tilde{P}d_i \le \bar{P}d_i + \hat{P}d_i$. This means that the optimal solutions happen at the upper or lower bounds of these box constraints as discussed above. Accordingly, an optimal solution of the middle problem is when the uncertain parameters reach either upper or lower bounds. Using Lemma 1, we write the $\tilde{P}g_i$ and $\tilde{P}d_i$ variables using binary variables as follows [407]:

$$\tilde{P}g_i = \bar{P}g_i + \hat{P}g_i\beta_i^{g+} - \hat{P}g_i\beta_i^{g-} \tag{7-37}$$

$$\tilde{P}d_i = \bar{P}d_i + \hat{P}d_i\beta_i^{d+} - \hat{P}d_i\beta_i^{d-} \tag{7-38}$$

Where $\beta_i^{g+}, \beta_i^{g-}, \beta_i^{d+}, \beta_i^{d-} \in \{0,1\}$. Based on these equations, the uncertain parameters reach their upper bounds with $\beta_i^{d(g)+} = 1$, their lower bounds with $\beta_i^{d(g)-} = 1$or meets its forecasted value when $\beta_i^{d(g)+} = \beta_i^{d(g)-}$. By substituting (7-37) and (7-38) in the nonlinear terms $\lambda_i \tilde{P}d_{i|i\in D}$,

$\bar{\alpha}_i \tilde{P}d_{i|i\in D}$, and $\bar{\gamma}_i \tilde{P}g_i$, the bilinear terms $\lambda_i \beta_i^{d+}$, $\lambda_i \beta_i^{d-}$, $\bar{\alpha}_i \beta_i^{d+}$, $\bar{\alpha}_i \beta_i^{d-}$, $\bar{\gamma}_i \beta_i^{g+}$, and $\bar{\gamma}_i \beta_i^{g-}$ will appear.

The bilinear terms:

The bilinear terms $\lambda_i \beta_i^{d+}$, $\lambda_i \beta_i^{d-}$, $\bar{\alpha}_i \beta_i^{d+}$, $\bar{\alpha}_i \beta_i^{d-}$, $\bar{\gamma}_i \beta_i^{g+}$, and $\bar{\gamma}_i \beta_i^{g-}$ and the term $z_{ij}\mu_{ij}$ in constraint (7-32) can be linearized using two auxiliary variables T and H [353, 367, 368]. For instance, $T_{ij} = z_{ij}\mu_{ij}$ can be linearized as follows:

$$T_{ij} = \mu_{ij} - H_{ij} \tag{7-39}$$

$$-B_1 z_{ij} \le T_{ij} \le B_1 z_{ij} \tag{7-40}$$

$$-B_1(1-z_{ij}) \le H_{ij} \le B_1(1-z_{ij}) \tag{7-41}$$

Where, B_1 is a suitably large constant.

Absolute values in (7-27) and (7-29):

To linearize the general formulation of the budget-based uncertainty set in (7-1), the definitions in (7-37), and (7-38) are substituted in (7-1). So we will have:

$$\sum_{i\in G} \left| \beta_i^{g+} - \beta_i^{g-} \right| \le DR^g; \quad \forall i \in G \tag{7-42}$$

$$\sum_{i\in D} \left| \beta_i^{d+} - \beta_i^{d-} \right| \le DR^d; \quad \forall i \in D \tag{7-43}$$

Then, to remove the absolute value terms in (7-42) and (7-43), we can replace (7-42) and (7-43) with (7-44)-(7-45) and (7-46)-(7-47), respectively.

$$\sum_{i\in G} (\beta_i^{g+} + \beta_i^{g-}) \le DR^g; \quad \forall i \in G \tag{7-44}$$

$$\beta_i^{g+} + \beta_i^{g-} \le 1; \quad \forall i \in G \tag{7-45}$$

$$\sum_{i\in D} (\beta_i^{d+} + \beta_i^{d-}) \le DR^d; \quad \forall i \in D \tag{7-46}$$

$$\beta_i^{d+} + \beta_i^{d-} \le 1; \quad \forall i \in D \tag{7-47}$$

Where $\beta_i^{g+}, \beta_i^{g-}, \beta_i^{d+}, \beta_i^{d-} \in \{0,1\}$.

7-4-3 Our final proposed MILP model

Our final proposed MILP model for the vulnerability assessment of power systems under uncertainties is set out in (7-48)-(7-65) below.

$$\underset{\substack{Z,\bar{Pg},\hat{Pd},\lambda_i,\mu_{ij},\bar{\alpha}_i \\ ,\bar{\omega}_i,\underline{\omega}_i,\bar{\gamma}_i,\underline{\varphi}_{ij},\bar{\varphi}_{ij}}}{Maximize} \begin{pmatrix} \sum_{i\in N}\bar{P}d_{i|i\in D}(\lambda_i+\bar{\alpha}_i)+\sum_{i\in N}(\hat{P}d_{i|i\in D}T_{1i}-\hat{P}d_{i|i\in D}T_{2i}) \\ +\sum_{i\in N}(\hat{P}d_{i|i\in D}T_{3i}-\hat{P}d_{i|i\in D}T_{4i})+\sum_{i\in G}\bar{\gamma}_i\bar{P}g_{i|i\in G} \\ +\sum_{i\in G}(\hat{P}g_{i|i\in G}T_{5i}-\hat{P}g_{i|i\in G}T_{6i})+\sum_{i,j\in N}(\bar{\varphi}_{ij}-\underline{\varphi}_{ij})S_{ij}^{\max} \\ +\sum_{i\in N}(\bar{\omega}_i-\underline{\omega}_i)\theta_i^{\max} \end{pmatrix} \tag{7-48}$$

s.t.:

$$0.5\times\sum_{i,j\in N}(1-z_{ij})=NPO;\quad z_{ij}\in\{0,1\}\quad \forall i,j\in N \tag{7-49}$$

$$z_{ij}=z_{ji};\quad z_{ij}\in\{0,1\}\quad \forall i,j\in N \tag{7-50}$$

$$\sum_{i\in G}(\beta_i^{g+}+\beta_i^{g-})\le DR^g;\quad \forall i\in G \tag{7-51}$$

$$\beta_i^{g+}+\beta_i^{g-}\le 1;\quad \forall i\in G \tag{7-52}$$

$$\sum_{i\in D}(\beta_i^{d+}+\beta_i^{d-})\le DR^d;\quad \forall i\in D \tag{7-53}$$

$$\beta_i^{d+}+\beta_i^{d-}\le 1;\quad \forall i\in D \tag{7-54}$$

$$-\lambda_i+\mu_{ij}+\underline{\varphi}_{ij}+\bar{\varphi}_{ij}=0;\quad \forall i,j\in N \tag{7-55}$$

$$\lambda_i+\bar{\gamma}_i\le 0;\quad \forall i\in G \tag{7-56}$$

$$\sum_{\substack{i,j\in N\\ |S(ij)=i}}B_{ij}T_{ij}-\sum_{\substack{i,j\in N\\ |R(ij)=i}}B_{ij}T_{ij}+\underline{\omega}_i+\bar{\omega}_i=0;\quad \forall i,j\in N \tag{7-57}$$

$$\bar{\alpha}_i+\lambda_i\le 1;\quad \forall i\in D \tag{7-58}$$

$$T_{ij}=\mu_{ij}-H_{ij},-B_1z_{ij}\le T_{ij}\le B_1z_{ij},-B_1(1-z_{ij})\le H_{ij}\le B_1(1-z_{ij});\forall i,j\in N \tag{7-59}$$

$$T_{1i}=\lambda_i-H_{1i},-B_2\beta_i^{d+}\le T_{1i}\le B_2\beta_i^{d+},-B_2(1-\beta_i^{d+})\le H_{1i}\le B_2(1-\beta_i^{d+});\forall i\in D \tag{7-60}$$

$$T_{2i}=\lambda_i-H_{2i},-B_2\beta_i^{d-}\le T_{2i}\le B_2\beta_i^{d-},-B_2(1-\beta_i^{d-})\le H_{2i}\le B_2(1-\beta_i^{d-});\forall i\in D \tag{7-61}$$

$$T_{3i}=\bar{\alpha}_i-H_{3i},-B_3\beta_i^{d+}\le T_{3i}\le B_3\beta_i^{d+},-B_3(1-\beta_i^{d+})\le H_{3i}\le B_3(1-\beta_i^{d+});\forall i\in D \tag{7-62}$$

$$T_{4i}=\bar{\alpha}_i-H_{4i},-B_3\beta_i^{d-}\le T_{4i}\le B_3\beta_i^{d-},-B_3(1-\beta_i^{d-})\le H_{4i}\le B_3(1-\beta_i^{d-});\forall i\in D \tag{7-63}$$

$$T_{5i}=\bar{\gamma}_i-H_{5i},-B_4\beta_i^{g+}\le T_{5i}\le B_4\beta_i^{g+},-B_4(1-\beta_i^{g+})\le H_{5i}\le B_4(1-\beta_i^{g+});\forall i\in G \tag{7-64}$$

$$T_{6i}=\bar{\gamma}_i-H_{6i},-B_4\beta_i^{g-}\le T_{6i}\le B_4\beta_i^{g-},-B_4(1-\beta_i^{g-})\le H_{6i}\le B_4(1-\beta_i^{g-});\forall i\in G \tag{7-65}$$

The final proposed MILP model (7-48)-(7-65) can be solved using off-the-shelf solvers such as Cplex [369]. These solvers can efficiently solve our MILP model to the desired level of accuracy. They can also provide the optimality certificate of the solution. This is while the original MITNLP model is an NP-hard optimization problem with no guarantee of finding the global solution [340].

7-5 Numerical results

7-5-1 The IEEE 24-bus reliability test systems

The IEEE Reliability Test System (RTS) is used in this chapter. Data availability makes the IEEE RTS an ideal test case for bulk power system vulnerability analysis. It contains 24 buses, 32 generators, and 38 branches (lines and transformers) as shown in Figure 7-3. The transmission lines operate at two different voltage levels, 132 kV and 230 kV. The systems working at 230 kV and 132 kV are represented in the upper half and the lower half of Figure 7-3, respectively. Table 7-1 presents the generating unit characteristics, other detailed data of the systems can be found in [240].

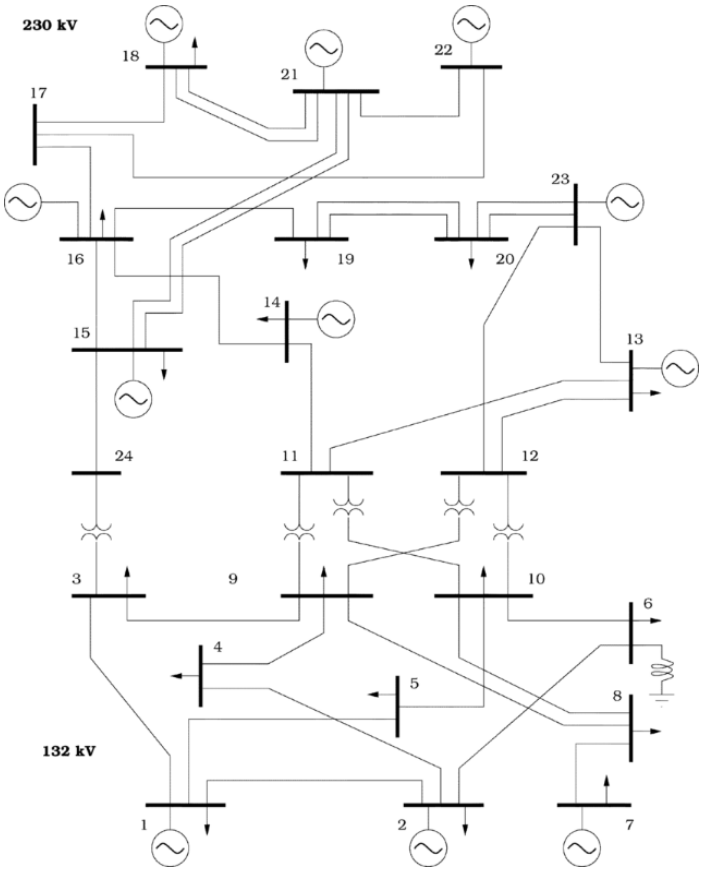

Figure 7-3. The topology of IEEE 24-bus reliability test systems (RTS).

Table 7-1. Generating unit characteristics

Generation units	Active power capacity (MW)	Connectivity to bus	Generation units	Active power capacity (MW)	Connectivity to bus
G1	40	1	G8	155	15
G2	152	1	G9	155	16
G3	40	2	G10	400	18
G4	152	2	G11	400	21
G5	300	7	G12	300	22
G6	591	13	G13	310	23
G7	60	15	G14	350	23

Our proposed MILP model has been successfully applied to the IEEE 24-bus reliability test system (RTS) [240]. The problems are solved on a laptop with a 2.2 GHz processor, and 8 GB of RAM. The Cplex solver in the GAMS (General Algebraic Modeling System) platform [413] is used to solve our proposed MILP model [372]. In all simulations, the Cplex relative optimality criterion was set at 0.001. Table 7-2 reports statistics regarding the size and complexity of the examined case comparing with the previous literature.

Four different scenarios are introduced in this chapter:

1. Vulnerability analysis without uncertainty ($DR^g = DR^d = 0$),
2. Vulnerability analysis with load uncertainty ($DR^g = 0, DR^d \geq 0$),
3. Vulnerability analysis with generation uncertainty ($DR^d = 0, DR^g \geq 0$),
4. Vulnerability analysis with both load and generation uncertainties ($DR^d \geq 0, DR^g \geq 0$).

Table 7-2. The size and complexity of the considered models for the IEEE RTS case measured by the number of equations and variables

Model statistics	Reference* [25]	This work**
Blocks of equations	12	46
Blocks of variables	12	28
Nonzero elements	1993	2979
Single equations	533	1046
Single variables	512	766
Binary variables	68	130

* This is based on the DCOPF-based bilevel optimization approach without considering the uncertainties.
** Our model has more variables and elements because it coonsiders uncertainties in its formulation.

Vulnerability analysis without uncertainty:

The proposed single-level MILP model is applied to the IEEE 24-bus network. The main aim is to check the model results with the results previously published [25, 346, 348] when we have no uncertainty, i.e. $DR^g = DR^d = 0$. Table 7-3 shows the six worst-case load shedding scenarios and their related critical lines for the IEEE 24-bus system. It shows that when $DR^g = DR^d = 0$, our model changes to the previous model when there is no uncertainty and our results are exactly the same as the reported results in [25, 346, 348].

Based on the simulation results for the IEEE 24-bus system, the potential critical lines are radial lines (e.g. line 7-8), parallel lines (e.g. lines 15-21 and 20-23), and the lines connecting the generation to demand zones (e.g. lines 11-13 and 12-13). It should be noted that when all lines are out of service, the system operator is forced to shed 1607 MW which is 56% of total demand [348]. As the remaining loads are directly connected to the generation units, our proposed MILP model shows that the maximum possible load shedding occurs with only 13 simultaneous outages.

Table 7-3. Six worst-case load shedding scenarios and their related lines for the IEEE 24-bus system without uncertainty

NPO	References [25, 346, 348]*		This work	
	Critical lines	LS (MW)	Critical lines	LS (MW)
1	-	0	-	0
2	16-19,20-23	309	16-19,20-23	309
3	7-8,15-21,16-17	387	7-8,15-21,16-17	387
4	3-24,12-23,13-23,14-16	516	3-24,12-23,13-23,14-16	516
5	12-23,13-23,15-21,16-17,20-23	872	12-23,13-23,15-21,16-17,20-23	872
6	11-13,12-13,12-23,15-21,16-17, 20-23	1198	11-13,12-13,12-23,15-21,16-17,20-23	1198

* Two parallel circuits are considered as two independent lines in references [346, 348].

Vulnerability analysis with load uncertainty:

The aim is to simulate the power system considering load uncertainty so as to assess vulnerability under load uncertainty. In order to consider the load uncertainty, the uncertainty budget for generation buses i.e. DR^g in our proposed model should be set to zero in all

simulations. Furthermore, we set the range of load variation to be $\hat{P}d_i = \alpha_i^d \bar{P}d_i, \forall i \in D$. In particular, in this case study we consider that α_i^d is always fixed at 0.05 (scenario I) and 0.1(scenario II) for all load buses. Moreover, the different uncertainty levels of the loads are tuned up by varying the uncertainty budget DR^d for load buses. It takes values in the range of zero (no uncertainty) to the total number of load buses (N(D) = 17).

The proposed one-level MILP problem is applied to the IEEE RTS case study. Figure 7-4 (a) shows the load shedding of the IEEE 24-bus system as a function of NPO (interdiction resources) under different load uncertainties. As can be seen in this figure, the optimal solutions or total load sheddings increase when DR^d increases and the maximum total load shedding occurs when DR^d is at its maximum value 17. Furthermore, we have compared the maximum difference of load shedding in comparison with the "no uncertainty" case when DR^d=17. Figure 7-4(b) shows that the maximum differences are 30% and 60% in scenarios I and II when NPO=3, respectively.

However, the load uncertainty is small which leads to proposing different critical lines in some NPOs. For instance, when NPO is 2, our proposed approach and the reported approach in [25, 346, 348] find similar critical lines (which are lines 16-19 and 20-23) under no uncertainty. This is while our approach proposes different lines (lines 15-21 and 16-17), in a higher level of uncertainty (for example when DR^d >6 in scenario I).

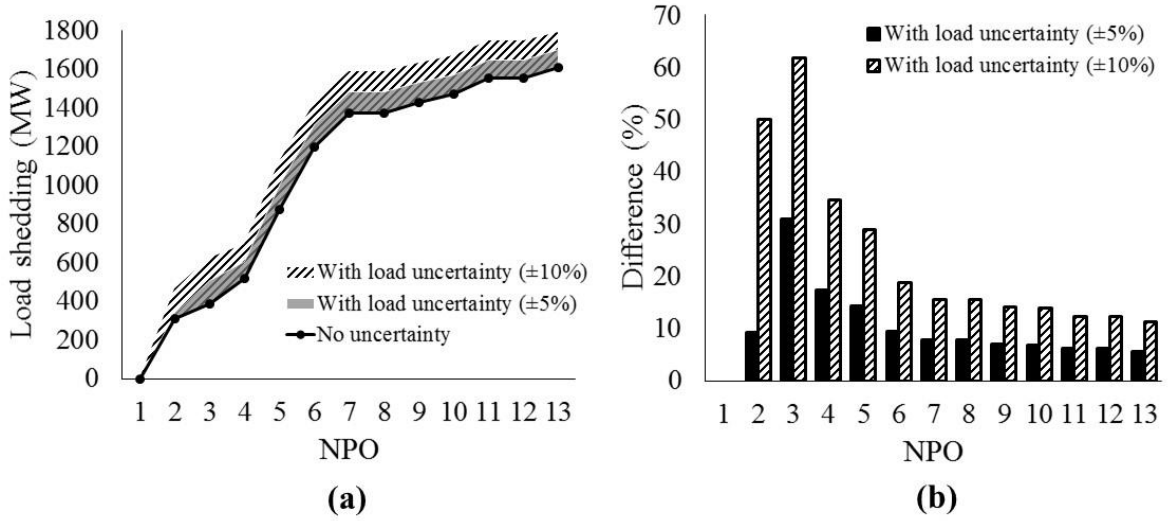

Figure 7-4. (a) Load shedding as a function of the number of outages (NPO) with and without load uncertainty (DR^d=0 (no uncertainty) to DR^d=17 (the most conservative case)), (b) Maximum difference of load shedding in comparison with "no uncertainty" case when DR^d=17.

Vulnerability analysis with generation uncertainty:

Similarly, the aim is to simulate the power system considering the uncertainty but only for the generation units. In order to consider the generation uncertainty, the uncertainty budget for load buses (DR^d) in our proposed model should be set to zero in all simulations. Furthermore, we set the range of generation variation to be $\hat{P}g_i = \alpha_i^g \bar{P}g_i, \forall i \in G$. In contrast to peak load variations, the peak generation capacity can deviate much more due to the failure of generation units or connected RES units. So, in this case study we consider that α_i^g is fixed at 0.2 (scenario III) and 0.5 (scenario IV) for all generation units. Moreover, the generation uncertainty levels are modeled by varying the uncertainty budget for generation units (DR^g). It takes values in the range of zero (no uncertainty) to the total number of generation units (N(D) = 14).

Our proposed MILP model is applied to the IEEE RTS case study. Figure 7-5(a) shows the load shedding of the IEEE 24-bus system as a function of NPO under different generation uncertainties. Similarly, this figure shows that the total load shedding increases when DR^g increases and the minimum total load shedding occurs in the no-uncertainty case and the maximum total load shedding occurs when DR^g is at its maximum value 14. Furthermore, Figure 7-5(b) shows that the maximum differences of load shedding between uncertainty case and no-uncertainty case reach approximately 118% and 342% in scenarios III and IV, respectively. With NPO = 1, the IEEE RTS case is "N-1" secure when there is no uncertainty.

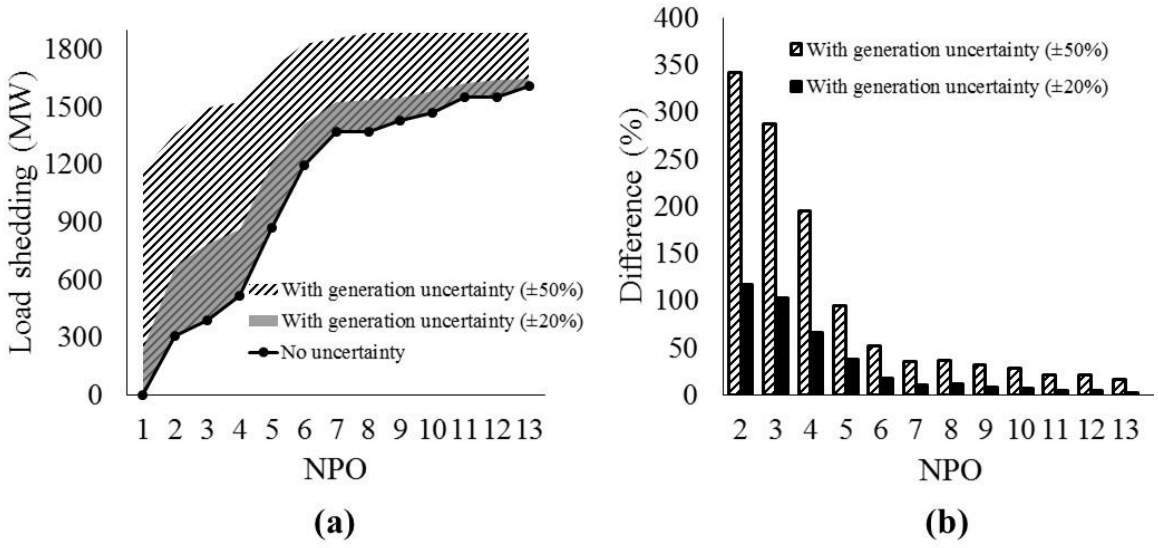

Figure 7-5. (a) Load shedding as a function of the number of outages (NPO) with and without generation uncertainty (DR^g=0 (no uncertainty) to DR^g=14 (the most conservative case)), (b) Maximum difference of load shedding in comparison with "no uncertainty" i.e. when DR^g=14.

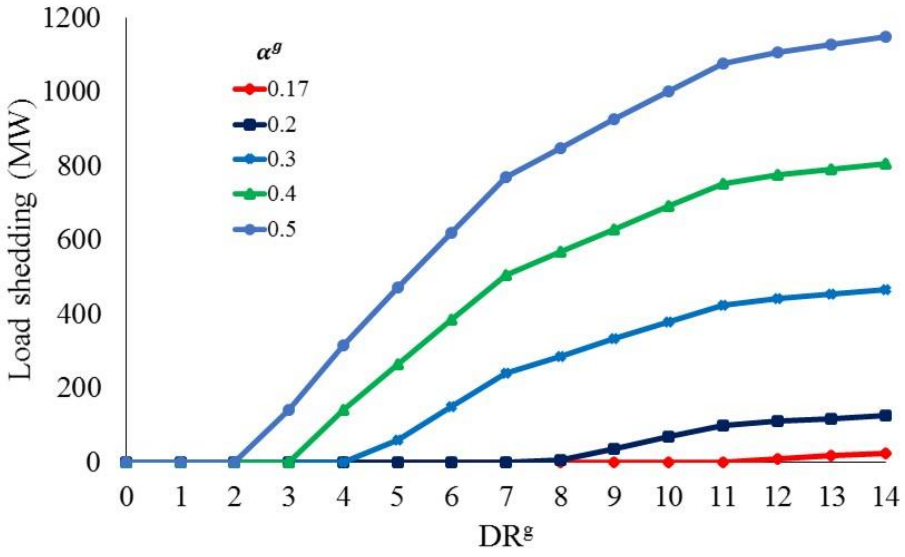

Figure 7-6. Load shedding as a function of DR^g when NPO=0.

But, the IEEE RTS case is not "N-1" secure when uncertainty increases in scenario III ($DR^g \geq 4$) and scenario IV ($DR^g \geq 1$), respectively. Note that when we set the NPO at zero the model considers the uncertainty of generation units. Figure 7-6 shows the load shedding as a function of DR^g when NPO = 0. As can be seen in this figure, the system has load shedding when α_i^g is larger than 17% (DR$^g \geq 11$). Similar to the load uncertainty, the generation uncertainty leads to proposing different critical lines in some NPOs.

Vulnerability analysis with both load and generation uncertainties:

Finally, both load and generation uncertainties are investigated. The proposed model is employed for different levels of uncertainty, which is modeled by varying the uncertainty budgets DR^d and DR^g. They take values in the range of zero (no uncertainty) to the total number of generation/load units which are 17 and 14 in this case study for load and generation units, respectively. Furthermore, we set the range of generation and load variations to be $\hat{P}g_i = \alpha_i^g \bar{P}g_i, \forall i \in G$ and $\hat{P}d_i = \alpha_i^d \bar{P}d_i, \forall i \in D$, respectively. We assume two scenarios. In scenario V, α_i^g and α_i^d are fixed at 0.2 and 0.05, respectively while for scenario VI, α_i^g and α_i^d are fixed at 0.5 and 0.1, respectively for all generation and load units.

Similarly, the proposed model is applied to the IEEE RTS case. Figure 7-7 and Figure 7-8 show load shedding as a function of DR^g and DR^d in scenarios V and VI, respectively. If we categorize the uncertain parameters involved in power system studies into two main groups

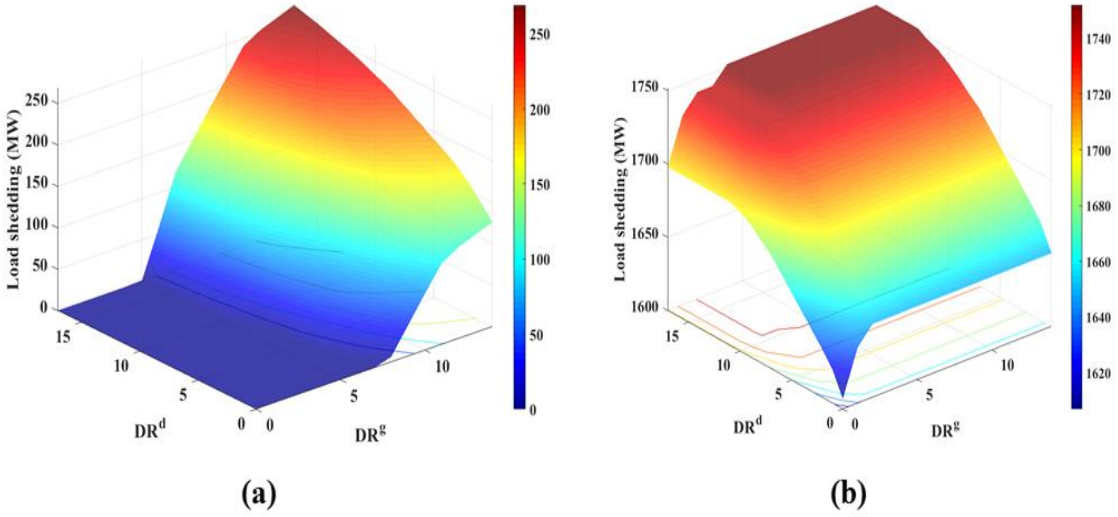

Figure 7-7. Load shedding as a function of DR^g and DR^d when (a) NPO=0 and (b) NPO=13 for scenario V.

[414], namely topological parameters (e.g. failure and forced outages) and operational parameters (e.g. demand and generation values), our model can address both uncertain parameters, simultaneously or independently.

Figure 7-7(a) and Figure 7-8(a) show that the IEEE RTS case is unreliable and unsafe even when we do not have any outage of the line (NPO = 0) for some of DR^g and DR^d. These figures present the worst-case scenarios that might be occurred due to solely uncertain operational parameters. As expected, the situation will be worse when we have line outages. Figure 7-7 (b) and Figure 7-8 (b) show the load shedding when we have 13 simultaneous outages. Moreover, Figure 7-7 (b) and Figure 7-8 (b) show that the minimum load shedding (1607 MW) is when we do not have uncertainty in generations and loads (when NPO=13) and maximum differences of load shedding when we have the maximum level of the uncertainties in comparison with "no uncertainty" case are 9% and 32% in scenarios V and VI, respectively.

The critical lines and components are presented in Table 7-4 and Table 7-5, respectively for scenarios V and VI. These tables show that increasing the level of uncertainty leads to higher load shedding levels and different critical lines in comparison with no uncertainty case (see Table 7-3). Moreover, based on the generation capacity and generation location in the network, some generation units and load buses with uncertainty play major roles in the worst-case scenarios. For instance, for scenario V and when $DR^g = DR^d = NPO = 1$, the uncertainty in generation unit G6 and load bus number 15 leads to a system which is not "N-1" secure.

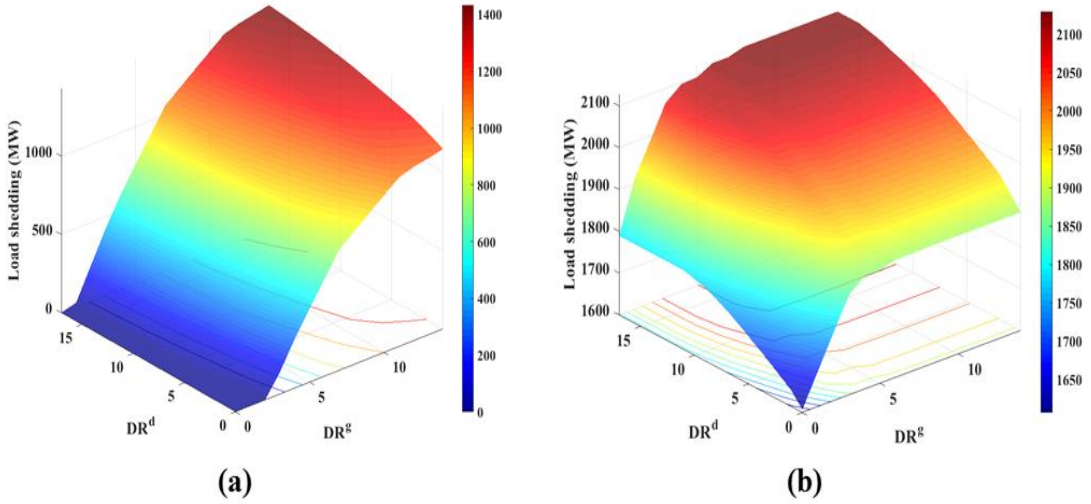

Figure 7-8. Load shedding as a function of DR^g and DR^d when (a) NPO=0 and (b) NPO=13 for scenario VI.

Table 7-4. Six worst-case scenarios and their related critical components for scenario V and when, $DR^g = DR^d =$ NPO

DR^g $=DR^d=$NPO	**Critical lines**	**Generation unit***	**Load bus number***	**LS (MW)**
1	-	-	-	0
2	15-21,16-17	G6,G14	13,15	429
3	7-8,15-21,16-17	G6,G13,G14	10,13,15	676
4	3-24,12-23,13-23,14-16	G2,G4,G5,G6	3,10,13,14	797
5	12-23,13-23,15-21,16-17,20-23	G4,G5,G6,G8,G9	10,13,14,15,19	1200
6	11-13,12-13,12-23,15-21,16-17,20-23	G2,G4,G5,G7,G8,G9	3,9,10,14,15,19	1455

* In these components, when the uncertain parameters reach the boundary of their intervals, the worst-case scenario occurs.

7-5-2 The Iran's 400-kV network

As a realistic test system, a modified Iran's 400-kV transmission network is used in this subsection. Iran's transmission network has voltage levels of 400 kV and 230 kV. The system is comprised of 52 buses, 28 generators, and 99 lines as shown in Figure 7-9. In this figure, the solid lines/circles are existing lines/substations and the dashed lines/circles are candidate 400-kV lines/substations which are planned to be added to the existing system as reported in [371]. The detailed data of this network can be found in [366, 371].

Table 7-5. Six worst-case scenarios and their related critical components for scenario VI and when, $DR^g = DR^d = NPO$

$DR^g = DR^d = NPO$	Critical lines	Generation unit*	Load bus number*	LS (MW)
1	15-21	G6	15	39
2	15-21,16-17	G6,G14	13,15	741
3	7-8,15-21,16-17	G6,G13,G14	10,13,15	1090
4	7-8,15-21,17-22,18-21	G6,G10,G13,G14	10,13,15,18	1257
5	12-23,13-23,15-21,16-17,20-23	G4,G5,G6,G8,G9	10,13,14,15,19	1664
6	12-23,13-23,15-21,17-22,18-21,20-23	G2,G5,G6,G8,G9,G10	10,13,14,15,18,19	1830

* In these components, when the uncertain parameters reach the boundary of their intervals, the worst-case scenario occurs.

Our proposed MILP problem is applied to the modified Iran's 400-kV transmission network. In this subsection, DR^d and DR^g take values in the range of zero (no uncertainty) to the total number of generation units and load buses which are 28 and 48, respectively. Furthermore, we set the range of generation and load variations to be $\hat{P}g_i = \alpha_i^g \bar{P}g_i, \forall i \in G$ and $\hat{P}d_i = \alpha_i^d \bar{P}d_i, \forall i \in D$, respectively. We assume α_i^g and α_i^d are fixed at 0.2 and 0.05 for all generation and load units, respectively. Moreover, the impact of the uncertainties on the vulnerability analysis is investigated for both existing and expanded networks.

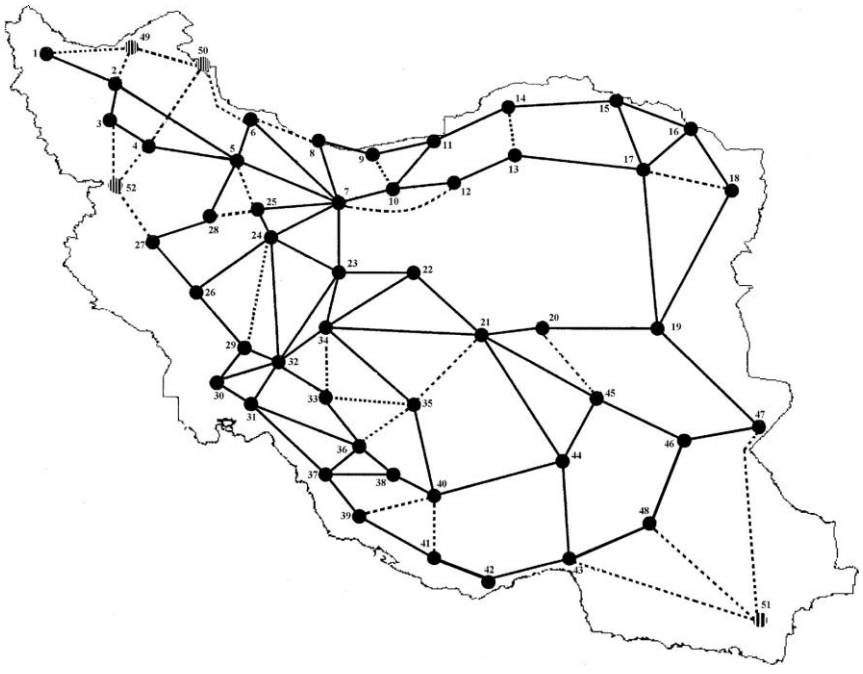

Figure 7-9. Modified Iran's 400-kV transmission network, existing lines/substations are black solid lines/ nodes and the candidate lines/ substations are black dash lines/nodes.

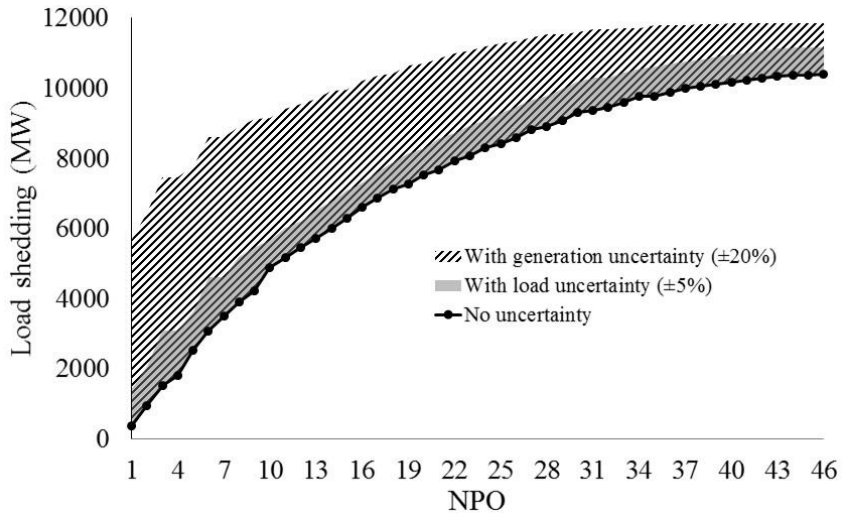

Figure 7-10. Load shedding as a function of NPO considering different uncertainties in the existing network (DR^d=DR^g=0 (no uncertainty) to DR^g=28 and DR^d=48 (the most conservative case)).

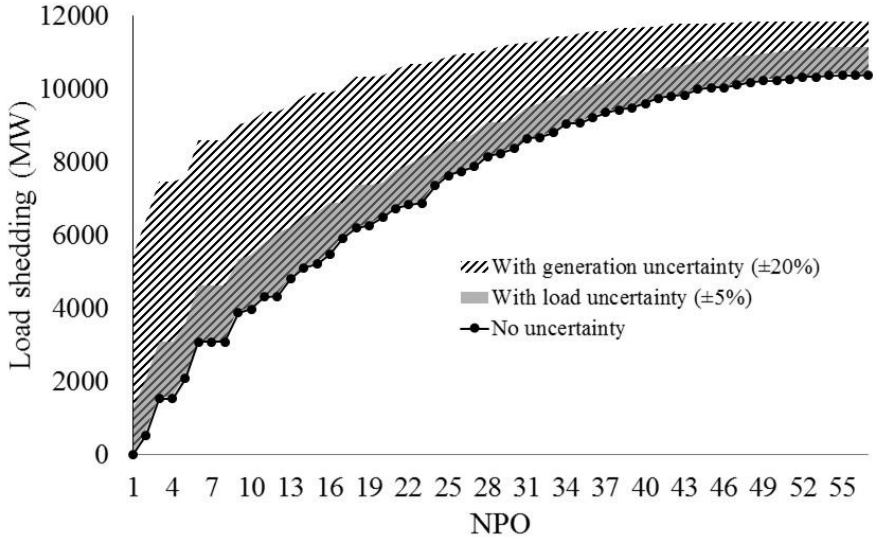

Figure 7-11. Load shedding as a function of NPO considering different uncertainties in the expanded networks (DR^d=DR^g=0 (no uncertainty) to DR^g=28 and DR^d=48 (the most conservative case)).

Figure 7-10 and Figure 7-11 show the imposed load shedding as a function of NPO in the two modeled topologies considering the uncertain parameters. As expected, the expanded network operates more reliable and robust than the existing network. For instance, when there is no uncertainty, the expanded network is N-1 secure and the total possible load shedding of 10390 MW will occur with more simultaneous line outages (as compared to the number of line outages in the existing network). Moreover, for a given NPO the load shedding in the expanded network is lower than the one for the existing one.

Figure 7-11 also highlights that the expanded network might be no longer N-1 secure when there are uncertain load and/or generation units. Finally, the proposed set of critical lines is also different. For example, when NPO = 1, line 1-2 is a critical line for the existing network but considering the uncertainty and the most conservative case, the critical line will change to line 30-31.

7-6 Conclusion

This chapter proposes a three-level optimization problem for power system vulnerability assessment in the context of system uncertainty. A robust optimization approach has been proposed. In our proposed model, the upper-level program represents the attacker, the middle-level program models the worst-case uncertainty level, and finally, the lower-level program represents the defender. The proposed model is a mixed-integer trilevel nonlinear program (MITNLP) which is hard to solve. Using the duality theory of the linear programs, the lower-level LP problem is replaced by its dual program. Then the original MITNLP problem is transformed to a max-max-max problem which can be written as a single-level mixed-integer nonlinear program (MINLP). The nonlinear terms in the MINLP model are handled using the Big-M linearization technique. We also observe two properties of our MITNLP model and prove a lemma that improves the computational performance of our proposed final MILP model. The proposed final MILP model has been applied to the IEEE 24-bus network and the modified Iran's transmission network and the simulation results are carefully studied. Our simulation results show that the power system vulnerability assessment without considering uncertainties leads to optimistic results. Moreover, increasing the level of uncertainty in our case studies leads to higher levels of load shedding and different critical lines in comparison with no uncertainty case. An interesting future direction is to explore how our proposed MILP model can be adjusted to accurately model the asymmetric uncertainties.

Chapter appendix A: Nomenclature

Indices

i,j	Indices of buses
k	Indices of buses that have uncertain power generation/load

Sets

D	Set of all buses with demand
G	Set of all buses with generation
K	Set of buses that have uncertain power generation/load
N	Set of all buses

Constants

B	A suitably large constant
$\bar{d}$	The expected value of the uncertain parameter
$\hat{d}$	Variation from the expected value
DR^g	The budget of uncertainty for generation buses
DR^d	The budget of uncertainty for load buses
NPO	Number of plausible outages (interdiction resources)
$\bar{P}d_i$	The expected value of the active load at bus *i* (MW)
$\hat{P}d_i$	Variation from the $\bar{P}d_i$ (MW)
$\bar{P}g_i$	The expected value of the active-power generation at bus *i* (MW)
$\hat{P}g_i$	Variation from the $\bar{P}g_i$ (MW)
R(ij)	Receiving bus of line *ij*
S(ij)	Sending bus of line *ij*
$S_{ij}^{\max}$	Maximum of apparent-power magnitude for line *ij* (MVA)
B_{ij}	Susceptance of line *ij* (p.u.)
$\theta_i^{\max}$	Maximum of voltage angle at bus *i* (Rad)
Δ	Budget of uncertainty

Variables

$\tilde{d}$	Uncertain variable
Ls_i	Active-power load shedding at bus *i* (MW)
P_{ij}	Active power-flow of line *ij* (MW)
Pg_i	Active power of generator at bus *i* (MW)
$\tilde{P}g_i$	Uncertain active power of generator at bus *i* (MW)
Pd_i	Active power demand at bus *i* (MW)

$\tilde{P}d_i$	Uncertain active power demand at bus *i* (MW)
T, H	Auxiliary variables to linearize the product of binary and continuous variables
Z / z_{ij}	Upper-level decision variable: the binary variable that is equal to 0 if line *ij* is out of service and otherwise, is equal to 1
θ_{ij}	Voltage-angle difference between bus *i* and *j* (Rad)
$\beta_i^{d+}, \beta_i^{d-}, \beta_i^{g+}, \beta_i^{g-}$	Binary variables
$\lambda_i, \mu_{ij}, \overline{\alpha}_i, \overline{\omega}_i, \underline{\omega}_i, \overline{\gamma}_i, \underline{\varphi}_{ij}, \overline{\varphi}_{ij}$	Dual variables associated with their corresponding constraints

Chapter appendix B: The model performance

Before observing the properties of the model and using the extreme points, we applied the binary expansion method [364, 415] to linearize the bilinear terms. The results (see Table 7-6) demonstrate that our approach significantly decreases the computational requirements. As can be expected, a major improvement is when both uncertainty parameters are considered i.e. scenarios V and VI.

Table 7-6. The size and complexity of our proposed model for different approaches used to linearize bilinear terms and the budget-based uncertainty set

Model statistics		**Binary expansion formulation**	**Extreme points**
Single equations		3121	1046
Single variables		1906	766
Binary variables		409	130
Average elapsed time/simulation (sec)*	scenario I	5.2	0.9
	scenario II	11.2	0.8
	scenario III	7.4	2.1
	scenario IV	2.8	0.7
	scenario V	553	3.0
	scenario VI	471	2.1

*In all scenarios, NPO is fixed to 13.

Chapter 8

Overall Conclusions and Future Works

In this chapter, we first provide a short overview of the research, followed by a summary of the main results, and finally some suggestions for future research.

8-1 Overview of the research

Several research questions motivated this work and to address those challenging questions novel computational frameworks, dedicated to analyze and quantify the vulnerability of the power system have been proposed in each chapter. The general objective of the thesis was to study and develop advanced modeling, simulation, analysis, and optimization methods for the vulnerability analysis of the power systems in order to proactively and properly protect, and mitigate such vulnerability when they suffered from low-probability high-consequence failures.

The above-stated objectives are addressed in three parts. Part one introduced the different definitions of vulnerability and reviewed and compared the previous methods. Part two found out the acceptable level of assumptions and available data to answer the reliability, vulnerability, and resilience questions. Afterward, the cascading failures and domino effects are addressed and finally, a framework for the integration of security methods capable of viewing the problem from different perspectives e.g. integrating reliability and vulnerability analyses is developed. The last part introduced and developed a hierarchical leader-follower problem where the upper level (leader) trying to maximize the damage with a limited interdiction budget

(e.g., outage of lines), and the follower (operator) trying to minimize the probable consequences. Thanks to this rational strategy, the critical components whose failures lead to the largest system loss can be determined. Then, the proposed model is extended to be used as a multi-period model and furthermore, as a model which is immunized against worst uncertainty realizations. All of the proposed models in Parts two and three are developed in MATLAB (using the open-source MATLAB based simulation package, MATPOWER) and the GAMS platform.

8-2 Summary of our approaches and achievements

The aim of this thesis was to address two main questions, i.e. (*i*) the systemic vulnerabilities of the power system under multiple contingencies and different operational uncertainties; (*ii*) the critical components which must be protected or fortified when the protective and financial resources are limited. Therefore, to accomplish these goals different methodologies and approaches are introduced in the previous chapters. The main achievements are given below.

In Chapter 2, we summarized 100 papers and reviewed about 300 articles. This chapter highlighted the advantages and disadvantages of the standard methods in the vulnerability analysis. It shows that no modeling approach can investigate all aspects of this field. In fact, the appropriate model depends on the type of event and the specific case study. We also focused on three classes of events, namely natural hazards, intentional attacks, and random failures that will help to determine the relevant application of the various methods available, including emerging methods.

In Chapter 3, the main aim was to compare two important security concepts, which are vulnerability and reliability assessments. Moreover, a novel methodology was developed for the joint consideration of vulnerability and reliability of power systems using multi-criteria decision-making (MCDM). Reliability and vulnerability assessment study the ability of a system to perform its desired functions under certain conditions for a given period and the weakness level of a system to failures, disasters or attacks, respectively. We presented that reliability assessment is dependent on the probability of component failure but systemic vulnerability assessment does not consider the probability. Another difference is the different number of simultaneous failures that both techniques take into account. Moreover, the results show that the percentage of simultaneous failures decreases when the dimension of the network increases, and reliability analysis only considers a maximum of 10.6% of the component outages in the IEEE test case. Therefore, the vulnerability assessment can complement the reliability analysis considering the rest of the N-k failures.

The capacity-based assessments such as vulnerability, reliability and contingency assessment need iterative power flow-based approaches to model the power system behavior. The main aim of Chapter 4 was to thoroughly investigate the effects of the DC power flow assumptions in our respective fields. Then, we tried to figure out the sources of inaccuracy in power flow-based models of different line capacity-based assessments. Moreover, different scenarios such as N-k′-1 contingency, cascading failure are modeled and a new index was introduced. The results presented that the related indices are very sensitive to the line capacity limits. Hence, DCM can lead to optimistic and inaccurate predictions in reliability. Furthermore, special care should be taken whenever DCM is used for the planning and operating of power systems.

The third part of the thesis introduced and developed the multilevel optimization-based approaches for the vulnerability analysis of the power systems. In these approaches, the upper level models the attacker, and the lower level models the defender. The attacker as the leader starts the leader-follower game with limited disruptive resources. The defender as the follower reacts against the set of out-of-service assets to mitigate its adverse consequences. This leader-follower rational interaction between the attacker and the defender presents the worst-case scenarios and the critical components, which their outages lead to major consequences.

The main idea of Chapter 5 was to develop an approximation model of the original AD problem. We were not intending to solve the original non-convex MIBNLP problem, which is NP-hard. The original MIBNLP problem has two main difficulties to be efficiently solved: (1) The non-convex ACOPF problem of the defender in the lower level: The ACOPF is an NP-hard non-convex optimization problem with no guarantee of finding the global optimal solution; (2) The AD model is a bilevel optimization problem with both binary variables and non-linear constraints. Solving a bilevel optimization problem with binary variables, nonlinear terms, and a non-convex lower-level problem is an extremely challenging mathematical exercise.

Accordingly, in this context, the literature proposes two ways to approach these types of problems: (1) approximation techniques and (2) the relaxation techniques. We have adopted the approximation techniques to solve the original MIBNLP problem. We have not done any approximation for the upper-level problem. Therefore, the upper-level solution from the approximation is also valid for the original problem. The main approximation is performed in the lower-level problem where we have replaced it with an LP. If our approximation assumptions are valid, then our approximate solution is also feasible for the original ACOPF.

We can broadly categorize the solution algorithms for bilevel optimization problems as (1) direct solution algorithms, (2) metaheuristic algorithms, and (3) single-level reformulation algorithms. The third approach is widely used in the relevant literature to solve the bilevel optimization problems. We have also adopted this approach in Chapters 6 and 7. We first approximated the lower-level problem by an LP model. Then using the duality theory the whole AD model is transformed to a tractable MILP which can be solved using efficient off-the-shelf solvers such as Cplex.

The most innovative part of Chapter 5 is to bring the ACOPF formulation into the power system vulnerability assessment models. As a result, our ACOPF-based vulnerability model is far more practical than current DCOPF-based vulnerability models existing in the relevant literature. By bringing the ACOPF formulation into our proposed model, we clearly showed that the results of the existing DCOPF-based models might lead to invalid vulnerability analysis as compared to the results from our proposed ACOPF-based model. Note that given the sensitivity of the vulnerability analysis in power systems, relying on the DCOPF-based approaches might lead to catastrophic societal and economic consequences. In this context, our proposed ACOPF-based approach provides far more practical analysis and also avoids such societal and economic consequences. In addition, the results demonstrate that vulnerability can be reduced by minimal changes in Iran's 400-kV transmission network.

A novel multi-period AC-based approach was presented in Chapter 6 to analyze N-k contingencies in order to enhance the resilience of a bulk power system under multiple outages. This model is an extension of our model in Chapter 5. The model is tested by different IEEE test cases. The method presented load shedding and the critical lines for each contingency over a range of system demand levels of this test system. Furthermore, the results show that in the congested systems especially where the reactive power flows predominate on some lines or buses such as cables or bus 6 in the IEEE RTS network, the assessment cannot be adequately conducted only by the active power flows.

Due to the increasing uncertainty caused by the dramatic increase of intermittent renewable energy sources (RESs) such as wind power, together with the load forecast errors and price-responsive demands, the traditional security assessment may not provide a holistic and optimal solution for the power system operation under uncertainty. In order to guarantee the operational security of power systems with such uncertainties, developing security models and tools for immunizing the system against worst uncertainty realizations has conducted in Chapter 7. In this chapter, a two-stage adaptive robust optimization model for the vulnerability assessment

of power systems is proposed. Our simulation results show that the power system vulnerability assessment without considering the uncertainties leads to optimistic results. Moreover, increasing the level of uncertainty in our case studies leads to higher levels of load shedding and different critical lines in comparison with no uncertainty case.

A preliminary study to assess the vulnerability of a power system to natural events is conducted in Appendix A. First, Complex network analysis (CNA) is introduced and then, the topology of the test case is modeled using Gephi, and five different measures of CNA such as degree, betweenness, closeness, PageRank, eigenvector centralities are compared. Moreover, extracting the required georeferenced model from open access resources such as Openstreetmap website [416], the Swiss transmission grid operator (Swissgrid), google map, Over-Turbo website [417] and map of European Network of Transmission System Operators for Electricity (ENTSO-E) [418] is introduced. This is a practical way to overcome the fact that it is not possible to access all data of a real-life network. This appendix went beyond a "pure" systemic vulnerability assessment. Indeed, it considered the power system exposure to a specific natural hazard.

In summary, this thesis focused on developing tools to identify the systemic vulnerabilities of the power system under multiple contingencies and different operational uncertainties. The performance of the models is illustrated using small-scale, medium-scale and real-life case studies. Finally, the projected result will have a practical as well as an academic interest. Planners in the power system sector can employ the proposed approaches and tools to ensure a resilient operation of the power system which is of paramount importance. Power system operators work hard to assure a safe and reliable service. The proposed techniques and approaches help operators to identify the critical components which must be protected or fortified when the protective and financial resources are limited.

8-3 Future works

As expected when coming to the end of a research project, there exist several areas worthy of further research. The following list gives a brief overview of directions for future research that are corresponding to the previous chapters:

- Vulnerability analysis is a topical field. Our published review paper [20] that is presented in Chapter 2, reviewed the literature up to the year 2019. However, we have cited new literature in our recent papers, new review paper is needed as an extension to Chapter 2. Moreover, adding new proposed approaches for vulnerability analysis of

interconnected networks such as integrated electricity and gas system (IEGS) may be a promising future research.

- In Chapter 3, an integrated assessment framework is proposed to improve the decision-making process on the best network topology using multi-criteria decision-making (MCDM). In this chapter, two important security assessment in power systems are employed. Adding other related concepts into this framework such as resiliency i.e. "integrated robustness, reliability, and resilience framework" and proposing a new approach to compare them can be good future extension of this chapter.
- In Chapter 4, we thoroughly investigate the effects of assumptions in DCM, especially when it is used for line capacity-based assessments such as reliability, vulnerability, and contingency analyses. It should be pointed out that the convergence and large computational burden still represent major problems for ACM. Further research should focus on a new power flow formulation that considers essential parameters that significantly affect the results, such as losses, reactive power flow, and voltage violations for transmission line capacity-based assessment.
- Chapter 5 introduced an MIBNLP problem and then approximate the nonlinear terms to solve effectively using efficient off-the-shelf solvers such as Cplex. If our approximation assumptions are not valid, there is no guarantee that our approximate solution is feasible in the original problem. For these cases, we proposed two solutions: (1) improving the accuracy of our LP model by including more linear terms associated with the approximation of nonlinear terms and (2) developing some heuristic techniques to recover a feasible point from our approximate solution. Another application of our approximate solution is to use it as the warm start of the solution algorithms for solving the original MIBNLP. Exploring these ideas represents an interesting extension of our work. In addition, we can broadly categorize the solution algorithms for bilevel optimization problems as (1) direct solution algorithms, (2) metaheuristic algorithms, and (3) single-level reformulation algorithms. Exploring the first and second techniques for solving the AD model proposed are good future works.
- Chapter 6 proposed a multi period vulnerability analysis where typically, the highest load demand forecast is used in each time period. In this model, the steady-state operation of the power system is modeled in the AD interaction. Modeling and simulation of the dynamics of the power system in the AD interaction is a good future extension of our work. Furthermore, the 2M piecewise linear (PWL) blocks and the n-

sided convex regular polygon are used for the approximation of nonlinear terms in the lower-level problem. The accuracy of our model can be improved by adding more linear terms (i.e., n and M). A large M or n improves the accuracy but increases the number of equations and accordingly the computational burden. Furthermore, a small n enforces more restrictions on transmission line capacity and might lead to the problem infeasibility. We set the linear terms based on the recommendations in [340, 365] for our test cases. Finding an optimal value of linear terms for a large-scale power system is good future work.

- An interesting future direction is to explore how our proposed MILP model in Chapters 6 and 7 can be adjusted to be used for the real-time vulnerability assessment of the power systems. As an alternative, tools based on Artificial Intelligence (AI) allow us to assess vulnerability in real-time using the knowledge obtained from off-line learning. Accordingly, our proposed MILP approach can be used for off-line training of AI-based tools which can be used for real-time decision making.
- Chapter 7 introduced a three-level optimization problem for power system vulnerability assessment in the context of system uncertainty. An interesting future direction is to explore how our proposed MILP model can be adjusted to accurately model the asymmetric uncertainties.
- A preliminary study on the vulnerability analysis of a power system subjected to natural hazards is conducted in Appendix A. An interesting future direction could be employing optimization-based approaches which is presented in Part three instead of CNA to improve the accuracy of the analysis. Furthermore, to rely on the georeferenced model extracted from open access resources, it is needed to be benchmarked with the real model to estimate the model errors.

This thesis focused on the vulnerability of the power system without considering its interdependencies with other infrastructures. Another fruitful avenue for future research is to identify the vulnerabilities and risks stemming from the interdependencies of large-scale electricity and gas systems to ensure a robust and resilient integrated electricity and gas system (IEGS) (see Figure 8-1). The interdependency is growing between electricity and gas networks in transmission and distribution levels. On the one hand, more power plants are being supplied by natural gas (G2Ps) owing to less contamination and lower costs compared to conventional power plants. On the other hand, the recent power to gas (P2G) technology allows a bi-directional interchange of energy and provides opportunities for

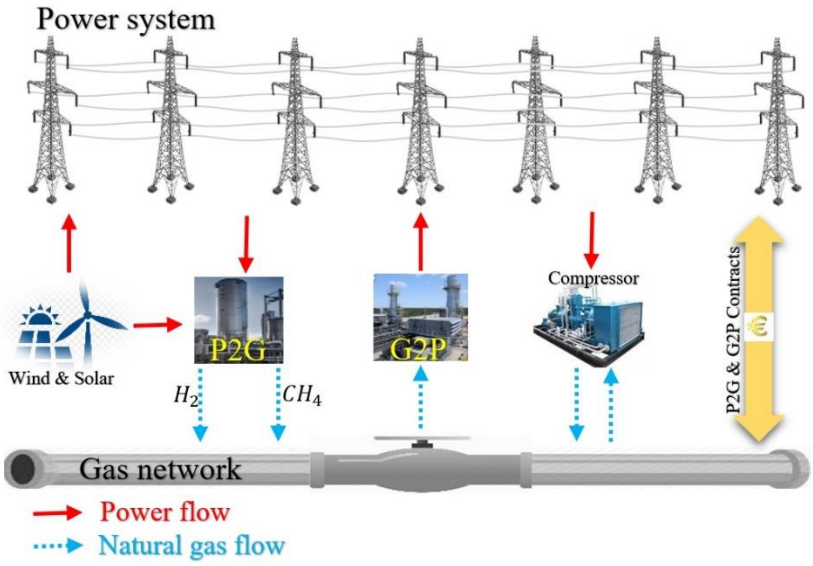

Figure 8-1. An integrated electricity and gas system (IEGS).

storing the renewable energy surplus and decreasing the operational cost. The interdependencies between the electricity and gas sectors are not limited to physical coupling components such as G2Ps, P2Gs, and the electricity-driven compressors in the gas network. They are, in most cases, operating with different utilities and independent system operators (ISO). The energy contracts between these two sectors introduce another layer of interdependency, that is, economic coupling. Hence, the vulnerability assessment of a power system with its interdependencies is a must and a good future direction of research.

Bibliography

1. Kröger, W., *Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools.* Reliability Engineering & System Safety, 2008. **93**(12): p. 1781-1787.
2. Gutierrez, F., et al., *Vulnerability Analysis of Power Grids Using Modified Centrality Measures.* Discrete Dynamics in Nature and Society, 2013.
3. Veloza, O.P. and R.H. Cespedes. *Vulnerability of the Colombian electric system to blackouts and possible remedial actions*. in *2006 IEEE Power Engineering Society General Meeting*. 2006.
4. Kamali, S. and T. Amraee, *Blackout prediction in interconnected electric energy systems considering generation re-dispatch and energy curtailment.* Applied Energy, 2017. **187**: p. 50-61.
5. Zio, E. and T. Aven, *Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?* Energy Policy, 2011. **39**(10): p. 6308-6320.
6. Veloza, O.P. and F. Santamaria, *Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes.* The Electricity Journal, 2016. **29**(7): p. 42-49.
7. Panteli, M. and P. Mancarella, *Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies.* Electric Power Systems Research, 2015. **127**: p. 259-270.
8. Bompard, E., et al., *Classification and trend analysis of threats origins to the security of power systems.* International Journal of Electrical Power & Energy Systems, 2013. **50**: p. 50-64.
9. Ding, T., L. Yao, and F.X. Li, *A multi-uncertainty-set based two-stage robust optimization to defender-attacker-defender model for power system protection.* Reliability Engineering & System Safety, 2018. **169**: p. 179-186.
10. VSE, *Wege in die neue Stromzukunft Gesamtbericht* 2012, Verband Schweizerischer Elektrizitätsunternehmen (VSE), Aarau.
11. Densing, M., S. Hirschberg, and H. Turton, *Review of Swiss electricity scenarios 2050.* Report prepared for the Group Energy Perspectives and the Swiss Competence Center for Energy Research "Supply of Electricity"(SCCER SoE). PSI Bericht, 2014(14-05).
12. Wimbish, W. and J. Sterling, *The National Infrastructure Simulation and Analysis Center (NISAC): A New Contributor to Strategic Leader Education and Formulation of Critical Infrastructure Policies and Decisions*. 2003.
13. Bie, Z., et al., *Battling the extreme: A study on the power system resilience.* 2017. **105**(7): p. 1253-1266.
14. Wang, J., et al., *Literature review on modeling and simulation of energy infrastructures from a resilience perspective.* Reliability Engineering & System Safety, 2019. **183**: p. 360-373.
15. Zio, E., *Challenges in the vulnerability and risk analysis of critical infrastructures.* Reliability Engineering & System Safety, 2016. **152**: p. 137-150.
16. Haidar, A.M.A., A. Mohamed, and A. Hussain. *Vulnerability Assessment of Power System Using Various Vulnerability Indices*. in *2006 4th Student Conference on Research and Development*. 2006.
17. Cuadra, L., et al., *A Critical Review of Robustness in Power Grids Using Complex Networks Concepts.* Energies, 2015. **8**(9): p. 9211-9265.

18. Arroyo, J.M. and F.J. Fernández, *A Genetic Algorithm for Power System Vulnerability Analysis under Multiple Contingencies*, in *Metaheuristics for Bi-level Optimization*, E.-G. Talbi, Editor. 2013, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 41-68.
19. Fang, Y.P., G. Sansavini, and E. Zio, *An Optimization-Based Framework for the Identification of Vulnerabilities in Electric Power Grids Exposed to Natural Hazards.* Risk Analysis, 2019. **39**(9): p. 1949-1969.
20. Abedi, A., L. Gaudard, and F. Romerio-Giudici, *Review of major approaches to analyze vulnerability in power system.* Reliability Engineering and System Safety, 2019. **183**: p. 153-172.
21. Abedi, A. and F. Romerio-Giudici. *Systemic Vulnerability of Swiss Power Grid to Natural Events*. in *MATEC Web Conf. 7th International Conference on Power Science and Engineering (ICPSE 2018)*. 2019.
22. Abedi, A., et al., *MCDM approach for the integrated assessment of vulnerability and reliability of power systems.* IET Generation, Transmission & Distribution, 2019. **13**(20): p. 4741-4746.
23. Abedi, A., L. Gaudard, and F. Romerio, *Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems: The benefits and limitations.* Reliability Engineering & System Safety, 2020. **201**: p. 106961.
24. Abedi, A. and F. Romerio, *Multi-period vulnerability analysis of power grids under multiple outages: An AC-based bilevel optimization approach.* International Journal of Critical Infrastructure Protection, 2020: p. 100365.
25. Abedi, A., M.R. Hesamzadeh, and F. Romerio, *An ACOPF-based bilevel optimization approach for vulnerability assessment of a power system.* International Journal of Electrical Power & Energy Systems, 2021. **125**: p. 106455.
26. Akdeniz, E. and M. Bagriyanik, *A knowledge based decision support algorithm for power transmission system vulnerability impact reduction.* International Journal of Electrical Power & Energy Systems, 2016. **78**: p. 436-444.
27. Sweeney, J.L., *The California electricity crisis*. 2002, Stanford, Calif.: Hoover Institution Press.
28. Mao, A., J. Yu, and Z. Guo. *Electric power grid structural vulnerability assessment*. in *2006 IEEE Power Engineering Society General Meeting*. 2006.
29. Pant, R., J.W. Hall, and S. Blainey, *Vulnerability assessment framework for interdependent critical infrastructures: case-study for Great Britain's rail network.* European Journal of Transport and Infrastructure Research, 2016. **16**(1): p. 174-194.
30. Bilis, E.I., W. Kroger, and C. Nan, *Performance of Electric Power Systems Under Physical Malicious Attacks.* IEEE Systems Journal, 2013. **7**(4): p. 854-865.
31. Chopade, P. and M. Bikdash, *New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts.* International Journal of Critical Infrastructure Protection, 2016. **12**: p. 29-45.
32. Bompard, E., et al., *A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator.* International Journal of Electrical Power & Energy Systems, 2016. **81**: p. 12-21.
33. Ferrario, E., N. Pedroni, and E. Zio, *Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation.* Reliability Engineering & System Safety, 2016. **155**: p. 78-96.
34. Bompard, E., L. Luo, and E. Pons, *A perspective overview of topological approaches for vulnerability analysis of power transmission grids.* International Journal of Critical Infrastructures, 2015. **11**(1): p. 15-26.
35. Pagani, G.A. and M. Aiello, *The Power Grid as a complex network: A survey.* Physica a-Statistical Mechanics and Its Applications, 2013. **392**(11): p. 2688-2700.
36. Yusta, J.M., G.J. Correa, and R. Lacal-Arantegui, *Methodologies and applications for critical infrastructure protection: State-of-the-art.* Energy Policy, 2011. **39**(10): p. 6100-6119.
37. Cavalieri, F., et al., *Models for Seismic Vulnerability Analysis of Power Networks: Comparative Assessment.* Computer-Aided Civil and Infrastructure Engineering, 2014. **29**(8): p. 590-607.
38. Bier, V.M. and M.N. Azaiez, *Game theoretic risk analysis of security threats*. International series in operations research & management science. 2009, New York: Springer Science+Business. vi, 236 p.

39. Jamshidi, M., *Systems of systems engineering : principles and applications*. 2009, Boca Raton, Fla.: Taylor & Francis
40. Ouyang, M., *Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks.* Reliability Engineering & System Safety, 2016. **154**: p. 106-116.
41. Zio, E., R. Piccinelli, and G. Sansavini, *An All-Hazard approach for the vulnerability analysis of critical infrastructures*, in *Advances in Safety, Reliability and Risk Management*. 2011, CRC Press. p. 2451-2458.
42. Wang, S.L., L. Hong, and X.G. Chen, *Vulnerability analysis of interdependent infrastructure systems: A methodological framework.* Physica a-Statistical Mechanics and Its Applications, 2012. **391**(11): p. 3323-3335.
43. Wang, S.L., et al., *Vulnerability analysis of interdependent infrastructure systems under edge attack strategies.* Safety Science, 2013. **51**(1): p. 328-337.
44. Agostino, G.D., et al. *Methodologies for inter-dependency assessment*. in *2010 5th International Conference on Critical Infrastructure (CRIS)*. 2010.
45. Johansson, J. and H. Hassel, *An approach for modelling interdependent infrastructures in the context of vulnerability analysis.* Reliability Engineering & System Safety, 2010. **95**(12): p. 1335-1344.
46. Wang, S. and J. Liu, *Robustness of single and interdependent scale-free interaction networks with various parameters.* Physica A: Statistical Mechanics and its Applications, 2016. **460**: p. 139-151.
47. Griot, C., *Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation.* International Journal of Critical Infrastructures, 2010. **6**(4): p. 363-379.
48. Huang, C.N., J.J.H. Liou, and Y.C. Chuang, *A method for exploring the interdependencies and importance of critical infrastructures.* Knowledge-Based Systems, 2014. **55**: p. 66-74.
49. Zio, E. and G. Sansavini, *Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins.* IEEE Transactions on Reliability, 2011. **60**(1): p. 94-101.
50. Eusgeld, I., C. Nan, and S. Dietz, *"System-of-systems" approach for interdependent critical infrastructures.* Reliability Engineering & System Safety, 2011. **96**(6): p. 679-686.
51. Gao, J.X., D.Q. Li, and S. Havlin, *From a single network to a network of networks.* National Science Review, 2014. **1**(3): p. 346-356.
52. Atputharajah, A. and T.K. Saha. *Power system blackouts - literature review*. in *2009 International Conference on Industrial and Information Systems (ICIIS)*. 2009.
53. Koc, Y., et al., *The impact of the topology on cascading failures in a power grid model.* Physica a-Statistical Mechanics and Its Applications, 2014. **402**: p. 169-179.
54. Carreras, B.A., et al., *Critical points and transitions in an electric power transmission model for cascading failure blackouts.* Chaos, 2002. **12**(4): p. 985-994.
55. Dobson, I., et al., *Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization.* Chaos, 2007. **17**(2).
56. Prieto, F., J.M. Sarabia, and A.J. Saez, *Modelling major failures in power grids in the whole range*. International Journal of Electrical Power & Energy Systems, 2014. **54**: p. 10-16.
57. Beck, G., et al. *Global blackouts–Lessons learned*. in *Power-Gen Europe*. 2005.
58. *Learning from the blackouts : transmission system security in competitive electricity markets*. 2005, Paris: International Energy Agency.
59. Eremia, M. and M. Shahidehpour, *Handbook of electrical power system dynamics : modeling, stability, and control*. 2013: John Wiley & Sons.
60. Huang, W., et al. *A lesson learned from recent cascading outages: Coupled interface and its impact on the smart-grid development*. in *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*. 2013.
61. Gomes, P. *New strategies to improve bulk power system security: lessons learned from large blackouts*. in *IEEE Power Engineering Society General Meeting, 2004.* 2004.
62. Begovic, M.M., *Electrical transmission systems and smart grids : selected entries from the Encyclopedia of sustainability science and technology*. 2013, New York: Springer. vi, 324 pages.

63. Zeng, B., et al., *An analysis of previous blackouts in the world: Lessons for China's power industry.* Renewable & Sustainable Energy Reviews, 2015. **42**: p. 1151-1163.
64. Lai, L.L., et al. *Lessons learned from July 2012 Indian blackout*. in *9th IET International Conference on Advances in Power System Control, Operation and Management (APSCOM 2012)*. 2012.
65. United States. Congress. Office of Technology Assessment., *Physical vulnerability of electric systems to natural disasters and sabotage*. 1990, Washington, D.C.: Congress of the U.S. For sale by the Supt. of Docs., U.S. G.P.O. viii, 63 p.
66. Murray, A.T. and T.H. Grubesic, *Critical infrastructure : reliability and vulnerability*. 2007, Berlin ; London: Springer.
67. Ouyang, M., *Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability.* Chaos, 2013. **23**(2).
68. Ke, S. and H. Zhen-Xiang. *Analysis and Comparison on Several Kinds of Models of Cascading Failure in Power System*. in *2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific*. 2005.
69. Chen, G., et al., *Attack structural vulnerability of power grids: A hybrid approach based on complex networks.* Physica a-Statistical Mechanics and Its Applications, 2010. **389**(3): p. 595-603.
70. Ouyang, M. and K. Yang, *Does topological information matter for power grid vulnerability?* Chaos: An Interdisciplinary Journal of Nonlinear Science, 2014. **24**(4): p. 043121.
71. Liu, C.C., et al., *The strategic power infrastructure defense (SPID) system - A conceptual design.* IEEE Control Systems Magazine, 2000. **20**(4): p. 40-52.
72. Zhenbo, W. and J. Liu. *Research on the electric power grid vulnerability under the directed-weighted topological model based on Complex Network Theory*. in *Mechanic Automation and Control Engineering (MACE), 2010 International Conference on*. 2010.
73. Huang, T., et al., *Analysis and Visualization of Natural Threats Against the Security of Electricity Transmission System*, in *The Scientific Bulletin of Electrical Engineering Faculty*. 2017.
74. Shen, B., D. Koval, and S. Shen. *Modelling extreme-weather-related transmission line outages*. in *Engineering Solutions for the Next Millennium. 1999 IEEE Canadian Conference on Electrical and Computer Engineering* 1999.
75. Zhu, Y.H., et al., *Resilience Analysis of Power Grids Under the Sequential Attack.* IEEE Transactions on Information Forensics and Security, 2014. **9**(12): p. 2340-2354.
76. Miller, C.R., *Electromagnetic pulse threats in 2010*. 2005, DTIC Document.
77. Liu, Y., P. Ning, and M.K. Reiter, *False Data Injection Attacks against State Estimation in Electric Power Grids.* Acm Transactions on Information and System Security, 2011. **14**(1).
78. Liu, X. and Z. Li, *Local Topology Attacks in Smart Grids.* IEEE Transactions on Smart Grid, 2016. **PP**(99): p. 1-10.
79. Kim, J. and L. Tong, *On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures.* IEEE Journal on Selected Areas in Communications, 2013. **31**(7): p. 1294-1305.
80. Liu, X. and Z.Y. Li, *Local Load Redistribution Attacks in Power Systems With Incomplete Network Information.* IEEE Transactions on Smart Grid, 2014. **5**(4): p. 1665-1676.
81. Hug, G. and J.A. Giampapa, *Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks.* IEEE Transactions on Smart Grid, 2012. **3**(3): p. 1362-1370.
82. Chen, P.Y. and A.O. Hero, *Assessing and safeguarding network resilience to nodal attacks.* IEEE Communications Magazine, 2014. **52**(11): p. 138-143.
83. Ouyang, M., et al., *Mitigating electric power system vulnerability to worst-case spatially localized attacks.* Reliability Engineering & System Safety, 2017. **165**: p. 144-154.
84. Pu, C.L. and W. Cui, *Vulnerability of complex networks under path-based attacks.* Physica a-Statistical Mechanics and Its Applications, 2015. **419**: p. 622-629.
85. Wolf, S., et al., *Clarifying vulnerability definitions and assessments using formalisation.* International Journal of Climate Change Strategies and Management, 2013. **5**(1): p. 54-70.

86. Dolan, M., et al., *Forensic Disaster Analysis of Flood Damage at Commercial and Industrial Firms*, in *Flood Damage Survey and Assessment*. 2017, John Wiley & Sons, Inc. p. 195-209.
87. Kundak, S., *Cascading and unprecedented effects of disasters in urban system*, in *Intelligent Systems and Decision Making for Risk Analysis and Crisis Response*. 2013, CRC Press. p. 743-748.
88. Pascale, S., F. Sdao, and A. Sole, *A model for assessing the systemic vulnerability in landslide prone areas.* Natural Hazards and Earth System Sciences, 2010. **10**(7): p. 1575-1590.
89. Veen, A.V.D. and C. Logtmeijer, *Economic Hotspots: Visualizing Vulnerability to Flooding.* Natural Hazards, 2005. **36**(1): p. 65-80.
90. Chang, L. and Z.G. Wu, *Performance and reliability of electrical power grids under cascading failures.* International Journal of Electrical Power & Energy Systems, 2011. **33**(8): p. 1410-1419.
91. French, G.S. and D. Gootzit, *Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack*, in *Vulnerability, Uncertainty, and Risk*. p. 782-789.
92. Holmgren, Å., *Vulnerability analysis of electric power delivery networks, PhD diss.*, . 2004, Mark och vatten.
93. Haimes, Y.Y., *On the definition of vulnerabilities in measuring risks to infrastructures.* Risk Analysis, 2006. **26**(2): p. 293-296.
94. Vereinte Nationen and International Strategy for Disaster Reduction, *Living with risk - a global review of disaster reduction initiatives*. 2004 ed. 2004, New York ; Geneva: United Nations. 2 Bd.
95. Johansson, J., H. Hassel, and E. Zio, *Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems.* Reliability Engineering & System Safety, 2013. **120**: p. 27-38.
96. Baldick, R., et al. *Vulnerability assessment for cascading failures in electric power systems*. in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*. 2009.
97. Ouyang, M., et al., *Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks.* Physica a-Statistical Mechanics and Its Applications, 2014. **403**: p. 45-53.
98. NERC, *Security guidelines for the electricity sector: Vulnerability and risk assessment.* Technical Report, Washington, DC, North American Electric Reliability Corporation., 2002.
99. Vamanu, B.I., A.V. Gheorghe, and P.F. Katina, *Critical Infrastructures: Risk and Vulnerability Assessment in Transportation of Dangerous Goods Transportation by Road and Rail*. 2016, Springer.
100. Dwivedi, A. and X.H. Yu, *A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis.* IEEE Transactions on Industrial Informatics, 2013. **9**(1): p. 81-88.
101. Gao, J.X., B. Barzel, and A.L. Barabasi, *Universal resilience patterns in complex networks.* Nature, 2016. **530**(7590): p. 307-312.
102. Hosseini, S., K. Barker, and J.E. Ramirez-Marquez, *A review of definitions and measures of system resilience.* Reliability Engineering & System Safety, 2016. **145**: p. 47-61.
103. Alipour, Z., M.A.S. Monfared, and E. Zio, *Comparing topological and reliability-based vulnerability analysis of Iran power transmission network.* Proceedings of the Institution of Mechanical Engineers Part O-Journal of Risk and Reliability, 2014. **228**(2): p. 139-151.
104. Rosas-Casals, M., S. Valverde, and R.V. SolÉ, *Topological vulnerability of the european power grid under errors and attacks.* International Journal of Bifurcation and Chaos, 2007. **17**(07): p. 2465-2475.
105. Bompard, E., D. Wu, and E. Pons, *Complex Science Application to the Analysis of Power Systems Vulnerabilities.*
106. Helber, S., *Performance analysis of flow lines with non-linear flow of material*. 1999, Berlin; New York: Spinger.
107. Tuffin, B., et al., *Simulation versus analytic-numeric methods: illustrative examples*, in *Proceedings of the 2nd international conference on Performance evaluation methodologies and tools*. 2007, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): Nantes, France. p. 1-10.

108. Billinton, R. and W. Li, *Reliability assessment of electric power systems using Monte Carlo methods*. The language of science. 1994, New York: Plenum Press. xvi, 351 p.
109. Liu, G.Y., C. Liu, and Y. Wang. *Montecarlo simulation for the seismic response analysis of electric power system in Taiwan*. in *NCREE/JRC joint workshop*. 2003. Citeseer.
110. Boccaletti, S., et al., *Complex networks: Structure and dynamics.* Physics Reports, 2006. **424**(4): p. 175-308.
111. Rosas-Casals, M., et al., *Knowing power grids and understanding complexity science.* International Journal of Critical Infrastructures, 2015. **11**(1): p. 4-14.
112. Dorogovtsev, S.N. and J.F.F. Mendes, *Evolution of Networks : From Biological Nets to the Internet and WWW.* 2003.
113. Ouyang, M., et al., *Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability.* Reliability Engineering & System Safety, 2014. **123**: p. 38-46.
114. Zhang, J., et al., *Structural vulnerability and intervention of high speed railway networks.* Physica A: Statistical Mechanics and its Applications, 2016. **462**: p. 743-751.
115. Haznagy, A., et al. *Complex network analysis of public transportation networks: A comprehensive study*. in *International Conference onModels and Technologies for Intelligent Transportation Systems (MT-ITS)*. 2015.
116. Dehghani, M.S. and H.D. Sherali, *A resource allocation approach for managing critical network-based infrastructure systems.* Iie Transactions, 2016. **48**(9): p. 826-837.
117. Hossain, M.M. and S. Alam, *A complex network approach towards modeling and analysis of the Australian Airport Network.* Journal of Air Transport Management, 2017. **60**: p. 1-9.
118. Bagler, G., *Analysis of the airport network of India as a complex weighted network.* Physica A: Statistical Mechanics and its Applications, 2008. **387**(12): p. 2972-2980.
119. Khakzad, N. and G. Reniers, *Using graph theory to analyze the vulnerability of process plants in the context of cascading effects.* Reliability Engineering & System Safety, 2015. **143**: p. 63-73.
120. Yong, S., et al. *Using complex network theory in the Internet engineering*. in *Computer Science & Education (ICCSE), 2012 7th International Conference on*. 2012.
121. Thai, M.T. and P.M. Pardalos, *Handbook of optimization in complex networks : communication and social networks*. Springer optimization and its applications,. 2012, Gainesville, FL: Springer. xii, 541 pages.
122. Thai, M.T. and P.M. Pardalos, *Handbook of optimization in complex networks : theory and applications*. Springer optimization and its applications,. 2012, New York, NY: Springer. xiv, 544 p.
123. De Meo, P., et al., *A novel measure of edge centrality in social networks.* Knowledge-Based Systems, 2012. **30**: p. 136-150.
124. Costa, L.d.F., et al., *Analyzing and modeling real-world phenomena with complex networks: a survey of applications.* Advances in Physics, 2011. **60**(3): p. 329-412.
125. Guimera, R. and L.A.N. Amaral, *Functional cartography of complex metabolic networks.* Nature, 2005. **433**(7028): p. 895-900.
126. Barrat, A., M. Barthelemy, and A. Vespignani, *Dynamical processes on complex networks*. 2008, Cambridge: Cambridge University Press.
127. Freeman, L.C., S.P. Borgatti, and D.R. White, *Centrality in Valued Graphs - a Measure of Betweenness Based on Network Flow.* Social Networks, 1991. **13**(2): p. 141-154.
128. Nasiruzzaman, A.B.M., H.R. Pota, and F.R. Islam. *Complex network framework based dependency matrix of electric power grid*. in *Universities Power Engineering Conference (AUPEC), 2011 21st Australasian*. 2011.
129. Fang, Y. and E. Zio, *Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems.* American Journal of Operations Research, 2013. **3**: p. 12.
130. Sánchez, J.E.C., *A complex network approach to analyzing the structure and dynamics of power grids*. 2009, The University of Vermont.
131. Ben-Naim, E., H. Frauenfelder, and Z. Toroczkai, *Complex networks*. 2004: Springer.
132. Newman, M.E.J., *Networks : an introduction*. 2010, Oxford: Oxford University Press.

133. Estrada, E., *The structure of complex networks : theory and applications*. 2012, New York: Oxford University Press.
134. Schneider, C.M., *The robustness of complex networks*. 2011, Technische Universität Dortmund.
135. Ayyub, B.M., *Vulnerability, uncertainty, and risk : analysis, modeling and management* 2011, Reston, Va.: American Society of Civil Engineers.
136. Costa, L.D., et al., *Characterization of complex networks: A survey of measurements.* Advances in Physics, 2007. **56**(1): p. 167-242.
137. Bompard, E., R. Napoli, and F. Xue, *Analysis of structural vulnerabilities in power transmission grids.* International Journal of Critical Infrastructure Protection, 2009. **2**(1-2): p. 5-12.
138. Newman, M.E.J., *A measure of betweenness centrality based on random walks.* Social Networks, 2005. **27**(1): p. 39-54.
139. Latora, V. and M. Marchiori, *A measure of centrality based on network efficiency.* New Journal of Physics, 2007. **9**(6): p. 188.
140. Guan, X., et al. *Power grids vulnerability analysis based on combination of degree and betweenness*. in *The 26th Chinese Control and Decision Conference (2014 CCDC)*. 2014.
141. Newman, M.E.J., *The Structure and Function of Complex Networks.* SIAM Review, 2003. **45**(2): p. 167-256.
142. Bai, W.j., et al. *Electric Power Grids and Blackouts in Perspective of Complex Networks*. in *2006 International Conference on Communications, Circuits and Systems*. 2006.
143. Klopotek, M.A., S.T. Wierzchon, and K. Trojanowski, *Intelligent Information Processing and Web Mining: Proceedings of the International IIS: IIPWM´06 Conference held in Ustron, Poland, June 19-22, 2006*. 2007: Springer Berlin Heidelberg.
144. Rosato, V., S. Bologna, and F. Tiriticco, *Topological properties of high-voltage electrical transmission networks.* Electric Power Systems Research, 2007. **77**(2): p. 99-105.
145. Hines, P. and S. Blumsack. *A Centrality Measure for Electrical Networks*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008.
146. Erdos, P. and A. Renyi, *On the Evolution of Random Graphs.* Bulletin of the International Statistical Institute, 1960. **38**(4): p. 343-347.
147. Watts, D.J. and S.H. Strogatz, *Collective dynamics of 'small-world' networks.* Nature, 1998. **393**(6684): p. 440-442.
148. Crucitti, P., V. Latora, and M. Marchiori, *Model for cascading failures in complex networks.* Physical Review E, 2004. **69**(4).
149. Pagani, G.A. and M. Aiello, *From the grid to the smart grid, topologically.* Physica a-Statistical Mechanics and Its Applications, 2016. **449**: p. 160-175.
150. Newman, M.E.J., *Analysis of weighted networks.* Phys. Rev. E, 2004. **70**(5): p. 056131.
151. Pagani, G.A. and M. Aiello, *A complex network approach for identifying vulnerabilities of the medium and low voltage grid.* International Journal of Critical Infrastructures, 2015. **11**(1): p. 36-61.
152. Zio, E. and L.R. Golea, *Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements.* Reliability Engineering & System Safety, 2012. **101**: p. 67-74.
153. Liu, C., et al. *Vulnerability evaluation of power system integrated with large-scale distributed generation based on complex network theory*. in *2012 47th International Universities Power Engineering Conference (UPEC)*. 2012.
154. Cadini, F., E. Zio, and C.-A. Petrescu, *Using Centrality Measures to Rank the Importance of the Components of a Complex Network Infrastructure*. 2009, Springer p. 155-167.
155. Nasiruzzaman, A.B.M., H.R. Pota, and M.A. Mahmud. *Application of centrality measures of complex network framework in power grid*. in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*. 2011.
156. Arianos, S., et al., *Power grid vulnerability: A complex network approach.* Chaos, 2009. **19**(1).
157. Crucitti, P., V. Latora, and M. Marchiori, *Locating critical lines in high-voltage electrical power grids.* Fluctuation and Noise Letters, 2005. **5**(2): p. L201-L208.
158. Holmgren, A.J., *Using graph models to analyze the vulnerability of electric power networks.* Risk Analysis, 2006. **26**(4): p. 955-969.

159. Chen, X., et al. *Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory*. in *2007 IEEE Power Engineering Society General Meeting*. 2007.
160. Zio, E., C.-A. Petrescu, and G. Sansavini. *Vulnerability analysis of a power transmission system*. in *Proc. International Probabilistic Safety Assessment and Management Conference (PSAM)*. 2008.
161. Buzna, L., L. Issacharoff, and D. Helbing, *The evolution of the topology of high-voltage electricity networks.* International Journal of Critical Infrastructures, 2009. **5**(1-2): p. 72-85.
162. Eusgeld, I., et al., *The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures.* Reliability Engineering & System Safety, 2009. **94**(5): p. 954-963.
163. Chen, G., et al., *An improved model for structural vulnerability analysis of power networks.* Physica a-Statistical Mechanics and Its Applications, 2009. **388**(19): p. 4259-4266.
164. Zio, E. and R. Piccinelli, *Randomized flow model and centrality measure for electrical power transmission network analysis.* Reliability Engineering & System Safety, 2010. **95**(4): p. 379-385.
165. Bompard, E., D. Wu, and F. Xue. *The Concept of Betweenness in the Analysis of Power Grid Vulnerability*. in *Complexity in Engineering, 2010. COMPENG '10.* 2010.
166. Jin, S., et al. *A novel application of parallel betweenness centrality to power grid contingency analysis*. in *2010 IEEE International Symposium on Parallel & Distributed Processing (IPDPS)*. 2010.
167. Wang, Z., A. Scaglione, and R.J. Thomas. *Electrical centrality measures for electric power grid vulnerability analysis*. in *49th IEEE Conference on Decision and Control (CDC)*. 2010.
168. Fu, L., et al. *Vulnerability Assessment for Power Grid Based on Small-world Topological Model*. in *2010 Asia-Pacific Power and Energy Engineering Conference*. 2010.
169. Hines, P., E. Cotilla-Sanchez, and S. Blumsack, *Do topological models provide good information about electricity infrastructure vulnerability?* Chaos, 2010. **20**(3).
170. Zhang, J.H., et al., *Attack vulnerability of self-organizing networks.* Safety Science, 2012. **50**(3): p. 443-447.
171. Bompard, E., R. Napoli, and F. Xue, *Extended topological approach for the assessment of structural vulnerability in transmission networks.* IET Generation Transmission & Distribution, 2010. **4**(6): p. 716-724.
172. Wang, K., et al., *An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load.* Physica a-Statistical Mechanics and Its Applications, 2011. **390**(23-24): p. 4692-4701.
173. Wu, Z.g., Q. Zhong, and Y. Zhang. *State Transition Graph of Cascading Electrical Power Grids*. in *2007 IEEE Power Engineering Society General Meeting*. 2007.
174. Bompard, E., D. Wu, and F. Xue, *Structural vulnerability of power systems: A topological approach.* Electric Power Systems Research, 2011. **81**(7): p. 1334-1340.
175. Zio, E., et al., *Application of the load flow and random flow models for the analysis of power transmission networks.* Reliability Engineering & System Safety, 2012. **103**: p. 102-109.
176. Bompard, E., E. Pons, and D. Wu, *Extended Topological Metrics for the Analysis of Power Grid Vulnerability.* IEEE Systems Journal, 2012. **6**(3): p. 481-487.
177. Kong, R., et al., *An Energy-Based Centrality for Electrical Networks.* Energy and Power Engineering, 2013. **5**: p. 6.
178. Huang, X., et al. *Vulnerability Analysis of Bus Failure in Power Grid*. in *Third International Conference on Control, Automation and Systems Engineering (CASE-13)*. 2013. Citeseer.
179. Zhang, G.D., et al., *Understanding the cascading failures in Indian power grids with complex networks theory.* Physica a-Statistical Mechanics and Its Applications, 2013. **392**(15): p. 3273-3280.
180. Monfared, M.A.S. and Z. Alipour, *Structural Properties and vulnerability of Iranian 400kv Power Transmission Grid: a Complex Systems Approach.* Industrial Engineering & Management 2013.
181. Kim, D.H., et al., *Network topology and resilience analysis of South Korean power grid.* Physica a-Statistical Mechanics and Its Applications, 2017. **465**: p. 13-24.

182. Ouyang, M., et al., *Correlation analysis of different vulnerability metrics on power grids.* Physica a-Statistical Mechanics and Its Applications, 2014. **396**: p. 204-211.
183. Xu, Y., A.J. Gurfinkel, and P.A. Rikvold, *Architecture of the Florida power grid as a complex network.* Physica a-Statistical Mechanics and Its Applications, 2014. **401**: p. 130-140.
184. Zhu, Y., et al., *Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph.* IEEE Transactions on Parallel and Distributed Systems, 2014. **25**(12): p. 3274-3284.
185. Li, C., et al. *Method for evaluating the importance of power grid nodes based on PageRank algorithm*. IET Generation, Transmission & Distribution, 2014. **8**, 1843-1847.
186. Zhang, J.H., et al., *Vulnerability analysis of the US power grid based on local load-redistribution.* Safety Science, 2015. **80**: p. 156-162.
187. Coelho, E.P., et al. *A complex network analysis of the Brazilian Power Test System*. in *Innovative Smart Grid Technologies Latin America (ISGT LATAM), 2015 IEEE PES*. 2015.
188. Chowdhury, T., A. Chakrabarti, and C.K. Chanda. *Analysis of Vulnerability indices of power grid integrated DG units based on Complex Network theory*. in *India Conference (INDICON), 2015 Annual IEEE*. 2015.
189. WANG, H., et al., *Evaluation method of node importance for power grid considering inflow and outflow power.* Journal of Modern Power Systems and Clean Energy, 2017. **5**(5): p. 696-703.
190. Albarakati, A., M. Bikdash, and X. Dai. *Line-graph based modeling for assessing the vulnerability of transmission lines*. in *SoutheastCon*. 2017. IEEE.
191. Dey, A.K., Y.R. Gel, and H.V. Poor, *Motif-based analysis of power grid robustness under attacks.* arXiv preprint arXiv:1708.06738, 2017.
192. Wang, S.L., et al., *Vulnerability analysis and critical areas identification of the power systems under terrorist attacks.* Physica a-Statistical Mechanics and Its Applications, 2017. **473**: p. 156-165.
193. Gupta, S., et al., *Analysis and prediction of vulnerability in smart power transmission system: A geometrical approach.* International Journal of Electrical Power & Energy Systems, 2018. **94**: p. 77-87.
194. Wang, Z.Y., et al., *A power flow based model for the analysis of vulnerability in power networks.* Physica a-Statistical Mechanics and Its Applications, 2016. **460**: p. 105-115.
195. Yuan, Y., et al., *Probabilistic load flow computation of a power system containing wind farms using the method of combined cumulants and Gram-Charlier expansion.* IET Renewable Power Generation, 2011. **5**(6): p. 448-454.
196. Kundur, P., N.J. Balu, and M.G. Lauby, *Power system stability and control*. The EPRI power system engineering series. 1994, New York: McGraw-Hill. xxiii, 1176 p.
197. Stevenson, W.D., *Elements of power system analysis*. 4th ed. McGraw-Hill series in electrical engineering Power and energy. 1982, New York: McGraw-Hill. xii, 436 p.
198. Saadat, H., *Power system analysis*. McGraw-Hill series in electrical and computer engineering. 1999, Boston: WCB/McGraw-Hill. xix, 697 p.
199. LaRocca, S., et al., *Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems.* Risk Analysis, 2015. **35**(4): p. 608-623.
200. Yan, J., et al., *Cascading Failure Analysis With DC Power Flow Model and Transient Stability Analysis.* IEEE Transactions on Power Systems, 2015. **30**(1): p. 285-297.
201. Carreras, B.A., et al. *Dynamical and probabilistic approaches to the study of blackout vulnerability of the power transmission grid*. in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. 2004.
202. Nedic, D.P., et al., *Criticality in a cascading failure blackout model.* International Journal of Electrical Power & Energy Systems, 2006. **28**(9): p. 627-633.
203. Dobson, I., B.A. Carreras, and D.E. Newman, *A loading-dependent model of probabilistic cascading failure.* Probability in the Engineering and Informational Sciences, 2005. **19**(1): p. 15-32.
204. Cupac, V., J.T. Lizier, and M. Prokopenko, *Comparing dynamics of cascading failures between network-centric and power flow models.* International Journal of Electrical Power & Energy Systems, 2013. **49**: p. 369-379.

205. Fitzmaurice, R., *Cascading Failure in a Complex System Model for Power Systems: Operating and Planning Policy*. 2010: University College Dublin.
206. Han, S.W., Z.X. Peng, and S.Q. Wang, *The maximum flow problem of uncertain network.* Information Sciences, 2014. **265**: p. 167-175.
207. Fan, W.L., S.W. Huang, and S.W. Mei, *Invulnerability of power grids based on maximum flow theory.* Physica a-Statistical Mechanics and Its Applications, 2016. **462**: p. 977-985.
208. Fang, J., et al., *Power System Structural Vulnerability Assessment based on an Improved Maximum Flow Approach.* IEEE Transactions on Smart Grid, 2016. **PP**(99): p. 1-1.
209. Zhang, P. and S.T. Lee, *Probabilistic load flow computation using the method of combined cumulants and Gram-Charlier expansion.* IEEE Transactions on Power Systems, 2004. **19**(1): p. 676-682.
210. Marah, B. and A.O. Ekwue. *Probabilistic load flows*. in *Power Engineering Conference (UPEC), 2015 50th International Universities*. 2015.
211. Ma, J., et al. *Probabilistic vulnerability assessment based on power flow and voltage distribution*. in *IEEE PES T&D 2010*. 2010.
212. Wang, X.F., Y. Song, and M. Irving, *Modern Power Systems Analysis*. 2010: Springer US.
213. Ran, X.H. and S.H. Miao, *Three-phase probabilistic load flow for power system with correlated wind, photovoltaic and load.* IET Generation Transmission & Distribution, 2016. **10**(12): p. 3093-3101.
214. Von Neumann, J. and O. Morgenstern, *Theory of games and economic behavior*. 3d ed. 1953, Princeton: Princeton University Press. 641 p.
215. Bompard, E., et al., *Risk Assessment of Malicious Attacks Against Power Systems.* IEEE Transactions on Systems Man and Cybernetics Part a-Systems and Humans, 2009. **39**(5): p. 1074-1085.
216. Cheng, M.X., M. Crow, and Q.M. Ye, *A game theory approach to vulnerability analysis: Integrating power flows with topological analysis.* International Journal of Electrical Power & Energy Systems, 2016. **82**: p. 29-36.
217. Wang, Q., *Game Theory Approach to Transportation Network Vulnerability Measurement.* 2012.
218. Bricha, N. and M. Nourelfath, *Critical supply network protection against intentional attacks: A game-theoretical model.* Reliability Engineering & System Safety, 2013. **119**: p. 1-10.
219. Flammini, F., *Critical infrastructure security : assessment, prevention, detection, response*. Information & communication technologies. 2012, Southampton ; Boston: WIT Press. 303 p.
220. Matsumoto, A. and F. Szidarovszky, *Game theory and its applications*. 2016, Toyko ; New York: Institute of Economic Research, Springer. xiv, 268 pages.
221. Holmgren, A.J., E. Jenelius, and J. Westin, *Evaluating strategies for defending electric power networks against antagonistic attacks.* IEEE Transactions on Power Systems, 2007. **22**(1): p. 76-84.
222. Korzhyk, D., et al., *Stackelberg vs. Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness.* Journal of Artificial Intelligence Research, 2011. **41**: p. 297-327.
223. Sinha, A., et al. *Stackelberg Security Games: Looking Beyond a Decade of Success*. in *IJCAI*. 2018.
224. Gomez, C., et al., *Hierarchical infrastructure network representation methods for risk-based decision-making.* Structure and Infrastructure Engineering, 2013. **9**(3): p. 260-274.
225. Agarwal, J., D. Blockley, and N. Woodman, *Vulnerability of structural systems.* Structural Safety, 2003. **25**(3): p. 263-286.
226. Cortes, J.A.M.B., M. Sanchez-Silva, and S. Tesfamariam, *A hierarchy- based approach to seismic vulnerability assessment of bulk power systems.* Structure and Infrastructure Engineering, 2015. **11**(10): p. 1352-1368.
227. Gómez, C., et al., *Vulnerability assessment of infrastructure networks by using hierarchical decomposition methods*, in *Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management*. 2011. p. 214-221.
228. Ruan, D., *Fuzzy systems and soft computing in nuclear engineering*. 2000, Heidelberg: Physica Verlag.

229. Schaeffer, S.E., *Graph clustering.* Computer Science Review, 2007. **1**(1): p. 27-64.
230. Dwivedi, A., X. Yu, and P. Sokolowski. *Analyzing power network vulnerability with maximum flow based centrality approach*. in *2010 8th IEEE International Conference on Industrial Informatics*. 2010.
231. Nasiruzzaman, A.B.M. and H.R. Pota. *Critical node identification of smart power system using complex network framework based centrality approach*. in *North American Power Symposium (NAPS), 2011*. 2011.
232. Wang, J., et al. *Identifying line vulnerability in power system using maximum flow based complex network theory*. in *IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society*. 2014.
233. Dai, Y., et al., *An improved framework for power grid vulnerability analysis considering critical system features.* Physica A: Statistical Mechanics and its Applications, 2014. **395**: p. 405-415.
234. Singh, A.K. and B.C. Pal, *IEEE PES Task Force on Benchmark Systems for Stability Controls Report on the 68-Bus, 16-Machine, 5-Area System*. 2013, Technical Report.
235. Correa, G.J. and J.M. Yusta, *Grid vulnerability analysis based on scale-free graphs versus power flow models.* Electric Power Systems Research, 2013. **101**: p. 71-79.
236. Correa-Henao, G.J. and J.M. Yusta-Loyo, *Representation of electric power systems by complex networks with applications to risk vulnerability assessment.* Dyna, 2015. **82**(192): p. 68-77.
237. Kim, T., et al., *Vulnerability analysis of power systems.* arXiv preprint arXiv:1503.02360, 2015.
238. Wang, X., et al. *A network approach for power grid robustness against cascading failures*. in *2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. 2015.
239. da Silva, A.M.L., et al., *A Method for Ranking Critical Nodes in Power Networks Including Load Uncertainties.* IEEE Transactions on Power Systems, 2016. **31**(2): p. 1341-1349.
240. Grigg, C., et al., *The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee.* IEEE Transactions on Power Systems, 1999. **14**(3): p. 1010-1020.
241. Werho, T., et al., *Power System Connectivity Monitoring Using a Graph Theory Network Flow Algorithm.* IEEE Transactions on Power Systems, 2016. **PP**(99): p. 1-8.
242. Li, J., et al., *AC power flow importance measures considering multi-element failures.* Reliability Engineering & System Safety, 2017. **160**: p. 89-97.
243. Fang, R., et al., *Identification of vulnerable lines in power grids with wind power integration based on a weighted entropy analysis method.* International Journal of Hydrogen Energy, 2017. **42**(31): p. 20269-20276.
244. Liu, B., et al., *Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality.* IEEE Transactions on Circuits and Systems II: Express Briefs, 2017.
245. Wang, A., et al., *Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory.* IEEE Transactions on Power Systems, 2011. **26**(1): p. 442-450.
246. Zhang, C., J.E. Ramirez-Marquez, and J.H. Wang, *Critical infrastructure protection using secrecy - A discrete simultaneous game.* European Journal of Operational Research, 2015. **242**(1): p. 212-221.
247. Zechman, E.M., *Agent-based modeling to simulate contamination events and evaluate threat management strategies in water distribution systems.* Risk Anal, 2011. **31**(5): p. 758-72.
248. Gonzalez de Durana, J.M., et al., *Agent based modeling of energy networks.* Energy Conversion and Management, 2014. **82**: p. 308-319.
249. Stroeve, S.H. and M.H.C. Everdij, *Agent-based modelling and mental simulation for resilience engineering in air transport.* Safety Science, 2017. **93**: p. 29-49.
250. Ali, A.M., M.E. Shafiee, and E.Z. Berglund, *Agent-based modeling to simulate the dynamics of urban water supply: Climate, population growth, and water shortages.* Sustainable Cities and Society, 2017. **28**: p. 420-434.
251. Galus, M.D., *Agent-based modeling and simulation of large scale electric mobility in power systems*. 2012.
252. Sujil, A., J. Verma, and R. Kumar, *Multi agent system: concepts, platforms and applications in power systems.* Artificial Intelligence Review, 2016.

253. Dehghanpour, K., C. Colson, and H. Nehrir, *A Survey on Smart Agent-Based Microgrids for Resilient/Self-Healing Grids.* Energies, 2017. **10**(5): p. 620.
254. Xie, J. and C.-C. Liu, *Multi-agent systems and their applications.* Journal of International Council on Electrical Engineering, 2017. **7**(1): p. 188-197.
255. Akyol, B., et al., *VOLTTRON: An Agent Execution Platform for the Electric Power System*. 2017.
256. Yan, H., et al. *Branch transient vulnerability assessment based on the transient energy function and complex network*. in *2014 International Conference on Power System Technology*. 2014.
257. Jurado, F. and J. Carpio, *Energy functions analysis in voltage collapse.* European Transactions on Electrical Power, 2001. **11**(4): p. 235-240.
258. Pai, M.A., *Energy function analysis for power system stability*. The Kluwer international series in engineering and computer science Power electronics and power systems. 1989, Boston: Kluwer Academic Publishers. viii, 240 p.
259. Tsolas, N.A., A. Arapostathis, and P.P. Varaiya, *A Structure Preserving Energy Function for Power-System Transient Stability Analysis.* IEEE Transactions on Circuits and Systems, 1985. **32**(10): p. 1041-1049.
260. Chow, J.H., et al., *Synchronized phasor data based energy function analysis of dominant power transfer paths in large power systems.* IEEE Transactions on Power Systems, 2007. **22**(2): p. 727-734.
261. Bhui, P. and N. Senroy, *Real-Time Prediction and Control of Transient Stability Using Transient Energy Function.* IEEE Transactions on Power Systems, 2017. **32**(2): p. 923-934.
262. Fouad, A.A., Z. Qin, and V. Vittal, *System vulnerability as a concept to assess power system dynamic security.* IEEE Transactions on Power Systems, 1994. **9**(2): p. 1009-1015.
263. Padiyar, K.R. and H.S.Y. Sastry, *Topological energy-function analysis of stability of power systems.* International Journal of Electrical Power & Energy Systems, 1987. **9**(1): p. 9-16.
264. Rangaiah, G.P., *Multi-objective optimization : techniques and applications in chemical engineering*, in *Advances in process systems engineering*. 2017, World Scientific Publishing,: Singapore.
265. Cho, J.H., et al., *A Survey on Modeling and Optimizing Multi-Objective Systems.* IEEE Communications Surveys and Tutorials, 2017. **19**(3): p. 1867-1901.
266. Babick, J.P., *Tri-level optimization of critical infrastructure resilience*. 2009, Monterey, California. Naval Postgraduate School.
267. Faramondi, L., et al., *Network Structural Vulnerability: A Multiobjective Attacker Perspective.* IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018(99): p. 1-14.
268. Mingoo, K., M.A. El-Sharkawi, and R.J. Marks. *Vulnerability indices for power systems*. in *Proceedings of the 13th International Conference on, Intelligent Systems Application to Power Systems*. 2005.
269. Haidar, A.M.A., A. Mohamed, and A. Hussain. *Vulnerability Assessment of a Large Sized Power System Using Radial Basis Function Neural Network*. in *2007 5th Student Conference on Research and Development*. 2007.
270. Pinar, A., A. Reichert, and B. Lesieutre. *Computing Criticality of Lines in Power Systems*. in *2007 IEEE International Symposium on Circuits and Systems*. 2007.
271. Jingling, L., J. QunXing, and Z. YongLi. *Power grid vulnerability assement based on energy function*. in *2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*. 2008.
272. Liu, Q., J. Liu, and Q. Huang. *Configure vulnerability assessment based on potential energy model*. in *2009 International Conference on Sustainable Power Generation and Supply*. 2009.
273. Dong, X., et al. *Vulnerability analysis of power grid based on multi-agent complex systems*. in *Proceedings of 2011 IEEE International Conference on Service Operations, Logistics and Informatics*. 2011.
274. Huang, Z.m. and H.q. Li. *Vulnerable Branch Assessment Based on Branch Energy Function*. in *2012 Asia-Pacific Power and Energy Engineering Conference*. 2012.
275. Witthaut, D., et al., *Critical Links and Nonlocal Rerouting in Complex Supply Networks.* Phys Rev Lett, 2016. **116**(13): p. 138701.

276. Kröger, W., E. Zio, and M. Schläpfer, *Vulnerable systems*. 2011, London: Springer. xiv, 204 pages.
277. Corder, G.W. and D.I. Foreman, *Nonparametric statistics for non-statisticians : a step-by-step approach*. 2009, Oxford: Wiley-Blackwell.
278. Zio, E., C.-A. Petrescu, and G. Sansavini. *Vulnerability analysis of a power transmission system*. in *international probabilistic safety assessment and management conference (PSAM)*. 2008.
279. Rocchetta, R. and E. Patelli, *Assessment of power grid vulnerabilities accounting for stochastic loads and model imprecision.* International Journal of Electrical Power & Energy Systems, 2018. **98**: p. 219-232.
280. Cadini, F., G.L. Agliardi, and E. Zio, *A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions.* Applied Energy, 2017. **185, Part 1**: p. 267-279.
281. Baldick, R., et al. *Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures*. in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*. 2008.
282. Rosato, V., et al., *Modelling interdependent infrastructures using interacting dynamical models.* International Journal of Critical Infrastructures, 2008. **4**(1-2): p. 63-79.
283. Arghandeh, R., et al., *On the definition of cyber-physical resilience in power systems.* Renewable & Sustainable Energy Reviews, 2016. **58**: p. 1060-1069.
284. Nezamoddini, N., S. Mousavian, and M. Erol-Kantarci, *A risk optimization model for enhanced power grid resilience against physical attacks.* Electric Power Systems Research, 2017. **143**(Supplement C): p. 329-338.
285. Ma, T.-L., et al., *Non-monotonic increase of robustness with capacity tolerance in power grids.* Physica A: Statistical Mechanics and its Applications, 2013. **392**(21): p. 5516-5524.
286. Schneider, C.M., et al., *Mitigation of malicious attacks on networks.* Proceedings of the National Academy of Sciences of the United States of America, 2011. **108**(10): p. 3838-3841.
287. Pagani, G.A. and M. Aiello, *Power grid complex network evolutions for the smart grid.* Physica a-Statistical Mechanics and Its Applications, 2014. **396**: p. 248-266.
288. Bompard, E., et al., *Classification and trend analysis of threats origins to the security of power systems.* International Journal of Electrical Power & Energy Systems, 2013. **50**(Supplement C): p. 50-64.
289. Chu, C.-C. and H.H.-C. Iu, *Complex Networks Theory For Modern Smart Grid Applications: A Survey.* IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2017.
290. Wang, C.W., C. Grebogi, and M.S. Baptista, *Control and prediction for blackouts caused by frequency collapse in smart grids.* Chaos, 2016. **26**(9).
291. Wang, W. and Z. Lu, *Survey Cyber security in the Smart Grid: Survey and challenges.* Comput. Netw., 2013. **57**(5): p. 1344-1371.
292. Gao, J., et al., *Recent Progress on the Resilience of Complex Networks.* Energies, 2015. **8**(10): p. 12187.
293. Heitzig, J., et al., *Interdisciplinary challenges in the study of power grid resilience and stability and their relation to extreme weather events.* European Physical Journal-Special Topics, 2014. **223**(12): p. 2383-2386.
294. Strbac, G., et al., *Microgrids: Enhancing the Resilience of the European Megagrid.* IEEE Power and Energy Magazine, 2015. **13**(3): p. 35-43.
295. Zio, E., *Critical Infrastructures Vulnerability and Risk Analysis.* European Journal for Security Research, 2016. **1**(2): p. 97-114.
296. Huang, T., et al., *The Structural Dimensions in the Security of Power Transmission Systems*, in *Infranomics: Sustainability, Engineering Design and Governance*, A.V. Gheorghe, M. Masera, and P.F. Katina, Editors. 2014, Springer International Publishing: Cham. p. 311-337.
297. Gheorghe, A.V., P.F. Katina, and M. Masera, *Infranomics : sustainability, engineering design and governance*. 2014: Springer, Cham.
298. Kadhem, A.A., et al., *Computational techniques for assessing the reliability and sustainability of electrical power systems: A review.* Renewable & Sustainable Energy Reviews, 2017. **80**: p. 1175-1186.

299. Billinton, R. and A. Sankarakrishnan. *A comparison of Monte Carlo simulation techniques for composite power system reliability assessment*. in *IEEE WESCANEX 95. Communications, Power, and Computing. Conference Proceedings*. 1995. IEEE.
300. Wang, S., et al., *Multiple perspective vulnerability analysis of the power network.* 2018. **492**: p. 1581-1590.
301. Murray, A.T. and T. Grubesic, *Critical infrastructure: Reliability and vulnerability*. 2007: Springer Science & Business Media.
302. Blockley, D., et al., *Structural vulnerability, reliability and risk.* 2002. **4**(2): p. 203-212.
303. Albert, R. and A.L. Barabasi, *Statistical mechanics of complex networks.* Reviews of Modern Physics, 2002. **74**(1): p. 47-97.
304. BEYZA, J., et al., *Vulnerability assessment of a large electrical grid by new graph theory approach.* 2018. **16**(2): p. 527-535.
305. Haidar, A.M., A. Mohamed, and A. Hussain. *Vulnerability assessment of a large sized power system using radial basis function neural network*. in *2007 5th Student Conference on Research and Development*. 2007. IEEE.
306. Bier, V.M., et al., *Methodology for identifying near-optimal interdiction strategies for a power transmission system.* Reliability Engineering & System Safety, 2007. **92**(9): p. 1155-1161.
307. Even, S., *Graph algorithms*. 2011: Cambridge University Press.
308. Wood, A.J., B.F. Wollenberg, and G.B. Sheblé, *Power generation, operation, and control*. 2013: John Wiley & Sons.
309. Billinton, R. and R.N. Allan, *Reliability evaluation of power systems*. 2nd ed. 1996, New York: Plenum Press. xx, 514 p.
310. Moazzami, M., et al., *Reliability evaluation for different power plant busbar layouts by using sequential Monte Carlo simulation.* 2013. **53**: p. 987-993.
311. Wen, J., et al., *A review on reliability assessment for wind power.* 2009. **13**(9): p. 2485-2494.
312. Zhou, P., et al., *Reliability and economic evaluation of power system with renewables: A review.* 2016. **58**: p. 537-547.
313. Zimmerman, R.D., C.E. Murillo-Sanchez, and R.J. Thomas, *MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education.* IEEE Transactions on Power Systems, 2011. **26**(1): p. 12-19.
314. Grigg, C., et al., *The IEEE reliability test system-1996.* . 1999. **14**(3): p. 1010-1020.
315. Billinton, R. and W. Wangdee, *Impact of utilising sequential and nonsequential simulation techniques in bulk-electric-system reliability assessment.* IEE Proceedings-Generation Transmission and Distribution, 2005. **152**(5): p. 623-628.
316. Yusta, J.M., G.J. Correa, and R.J.E.p. Lacal-Arántegui, *Methodologies and applications for critical infrastructure protection: State-of-the-art.* 2011. **39**(10): p. 6100-6119.
317. Behzadian, M., et al., *A state-of the-art survey of TOPSIS applications.* 2012. **39**(17): p. 13051-13069.
318. Almoghathawi, Y., et al., *A multi-criteria decision analysis approach for importance identification and ranking of network components.* 2017. **158**: p. 142-151.
319. Campbell, R.J. and S. Lowry. *Weather-related power outages and electric system resiliency*. 2012. Congressional Research Service, Library of Congress Washington, DC.
320. Commission, E.E., *"Energy roadmap 2050"*. COM (2011), 2011. **885**: p. 15.
321. Koranyi, D., *A US Strategy for Sustainable Energy Security*. 2016: Atlantic Council.
322. Fang, Y.P., G. Sansavini, and E. Zio, *An Optimization-Based Framework for the Identification of Vulnerabilities in Electric Power Grids Exposed to Natural Hazards.* Risk Analysis, 2019. **39**(9): p. 1949-1969.
323. Abunima, H., et al., *A Systematic Review of Reliability Studies on Composite Power Systems: A Coherent Taxonomy Motivations, Open Challenges, Recommendations, and New Research Directions.* Energies, 2018. **11**(9).
324. Cetinay, H., et al., *Comparing the Effects of Failures in Power Grids under the AC and DC Power Flow Models.* IEEE Transactions on Network Science and Engineering, 2018: p. 1-1.
325. Qi, Y., D. Shi, and D. Tylavsky. *Impact of assumptions on DC power flow model accuracy*. in *2012 North American Power Symposium (NAPS)*. 2012.

326. Overbye, T.J., X. Cheng, and Y. Sun, *A Comparison of the AC and DC Power Flow Models for LMP Calculations*, in *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2 - Volume 2*. 2004, IEEE Computer Society. p. 20047.1.
327. Qin, W., et al., *Reactive Power Aspects in Reliability Assessment of Power Systems.* IEEE Transactions on Power Systems, 2011. **26**(1): p. 85-92.
328. Benidris, M. and J. Mitra, *Reliability and sensitivity analysis of composite power systems considering voltage and reactive power constraints.* IET Generation, Transmission & Distribution, 2015. **9**(12): p. 1245-1253.
329. Kile, H., et al. *A comparison of AC and DC power flow models for contingency and reliability analysis*. in *Power Systems Computation Conference (PSCC), 2014*. 2014. IEEE.
330. Li, J., et al., *AC power flow importance measures considering multi-element failures.* Reliability Engineering & System Safety, 2017. **160**: p. 89-97.
331. Saadat, H., *Power system analysis*. 1999, Boston: WCB/McGraw-Hill. 697 pages.
332. Zhu, J., *Optimization of power system operation*, in *IEEE Press series on power engineering*. 2015, John Wiley & Sons.
333. Abedi, A. and F. Romerio. *Systemic Vulnerability of Swiss Power Grid to Natural Events*. in *2018 7th International Conference on Power Science and Engineering (ICPSE 2018)* 2018.
334. Koç, Y., et al. *Matcasc: A tool to analyse cascading line outages in power grids*. in *2013 IEEE International Workshop on Inteligent Energy Systems (IWIES)*. 2013. IEEE.
335. Chatterjee, D., et al. *N-1-1 AC contingency analysis as a part of NERC compliance studies at midwest ISO*. in *Transmission and Distribution Conference and Exposition, 2010 IEEE PES*. 2010.
336. Billinton, R. and A. Sankarakrishnan, *A comparison of Monte Carlo simulation techniques for composite power system reliability assessment.* IEEE Wescanex '95 - Communications, Power, and Computing, Conference Proceedings, Vols 1 and 2, 1995: p. 145-150.
337. Moazzami, M., et al., *Reliability evaluation for different power plant busbar layouts by using sequential Monte Carlo simulation.* International Journal of Electrical Power & Energy Systems, 2013. **53**: p. 987-993.
338. Billinton, R. and R.N. Allan, *Reliability evaluation of engineering systems*. 1992: Springer.
339. SFOE, S.F.O.o.E. *Energy Strategy 2050*. 2017; Available from: http://www.bfe.admin.ch/energiestrategie2050/index.html?lang=en.
340. Akbari, T. and M.T. Bina, *Linear approximated formulation of AC optimal power flow using binary discretisation.* IET Generation Transmission & Distribution, 2016. **10**(5): p. 1117-1123.
341. Salmeron, J., K. Wood, and R. Baldick, *Analysis of electric grid security under terrorist threat.* IEEE Transactions on Power Systems, 2004. **19**(2): p. 905-912.
342. Sinha, A., P. Malo, and K. Deb, *A Review on Bilevel Optimization: From Classical to Evolutionary Approaches and Applications.* IEEE Transactions on Evolutionary Computation, 2018. **22**(2): p. 276-295.
343. Stackelberg, H.v., *The theory of the market economy*. 1952, New York,: Oxford University Press.
344. Smith, J.C. and Y. Song, *A survey of network interdiction models and algorithms.* European Journal of Operational Research, 2020. **283**(3): p. 797-811.
345. Doumpos, M., et al., *New Perspectives in Multiple Criteria Decision Making: Innovative Applications and Case Studies*. 2019: Springer.
346. Arroyo, J.M. and F.D. Galiana, *On the solution of the bilevel programming formulation of the terrorist threat problem.* IEEE Transactions on Power Systems, 2005. **20**(2): p. 789-797.
347. Motto, A.L., J.M. Arroyo, and F.D. Galiana, *A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat.* IEEE Transactions on Power Systems, 2005. **20**(3): p. 1357-1365.
348. Arroyo, J.M., *Bilevel programming applied to power system vulnerability analysis under multiple contingencies.* IET Generation Transmission & Distribution, 2010. **4**(2): p. 178-190.
349. Salmeron, J., K. Wood, and R. Baldick, *Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids.* IEEE Transactions on Power Systems, 2009. **24**(1): p. 96-104.

350. Delgadillo, A., J.M. Arroyo, and N. Alguacil, *Analysis of Electric Grid Interdiction With Line Switching.* IEEE Transactions on Power Systems, 2010. **25**(2): p. 633-641.
351. Arroyo, J.M. and F.J. Fernández, *Application of a genetic algorithm to n-K power system security assessment.* International Journal of Electrical Power & Energy Systems, 2013. **49**: p. 114-121.
352. Brown, G., et al., *Defending Critical Infrastructure.* INFORMS Journal on Applied Analytics, 2006. **36**(6): p. 530-544.
353. Alguacil, N., A. Delgadillo, and J.M. Arroyo, *A trilevel programming approach for electric grid defense planning.* Computers & Operations Research, 2014. **41**: p. 282-290.
354. Wu, X. and A.J. Conejo, *An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning.* IEEE Transactions on Power Systems, 2017. **32**(4): p. 2984-2994.
355. Fang, Y.-P. and E. Zio, *An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards.* European Journal of Operational Research, 2019. **276**(3): p. 1119-1136.
356. Sayed, A.R., C. Wang, and T.S. Bi, *Resilient operational strategies for power systems considering the interactions with natural gas systems.* Applied Energy, 2019. **241**: p. 548-566.
357. Yuan, W., L. Zhao, and B. Zeng, *Optimal power grid protection through a defender–attacker–defender model.* Reliability Engineering & System Safety, 2014. **121**: p. 83-89.
358. Yuan, W. and B. Zeng, *Cost-effective power grid protection through defender–attacker–defender model with corrective network topology control.* Energy Systems, 2019: p. 1-27.
359. Grigsby, L.L., *Power system stability and control*. 2016: CRC press.
360. Kim, T., et al., *Analyzing Vulnerability of Power Systems with Continuous Optimization Formulations.* IEEE Transactions on Network Science and Engineering, 2016. **3**(3): p. 132-146.
361. Bienstock, D. and A. Verma, *Strong NP-hardness of AC power flows feasibility.* Operations Research Letters, 2019. **47**(6): p. 494-501.
362. Tómasson, E., M.R. Hesamzadeh, and F.A. Wolak, *Optimal offer-bid strategy of an energy storage portfolio: A linear quasi-relaxation approach.* Applied Energy, 2020. **260**: p. 114251.
363. Motto, A.L., et al., *Network-constrained multiperiod auction for a pool-based electricity market.* IEEE Transactions on Power Systems, 2002. **17**(3): p. 646-653.
364. Pereira, M.V., et al., *Strategic bidding under uncertainty: A binary expansion approach.* IEEE Transactions on Power Systems, 2005. **20**(1): p. 180-188.
365. Arabpour, A., M.R. Besmi, and P. Maghouli, *Transmission Expansion Planning with Linearized AC Load Flow by Special Ordered Set Method.* Journal of Energy Engineering, 2018. **144**(2).
366. Akbari, T. and M.T. Bina, *Approximated MILP model for AC transmission expansion planning: global solutions versus local solutions.* IET Generation Transmission & Distribution, 2016. **10**(7): p. 1563-1569.
367. Floudas, C.A., *Nonlinear and mixed-integer optimization: fundamentals and applications*. 1995: Oxford University Press.
368. Hesamzadeh, M.R., N. Hosseinzadeh, and P.J. Wolfs, *A leader–followers model of transmission augmentation for considering strategic behaviours of generating companies in energy markets.* International Journal of Electrical Power & Energy Systems, 2010. **32**(5): p. 358-367.
369. Moiseeva, E. and M.R. Hesamzadeh, *Bayesian and Robust Nash Equilibria in Hydrodominated Systems Under Uncertainty.* IEEE Transactions on Sustainable Energy, 2018. **9**(2): p. 818-830.
370. Ha, D.T., *Modèles et indicateurs pour l'analyse des vulnérabilités des réseaux électriques aux pertes de lignes*, in *Université Grenoble Alpes*. 2018.
371. Maghouli, P., et al., *A Scenario-Based Multi-Objective Model for Multi-Stage Transmission Expansion Planning.* IEEE Transactions on Power Systems, 2011. **26**(1): p. 470-478.
372. Che, L., et al., *A Mixed Integer Programming Model for Evaluating the Hidden Probabilities of N-k Line Contingencies in Smart Grids.* IEEE Transactions on Smart Grid, 2019. **10**(1): p. 1036-1045.
373. Scaparra, M.P. and R.L. Church, *A bilevel mixed-integer program for critical infrastructure protection planning.* Computers & Operations Research, 2008. **35**(6): p. 1905-1923.
374. Faramondi, L., et al., *Network Structural Vulnerability: A Multiobjective Attacker Perspective.* IEEE Transactions on Systems Man Cybernetics-Systems, 2019. **49**(10): p. 2036-2049.

375. Marrone, S., et al., *Vulnerability modeling and analysis for critical infrastructure protection applications.* International Journal of Critical Infrastructure Protection, 2013. **6**(3-4): p. 217-227.
376. Yang, Y.F., X.H. Guan, and Q.Z. Zhai, *Fast Grid Security Assessment With N-k Contingencies.* IEEE Transactions on Power Systems, 2017. **32**(3): p. 2193-2203.
377. NERC, *Evaluation of Criteria, Methods, and Practices Used for System Design, Planning, and Analysis Response to NERC Blackout Recommendation 13c*. 2019.
378. Sundar, K., et al., *Probabilistic N-k failure-identification for power systems.* Networks, 2018. **71**(3): p. 302-321.
379. Kaplunovich, P. and K. Turitsyn, *Fast and Reliable Screening of N-2 Contingencies.* IEEE Transactions on Power Systems, 2016. **31**(6): p. 4243-4252.
380. Fan, N., R. Chen, and J. Watson. *N-1-1 contingency-constrained optimal power flow by interdiction methods*. in *2012 IEEE Power and Energy Society General Meeting*. 2012.
381. Abdi-Khorsand, M., M. Sahraei-Ardakani, and Y.M. Al-Abdullah, *Corrective Transmission Switching for N-1-1 Contingency Analysis.* IEEE Transactions on Power Systems, 2017. **32**(2): p. 1606-1615.
382. Nemati, H., M.A. Latify, and G.R. Yousefi, *Tri-level transmission expansion planning under intentional attacks: virtual attacker approach - part I: formulation.* IET Generation Transmission & Distribution, 2019. **13**(3): p. 390-398.
383. Nemati, H., M.A. Latify, and G.R. Yousefi, *Tri-level transmission Expansion planning under intentional attacks: virtual attacker approach-part II: case studies.* IET Generation Transmission & Distribution, 2019. **13**(3): p. 399-408.
384. Karimi, S., P. Musilek, and A.M. Knight, *Dynamic thermal rating of transmission lines: A review*. Renewable & Sustainable Energy Reviews, 2018. **91**: p. 600-612.
385. Frank, S., J. Sexauer, and S. Mohagheghi, *Temperature-Dependent Power Flow*. IEEE Transactions on Power Systems, 2013. **28**(4): p. 4007-4018.
386. Soroudi, A., *Power system optimization modeling in GAMS*. Vol. 78. 2017: Springer.
387. Akbari, T. and M.T. Bina, *A linearized formulation of AC multi-year transmission expansion planning: A mixed-integer linear programming approach.* Electric Power Systems Research, 2014. **114**: p. 93-100.
388. Matoušek, J. and B. Gärtner, *Understanding and using linear programming*. Universitext. 222 p.
389. Christie, R. and I. Dabbagchi, *IEEE 57-Bus System.* 1993.
390. Anghilante, R., et al., *Innovative power-to-gas plant concepts for upgrading of gasification bio-syngas through steam electrolysis and catalytic methanation.* Energy Conversion and Management, 2019. **183**: p. 462-473.
391. Nagarajan, R. and C. Singh. *Multi-area reliability evaluation using composite system framework*. in *2016 IEEE International Conference on Power System Technology (POWERCON)*. 2016.
392. Sayed, A.R., C. Wang, and T. Bi, *Resilient operational strategies for power systems considering the interactions with natural gas systems.* Applied Energy, 2019. **241**: p. 548-566.
393. Lin, Y. and Z. Bie, *Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding.* Applied Energy, 2018. **210**: p. 1266-1279.
394. Fang, Y.P. and E. Zio, *An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards.* European Journal of Operational Research, 2019. **276**(3): p. 1119-1136.
395. Bai, X.Q., L.Y. Qu, and W. Qiao, *Robust AC Optimal Power Flow for Power Networks With Wind Power Generation.* IEEETransactions on Power Systems, 2016. **31**(5): p. 4163-4164.
396. Hesamzadeh, M.R., J. Rosellón, and I. Vogelsang, *Transmission Network Investment in Liberalized Power Markets*. 2020, Springer.
397. Bertsimas, D., et al., *Adaptive Robust Optimization for the Security Constrained Unit Commitment Problem.* IEEE Transactions on Power Systems, 2013. **28**(1): p. 52-63.
398. Dai, C., L. Wu, and H. Wu, *A Multi-Band Uncertainty Set Based Robust SCUC With Spatial and Temporal Budget Constraints.* IEEE Transactions on Power Systems, 2016. **31**(6): p. 4988-5000.

399. Verastegui, F., et al., *An Adaptive Robust Optimization Model for Power Systems Planning With Operational Uncertainty*. IEEE Transactions on Power Systems, 2019. **34**(6): p. 4606-4616.
400. Jabr, R.A., *Robust Transmission Network Expansion Planning With Uncertain Renewable Generation and Loads.* IEEETransactions on Power Systems, 2013. **28**(4): p. 4558-4567.
401. Morales, J.M., et al., *Integrating renewables in electricity markets: operational problems*. Vol. 205. 2013: Springer Science & Business Media.
402. Zhang, X. and A.J. Conejo, *Coordinated Investment in Transmission and Storage Systems Representing Long- and Short-Term Uncertainty.* IEEE Transactions on Power Systems, 2018. **33**(6): p. 7143-7151.
403. García-Cerezo, Á., L. Baringo, and R. García-Bertrand. *Robust Transmission Network Expansion Planning Problem Considering Storage Units*. in *2019 International Conference on Smart Energy Systems and Technologies (SEST)*. 2019. IEEE.
404. Ruiz, C. and A.J. Conejo, *Robust transmission expansion planning.* European Journal of Operational Research, 2015. **242**(2): p. 390-401.
405. Street, A., F. Oliveira, and J.M. Arroyo, *Contingency-Constrained Unit Commitment With $n - K$ Security Criterion: A Robust Optimization Approach.* IEEE Transactions on Power Systems, 2011. **26**(3): p. 1581-1590.
406. Jiang, R., J. Wang, and Y. Guan, *Robust Unit Commitment With Wind Power and Pumped Storage Hydro.* IEEE Transactions on Power Systems, 2012. **27**(2): p. 800-810.
407. Amjady, N., et al., *Adaptive robust network-constrained AC unit commitment.* IEEE transactions on power systems, 2016. **32**(1): p. 672-683.
408. Yanıkoğlu, İ., B.L. Gorissen, and D.J.E.J.o.O.R. den Hertog, *A survey of adjustable robust optimization.* 2019. **277**(3): p. 799-813.
409. Conejo, A.J., et al., *Investment in electricity generation and transmission*. 2016.
410. Du, P., R. Baldick, and A.J.S.d. Tuohy, *Integration of large-scale renewable energy into bulk power systems.* 2017. **10**: p. 978-3.
411. Matousek, J. and B. Gärtner, *Understanding and using linear programming*. 2007: Springer Science & Business Media.
412. Bard, J.F., *Practical bilevel optimization : algorithms and applications*. Nonconvex optimization and its applications. 1998, Dordrecht ; Boston: Kluwer Academic Publishers. xii, 473 p.
413. Bussieck, M.R. and A. Meeraus, *General algebraic modeling system (GAMS)*, in *Modeling languages in mathematical optimization*. 2004, Springer. p. 137-157.
414. Soroudi, A. and T. Amraee, *Decision making under uncertainty in energy systems: State of the art.* Renewable and Sustainable Energy Reviews, 2013. **28**: p. 376-384.
415. Uzuncan, E., M.R. Hesamzadeh, and A. Balkwill, *Optimal transmission access for generators in wind-integrated power systems: stochastic and robust programming approaches.* IET Generation Transmission & Distribution, 2017. **11**(6): p. 1345-1359.
416. Faramarzi, S., M. Moradi, and A. Abedi, *Comparing the Effect of Thinking Maps Training Package Developed by the Thinking Maps Method on the Reading Performance of Dyslexic Students.* Journal of Psycholinguistic Research, 2018. **47**(3): p. 627-640.
417. *Over-Turbo website* 2018; Available from: https://overpass-turbo.eu/.
418. *European Network of Transmission System Operators for Electricity* 2018; Available from: https://www.entsoe.eu/map/Pages/default.aspx.
419. Komendantova, N., et al., *Protecting Electricity Networks from Natural Hazards*. 2016, Organization for Security and Cooperation in Europe (OSCE).
420. Nicholson, C.D., K. Barker, and J.E. Ramirez-Marquez, *Flow-based vulnerability measures for network component importance: Experimentation with preparedness planning.* Reliability Engineering & System Safety, 2016. **145**: p. 62-73.
421. Behzadian, M., et al., *A state-of the-art survey of TOPSIS applications.* Expert Systems with Applications, 2012. **39**(17): p. 13051-13069.
422. Almoghathawi, Y., et al., *A multi-criteria decision analysis approach for importance identification and ranking of network components.* Reliability Engineering & System Safety, 2017. **158**: p. 142-151.
423. *Disasters and Emergencies in Switzerland 2015*. July 2015: Bern.

424. *European Facilities for Earthquake Hazard and Risk*. 2018; Available from: http://www.efehr.org/en/hazard-data-access/Intro/.
425. *Earthquake Hazards Technical Q&A*. 2018 20.04.2018]; Available from: https://earthquake.usgs.gov/hazards/learn/technical.php.
426. Bastian, M., S. Heymann, and M. Jacomy, *Gephi: An Open Source Software for Exploring and Manipulating Networks*. 2009.
427. *Statistical Data on Switzerland 2017, .* March 2017: Neuchâte, switzerland.

Appendix

This appendix has been conducted as my final dissertation for CERG-C[1] (2017) and published in:

Abedi, A. and F. Romerio-Giudici. *Systemic Vulnerability of Swiss Power Grid to Natural Events*. in *MATEC Web Conf. 7th International Conference on Power Science and Engineering (ICPSE 2018)*. 2019.

Abedi, A. *Systemic vulnerability of Swiss power grid to natural events*. 2018 https://archive-ouverte.unige.ch/unige:118267.

[1] (Certificat de spécialisation en évaluation et management des Risques Géologiques et risques liés au climat / Specialization certificate for the assessment and management of geological and climate related risk)

Appendix A

Systemic vulnerability of a power system to natural events: a preliminary study

A-1 Introduction

Today more than ever, electrical energy has become a key commodity to any growing society. In the context of power grids, a cascading outage is a sequence of failures and disconnections triggered by an initial event, which can be caused by natural hazards, human actions the emergence of imbalances between load and generation [2].

Recent data show that climate change leads to increase number of extreme weather disasters, thus increasing the likelihood of severe impacts on power grid (big power outage, blackouts). In addition, many developments and changes in power grids such as decentralizing electricity generation, intermittent renewable generation and so on, might increase its complexity [419]. In USA, for example, the annual impact of weather-related blackouts ranges from $20 to $55 billion and the trend of such events shows that their frequency has increased over the last 30 years [7]. Therefore, evaluating the robustness of critical infrastructures (CI) is mandatory to improve their design and control systems and reduce their vulnerability to unpredictable events [33].

"Vulnerability analysis" in power systems is important so as to determine how vulnerable a power system is in case of any unforeseen catastrophic events and is used to detect and rank the most critical elements of a power grid under a variety of scenarios such as natural disasters and so on [276].

There are different forms of vulnerability, including physical, social, organizational, economic, environmental, territorial and systemic vulnerabilities [86, 87]. Among different type of vulnerabilities, physical and systemic vulnerabilities are more common in the risk and vulnerability analyses. Physical vulnerability represents the degree of loss of an element due to external pressure such as natural hazard while systemic vulnerability represents the degree of redundancy, functionality and dependency of an element in a system or the system as a whole due to failure of each element in the system or failure of interconnected systems [89]. In this work, systemic vulnerability is focused on identifying the degree of redundancy, functionality and dependency of elements inside a power grid and in the rest of this research work, vulnerability analysis means systemic vulnerability analysis.

Vulnerability analysis usually has different steps. The main goals of such an analysis are as follows [15, 41, 66, 98, 99]:

- Determine the critical components (due to their location, function, or the load they carry) that require protection,
- Identify possible undesirable events and their impacts,
- Prioritize the components based on consequence of loss e.g. the rate of important blackouts (number per year) and their severity, which is generally measured either in power lost or un-served energy,
- Identify potential and inherent vulnerabilities related to specific components or the system as a whole,
- Identify existing countermeasures and their level of effectiveness to act for managing and reducing vulnerabilities and improve their resilience,
- Estimate the degree of vulnerability relative to each component.

The goal of this preliminary study is to carry out a vulnerability analysis of a power system and the Swiss grid is used as the case study. The rest of this chapter is as follows: first, our methodology and required data are introduced in Section A-2. Then, model of Swiss power grid is presented in Section A-3. Finally, in Section A-4, different results for vulnerability analysis

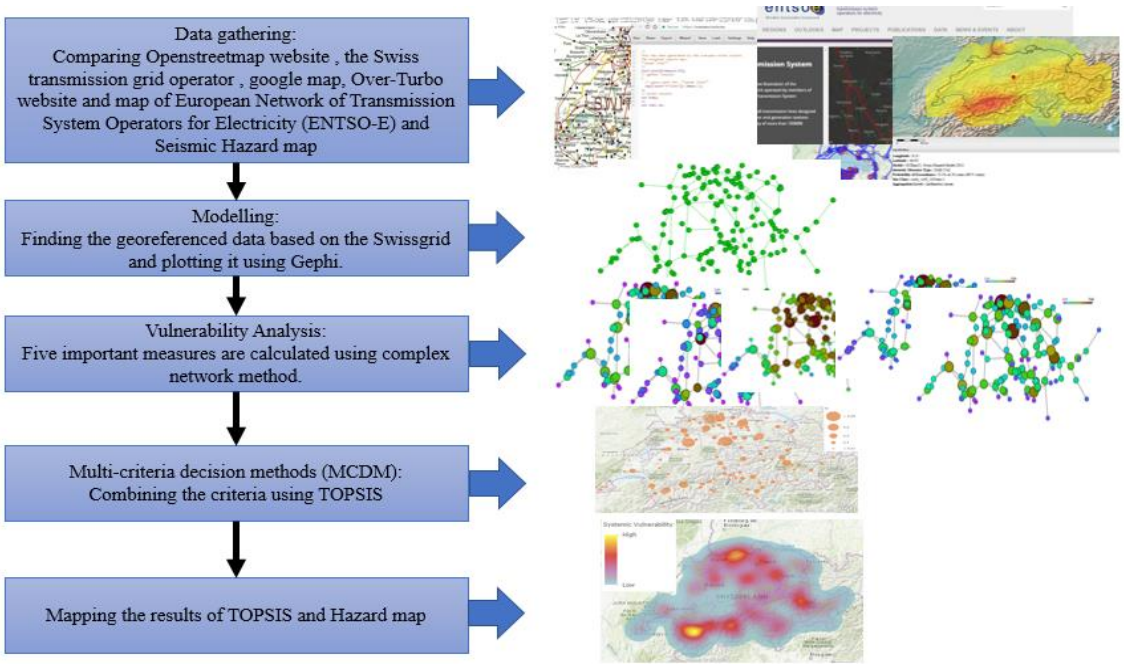

Figure A-1. Procedure of systemic vulnerability calculation due to seismic hazard.

of Swiss power grid are compared and systemic vulnerability of power grid due to seismic hazard is also presented. The conclusions and discussion will be provided in Section A-5.

A-2 Methodology and data

We will analyze the systemic vulnerability of the Swiss power grid following the scheme defined in Figure A-1. The main steps will be described in the subsequent parts.

A-2-1 Complex network method

There are two different approaches for vulnerability analysis, analytical and simulation methods [7, 95]. Analytical methods can be categorized into topological and structural methods defined as Complex Network Analysis (CNA) [181], logical methods [216], functional methods [249, 250] and flow methods [420]. All of methods are compared recently in our review paper [20]. Complex network methods are very fast and need few data while Monte Carlo methods are very slow, need many data, but have high accuracy. Characteristic of other methods are between them. In this work, Complex network analysis is selected because it is the fastest among them and can be achieved with the data at hand.

CNA is a relatively young field of research. The first systematic studies appeared in the late 1990s having the goal of studying and analyzing structure, dynamics and evolution of many complex systems.

A network in CNA is composed of a set of nodes or vertices (in reality, substations or power plants in a power system) that are connected to each other by means of links or edges, e.g., power transmission lines in a power grid [17]. In CNA, some metrics and indices (centralities) have been developed to identify that some nodes and edges are more critical or more important in a network than others are. The concept of centrality is from the idea that the closer a person to others is, the more important and critical information he/she holds. In turn, he/she has more power, and greater influence [127].

In purely complex network analysis, the basis is the mapping of buses and transmission lines of power grids to nodes and edges, respectively. The defined centralities in complex network theory are used to analyze their vulnerability. Metrics and centralities in complex network theory can be divided into two groups. The first one calculates the closeness of nodes/edges to each other such as degree and closeness centralities. The second group is based on how nodes/edges stand between the others, for instance, efficiency (shortest-path) or flow betweenness centralities [138]. However, there are other centralities that combine two above mentioned ideas such as delta centrality (or Δ centralities) [139] and combined degree-betweenness centrality [140].

***Degree*:** degree probability distribution can show topological features of a network.

$$\frac{\sum a_{ij}}{N-1} \tag{A-1}$$

***Closeness*:** closeness centrality of a node is defined as the sum of all its shortest paths and can be used to quantify how rapidly the information injected in each node spreads in the network [2].

$$\frac{N-1}{\sum d_{ij}} \tag{A-2}$$

***Betweenness*:** betweenness measures the ratio and total number of shortest paths in a graph and as a result, nodes with high values of the metric can be designated to control or regulate information flowing within a network [2].

$$\frac{1}{(N-1)(N-2)} \sum_{i \neq j \neq k} \frac{n_{jk}(i)}{n_{jk}} \tag{A-3}$$

Eigenvector Centrality: The eigenvector centrality is based on the idea that a node is important if it is connected to other important nodes [244].

$$\frac{1}{\lambda}\sum_{j=1}^{N} w_{ij} e_j \tag{A-4}$$

PageRank (PR) algorithm: The essence of PR algorithm is that the rank of a node will be certainly high if the node is linked from a high-ranked one [185].

$$\frac{1-q}{N} + q \sum_{D_{in}(p_i)} \frac{PR(p_j)}{D_{out}(p_j)} \tag{A-5}$$

Where in (A-1) to (A-5): G is the graph descriptive of the structure of the real network with N nodes, $i, j, k \in G$. a_{ij} is 1 if node i is connected to node j. d_{ij} is the shortest path from node i to node j; $n_{jk}(i)$ is the number of shortest paths that contain i; n_{jk} is the number of shortest paths from node k to node j. λ and W_{ij} are a constant and weight respectively. q is the damping factor, which would be set to 0.85, and D is equal to the number of the directed transmission lines. $D_{in}(p_i)$ is the number of in-linked webpages of webpage p_i. $D_{out}(p_j)$ is the number of out linked webpage of webpage p_j.

A-2-2 Multi-criteria decision methods (MCDM)

For vulnerability and risk analyses of complex networks, there is no holistic analysis to integrate the structural, static, dynamic, operational features and complexity of these networks and instead, the so-called reductionist methods are proposed such as complex network methods, power flow methods, logical methods, functional methods and Monte Carlo simulation. So, important or critical measures (indices) based on different definitions lead to different ranking results. Therefore, these results should be combined with approaches such as multi-criteria decision methods (MCDM) and provide a unique ranking from different measures to be useful for decision makers.

The Technique for Order Preferences by Similarity to an Ideal Solution (TOPSIS) is one of the MCDM to find a best alternative that is the closest to the positive ideal solution and farthest to the negative ideal solution [421, 422]. Figure A-2 shows stepwise of TOPSIS methodology. In this work, TOPSIS is used to combine different complex network metrics introduced in the previous subsection.

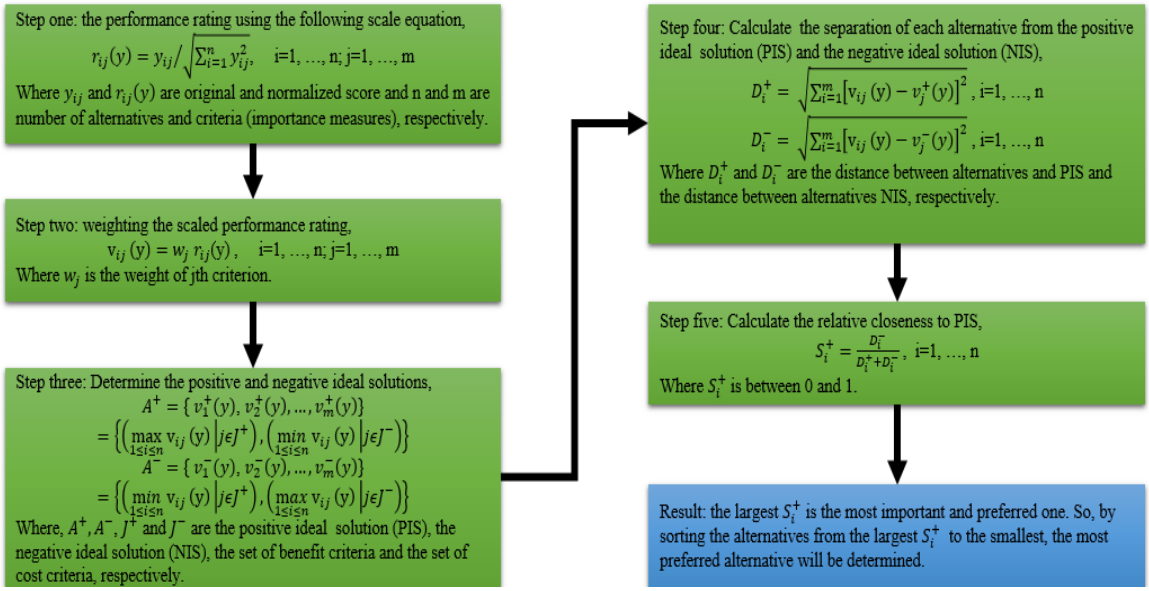

Figure A-2. Different steps of TOPSIS.

A-3 Required data

A-3-1 Seismic hazard map

According to reference [419], earthquakes, storms, floods, landslides and heat waves are among the major causes of electricity blackouts during natural disasters. These events can destroy or damage the electrical infrastructures and trigger cascading effects. Earthquake is one of the most important hazards that can impact different parts of power system such as nodes (generator, transformers, substation and control centers) and edges (overhead line and cables). It should be noted that in each country one of natural hazards are the major according to historical records and based on their frequency and impacts. Storms are more frequent in Switzerland but earthquakes are more costly [73, 423], herein, seismic hazard is selected as the scenario.

The data on seismic hazard for Switzerland and its assumptions (see Figure A-3) is provided by European Facilities for Earthquake Hazard and Risk (EFEHR) [424]. Spectral Acceleration (SA) is approximately what is experienced by a building during earthquakes. Short buildings (less than 7 stories) have short natural periods (0.2 to 0.6 sec) [425]. Buildings and structures in the case (substations and transformers) are usually in this category and have heights less than 2 stories tall. That is why 4 Hz (0.25 s) is selected for this goal. In addition, the choice of return period depends on the importance of the structure for the functioning of the society. Because a power grid is one of the most important infrastructure, one needs to consider the highest return

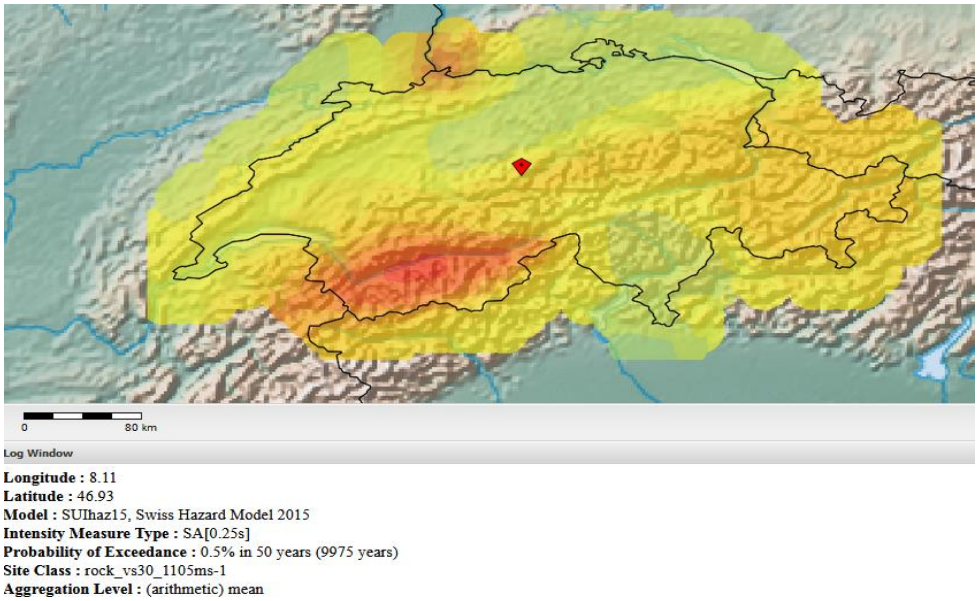

Figure A-3. Swiss seismic hazard map and its assumptions.

period as it provides the highest level of expected spectral acceleration the infrastructure will be submitted to.

A-3-2 Swiss power grid modelling

The power grid topology is achieved from comparing Openstreetmap website [416], the Swiss transmission grid operator (Swissgrid), google map, Over-Turbo website [417] and map of European Network of Transmission System Operators for Electricity (ENTSO-E) [418]. The georeferenced model based on the Swiss transmission system is plotted using Gephi (an open

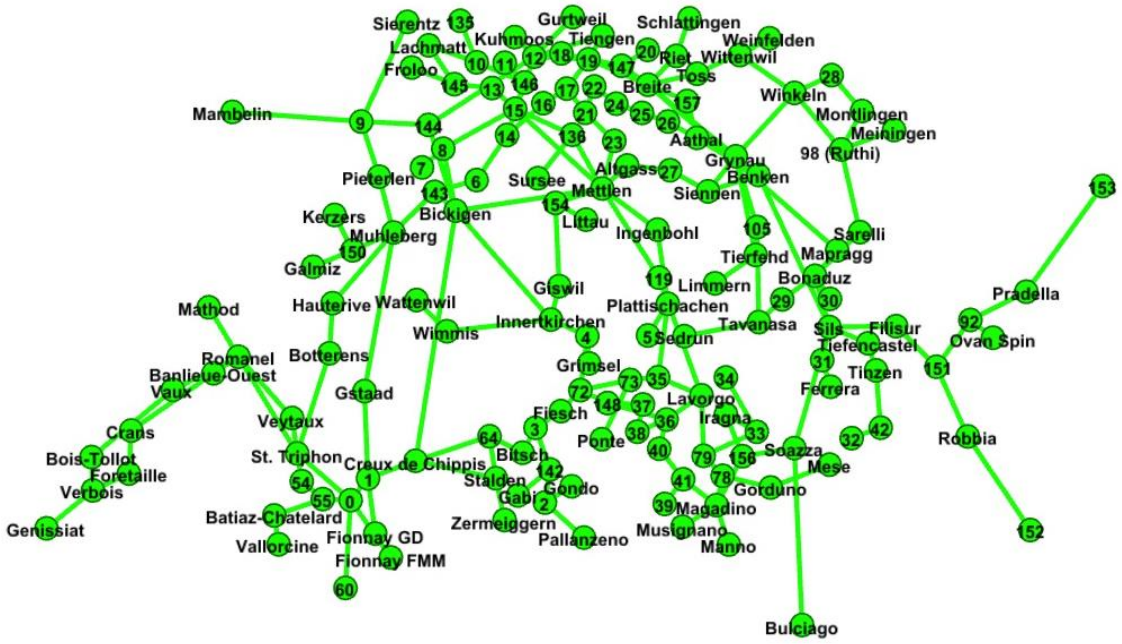

Figure A-4. Georeferenced model based on the Swiss transmission system is plotted using Gephi (an open source software).

source software) [426] in Figure A-4. A network in CNA is composed of a set of nodes or vertices (in reality, substations or power plants in a power system) that are connected by links or edges, e.g., power transmission lines in a power grid [17].

A-4 Results

Data gathering and modelling of power grid (the nodes that can be substations, power plants, etc. and the lines are assumed a straight line between nodes) are discussed in the previous sections. In this section, the modelled grid is used and at first, the five centralities for this topology are calculated. Table A-1 shows top ten important nodes in Swiss grid using different metrics.

Table A-1. Top ten important nodes in Swiss grid using different metrics

Rank	Degree	Closeness	Betweenness	Page Rank	Eigenvector
1	12	Mettlen	Bickigen	12	12
2	Mettlen	Bickigen	Mettlen	Mettlen	Mettlen
3	Breite	12	Chippis	Breite	19
4	Bickigen	144	12	Sils	15
5	19	15	Sils	Magadino	Breite
6	Grynau	Altgass	1	Grynau	Bickigen
7	Sils	19	Breite	Bickigen	Grynau
8	15	119	19	0	144
9	Muhleberg	Chippis	0	Romanel	18
10	Bonaduz	8	144	19	Tiengen

As shown in Figure A-5 and Table A-1, the results are not exactly the same because of different definitions and criteria used for the analysis. For instance, Node 12, located north of Switzerland, is the most important node according to three metrics, while for the last two metrics; it appears at the 3rd and 4th rank. The node Mettlen is another example, being at the 2nd rank for 4 metrics, and 1st in one metrics.

Therefore, depending on the criteria (indices) used, the analysis leads to different ranking results. So, these results should be combined with approaches such as Multi-Criteria Decision Methods (MCDM) in order to provide a unique ranking from different measures to be useful for decision makers (see Figure A-2). Herein, TOPSIS is used to combine different complex network metrics calculated above. Figure A-5f and Table A-2 show the results of TOPSIS.

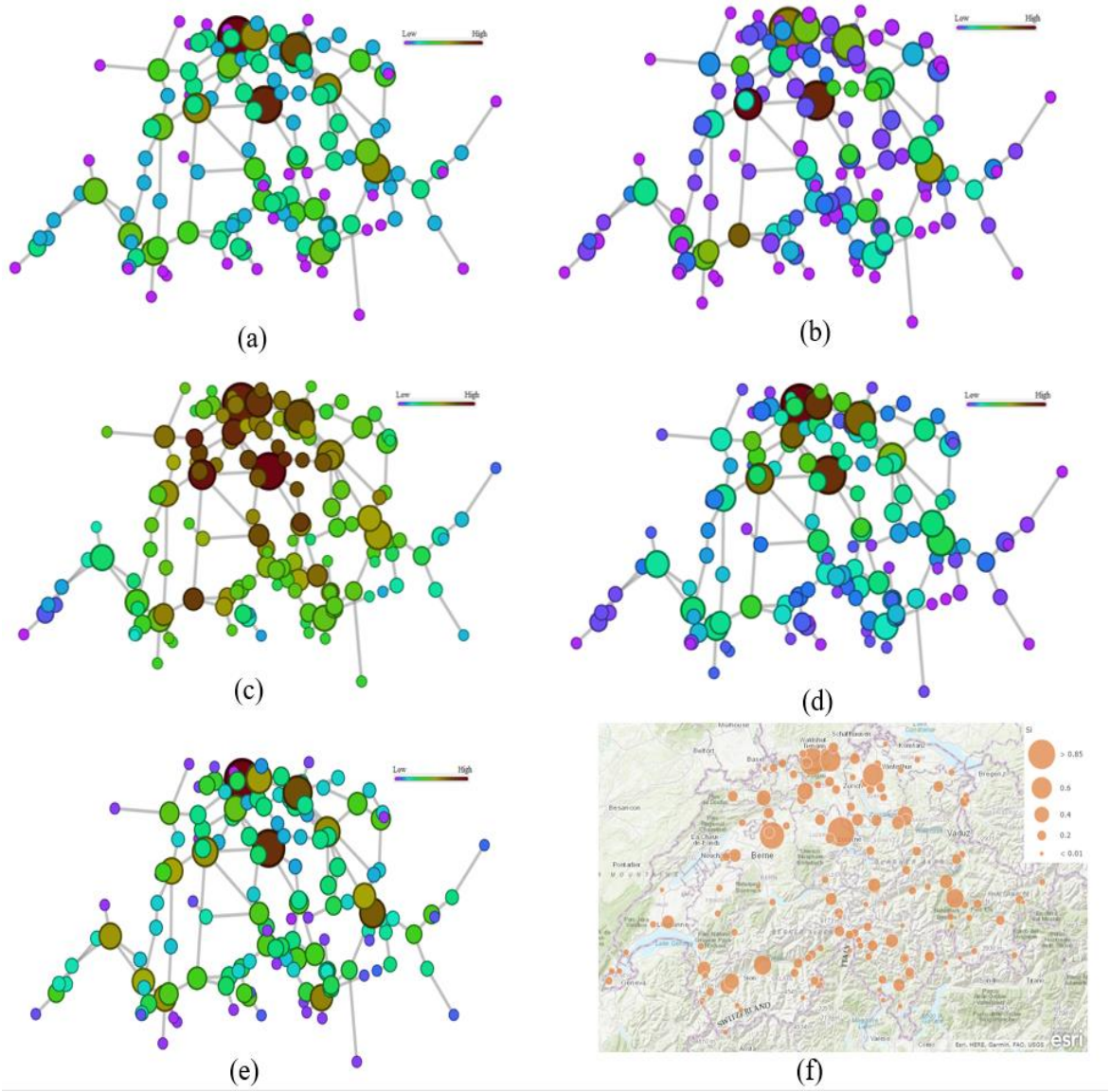

Figure A-5. Vulnerability analysis of Swiss power grid (nodes) using (a) using degree definition, (b) betweenness centrality, (c) closeness centrality, (d) eigenvector centrality, (e) PageRank centrality and (f) Combining different complex network metrics using TOPSIS. Numbers are dimensionless. The higher the value, the more vulnerable the node is.

According to the results, node Mettlen is the most important and critical node in Swiss power grid without considering its environment. The magnitudes in this figure are TOPSIS results and are dimensionless. In Figure A-5, the more one (bigger circle) is the more vulnerable node.

Finally, it is needed to consider the position of nodes in relation to seismic hazard to define what would be the most exposed nodes in case of earthquakes. In order to achieve this task, hazard data were extracted using ArcMap software from downloaded shape-file are combined by multiplying the value of the spectral acceleration as a weight with the value obtained from the TOPSIS analysis using MATLAB programming. Figure A-6 shows the most critical nodes

in regards with seismic hazard. As shown in Table A-3, node “Creux de Chippis” is the most node at risk in Switzerland when considering seismic hazard.

Table A-2. Top ten important nodes in Swiss grid using TOPSIS

Node Label	D+	D-	Si	Rank
Mettlen	0.017	0.103746	0.859205	1
12	0.028848	0.103048	0.781281	2
Bickigen	0.030411	0.10054	0.767766	3
Breite	0.04635	0.076886	0.623891	4
19	0.047667	0.077388	0.61883	5
Creux de Chippis	0.060774	0.067148	0.524915	6
Sils	0.060439	0.064619	0.516715	7
15	0.070294	0.059663	0.459099	8
Grynau	0.068742	0.056182	0.44973	9
0	0.071271	0.052385	0.423633	10

Table A-3. Top ten important nodes due to seismic Hazard

Node Label	Latitude	Longitude	Systemic Vulnerability	Rank
Creux de Chippis	46.28685	7.55782	0.536147	1
0	46.15828	7.20941	0.417621	2
1	46.18547	7.24901	0.410494	3
Mettlen	47.1154	8.33728	0.369693	4
12	47.54997	8.04951	0.339473	5
Sils	46.70475	9.46719	0.33664	6
St. Triphon	46.26626	6.97461	0.277301	7
Bickigen	47.09347	7.64759	0.273307	8
Grynau	47.22019	8.97458	0.256129	9
Breite	47.46653	8.65195	0.23326	10

Cost of blackout in different cantons during a blackout: However, blackout is a low-probability event; it should be considered because of its high economic and social impacts. Recently, a large number of people have been affected by blackout through the world, for instance, about 128 million people in Iran, the USA, Canada and Italy due to different events (2003), 670 million people in India (2012), 70 million people in Turkey (2015) and so on [3-

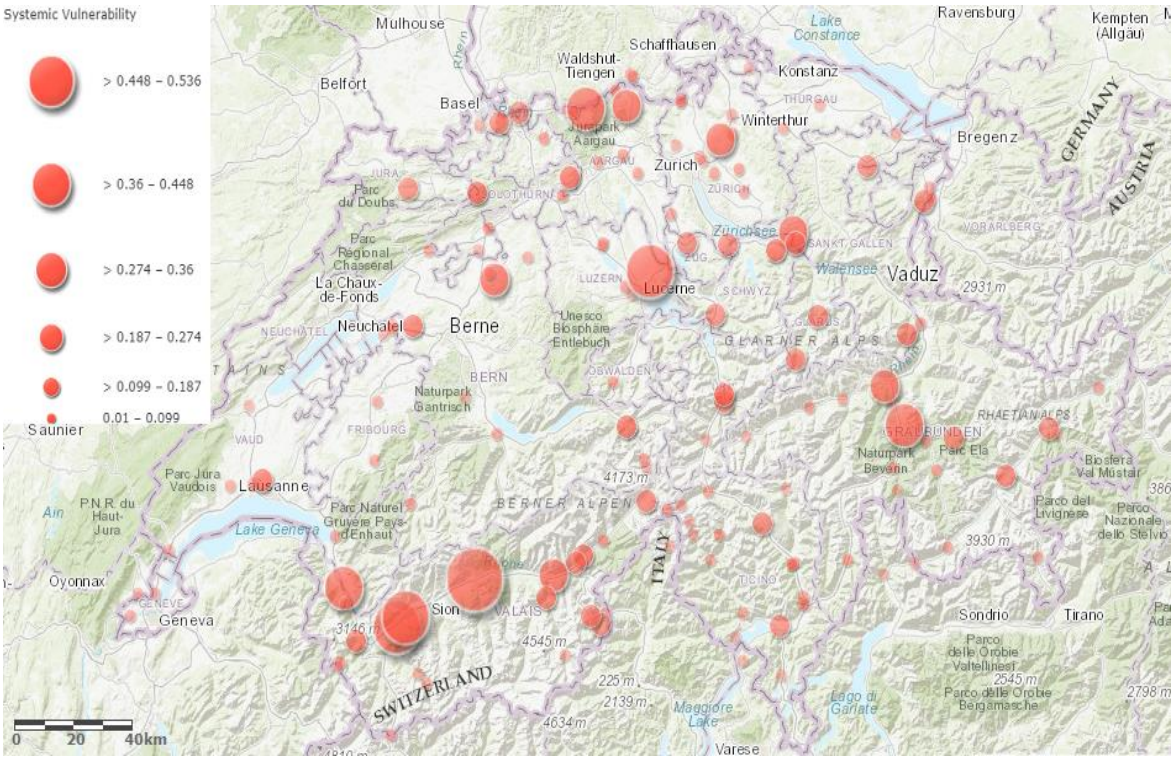

Figure A-6. Systemic vulnerability of Swiss power grid due to seismic hazard.

6]. In the USA, the annual impact/cost of weather-related blackouts ranges from $20 to $55 billion and the trend of such events shows that their frequency has increased over the last 30 years [7, 8]. In Switzerland, VSE company reported the cost of a blackout is 2-4 billion CHF per day [10, 11]. Therefore, evaluating the robustness of CIs is mandatory to improve their design and control systems and reduce their vulnerability to unpredictable events [33].

For calculating the costs of a blackout per day in different Swiss cantons, the results of above report are used. Then, using the number of population in each canton and their share in Switzerland GDP [427], the costs of a blackout are calculated. Figure A-7 shows the costs of a blackout per day in different Swiss cantons in 2020 based on VSE report in 2012.

A-5 Conclusion

"Vulnerability analysis" of power systems is used to detect and rank the most critical elements of a power grid under a variety of attack scenarios. On the other hand, the robustness of CIs must be evaluated to improve their design and control systems, and to reduce the vulnerability to unpredictable events. In this work, the main goal was calculation of vulnerability in Swiss power grid. So, it is modelled using Gephi and five different measures of complex network method such as degree, betweenness, closeness, PageRank, eigenvector centralities are

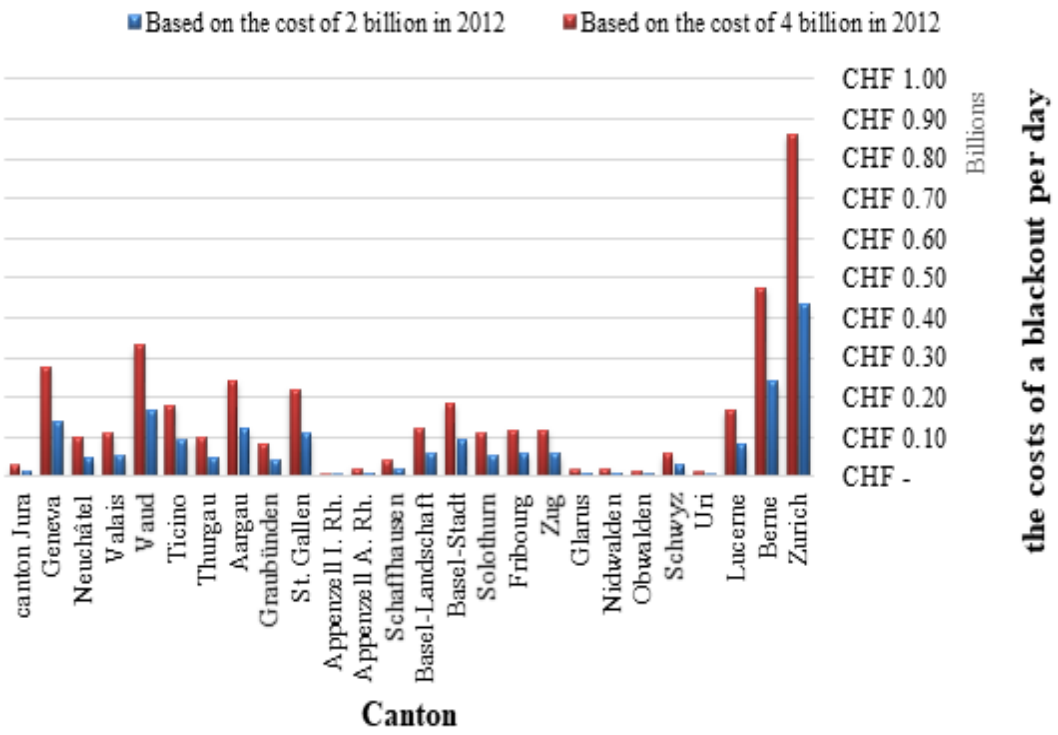

Figure A-7. The predicted costs of a blackout per day in different Swiss cantons in 2020 based on VSE report in 2012.

calculated. Then, these measures are combined using TOPSIS method and a unique importance ranking is calculated. These results are then combined with seismic hazard to identify the more exposed nodes. It is shown that important and critical nodes are different for the scenarios. Node "Creux de Chippis" is the most important node in Switzerland due to seismic hazard while node Mettlen is the most important and critical node in Swiss power grid without considering their environment.In the last section, calculation of the costs of a blackout per day in different Swiss cantons is done using the number of population in each canton and their share in Switzerland GDP. The results show that the maximum cost will be in Zurich with costs about 0.9 Billion CHF per day in 2020.