# MULTI HAZARD DISASTER RESILIENCE ASSESSMENT:

# METHODS AND IMPLEMENTATION

By

XI CHEN

A thesis submitted to the

School of Graduate Studies

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Master of Science

Graduate Program in Industrial and Systems Engineering

Written under the direction of

Elsayed A. Elsayed

And approved by

_____

_____

_____

New Brunswick, New Jersey

January 2019

ABSTRACT OF THE THESIS

Multi Hazard Disaster Resilience Assessment: Methods and Implementation

by XI CHEN

Thesis Director:

Elsayed A. Elsayed

The continuous improvements in systems engineering and the unprecedented rate of technological advances not only take the quality and reliability engineering to the forefront, but also bring the large and complex engineered systems into practical use. On the one hand, the ever-rising expectations of the customers of the reliability of products and services have enhanced the design, operation and maintenance phases during their life cycles. Moreover, cascading effects, significant damages and interruptions of services caused by failures of large and complex systems, such as telecommunication networks, power grids, transportation systems, healthcare delivery systems, information systems, financial systems and supply chain systems, have

aroused researchers' attention.

The last two decades have witnessed increasing reliance of these systems on computers, sensors, software and applications that have become targets of cyber attack and software failures with major consequences. Natural disasters and hazards such as floods, hurricanes and earthquakes particularly cause significant disruptions of the systems' services. Restorations of their functionality under limited resources and time constraints have given rise to the assessment of such systems' resilience. However, traditional reliability metrics are inadequate to assess the resilience characteristics in many applications and critical infrastructure sectors. Therefore, resilience as a new extension of reliability metrics has been gradually and widely used to evaluate the performance of large and complex systems.

Ideally, system recovery is "optimized" when all failed (and degraded) units are recovered immediately after the hazard; which is unrealistic due to the limited recovery resources and repair times needed to restore the system to its operational levels. Therefore, to recover system performance to a desired level within the shortest period, it becomes important to determine the sequence in which failed and degraded units are repaired sequentially (or simultaneously when possible). Specifically, it is necessary to obtain the criticality of the failed and degraded units during the recovery process and allocate the repair resources to the most important units which have the highest impact on the system recovery by using an importance measure (IM). IM is also used for

identifying system design weakness and component (or subsystem) failures that are crucial to the system performance, and therefore determine the allocation of redundancy or repair resources to achieve system performance improvement.

In this thesis, we provide a detailed overview of potential hazards and methods of their predictions and quantification; we present several definitions of resilience as well as methods of its assessment in different applications; we also present the development of importance measures and compare them in different scenarios; we review cascading failure occurring in systems and models of their assessment and prevention. We propose general resilience metrics for non-repairable and repairable systems and demonstrate their estimation through applications. We finally propose approaches to prioritize units of the system in order of their importance to the system functions and to optimize the maintenance resources in order to recover system performance to a desired level within the shortest period.

## ACKNOWLEDGEMENT

Firstly, I would like to express my sincere gratitude to my advisor Professor Elsayed A. Elsayed for his continuous support, patience, motivation, and immense knowledge. Professor Elsayed's guidance helped me in all the time not only of research and the writing of this thesis but also of my life. Under the profound influence of his personality, I gradually become a precise, strict, responsible, patient, and determined person, and I could not have imagined having a better advisor and mentor for my study and life. Without his patient encouragement, this thesis could not have been accomplished.

Besides my advisor, I would like to sincerely thank the rest of my thesis committee: Professor Weihong Guo who is the first person leading me to the academic research and Professor Kang Li who leads me to Rutgers University initiating my wonderful foreign life, for their insightful comments, valuable suggestions and encouragement.

I also would like to take this opportunity to thank my parents and my girlfriend for supporting me spiritually throughout writing this thesis and my life in general.

**TABLE OF CONTENTS**

## LIST OF FIGURES

## LIST OF TABLES

# CHAPTER 1

# INTRODUCTION

## 1.1 Background and Motivation of Research

System is defined as "a regularly interacting or interdependent group of items forming a unified whole" (Merriam-Webster dictionary 2018). Depending on specific compositions and structures of this group of items, every system realizes certain functions and objectives. In this thesis, we focus on engineering systems, especially large and complex systems. With the gradual improvements in systems engineering and the unprecedented rate of technological advances, systems which are becoming more interconnected from basic components to subsystems to the system of systems resulting in larger and more complex and complicated systems. Large and complex systems, such as telecommunication networks, power grids, transportation systems, healthcare delivery systems, information technology, financial systems and supply chain systems, are also increasingly being developed and utilized to achieve more functionality. Meanwhile, they are intrinsically difficult to be modeled not only due to a substantial number of subsystems and components but also the dependencies, relationships, or interactions among them under given a specific working environment.

The recent decades have also witnessed rapid advances in large and complex systems with major consequences when failures occur. Failures of such systems may result in

cascading effects and significant damages and interruptions of their services. For example, a small-scale initial power outage cascaded into a complicated sequence of dependent outages on August 10th, 1996 (Venkatasubramanian (2003)). Within a few seconds, several dozen lines had opened across the interconnection, and more than a dozen generating units went offline, leaving Oregon disconnected from California and Northern California disconnected from Southern California. This blackout disconnected power to about 7.5 million customers in seven western U.S. states, two Canadian provinces (Kosterev *et al.* (1999)). A similar failure on August 14th, 2003, resulted in a blackout of about 50 million customers in the Northeastern United States and Canada (Force *et al.* (2004)). Large blackout not only has a strong effect on shaping the regulated power systems and the reputation of the power industry but also involves social disruption that can multiply the economic damage. Moreover, some extreme events may cause possible deaths, which underscores the engineer's responsibility to work to avoid the blackout. In addition to these normal failures of components or systems, the last two decades have witnessed increasing reliance of systems on computers, sensors, software and applications that have become targets of cyber attack and software failures with major consequences. Moreover, natural disasters such as floods, hurricanes and earthquakes might also cause significant disruptions of the systems' services.

The design stage of such system is especially important in order to minimize the negative impact of the hazard, minimize system performance loss, and minimize the

length of the deterioration period, i.e., maximize the robustness of the large and complex systems. Through a rigorous and optimized configuration, engineers can maximally maintain the normal operation of the systems as long as possible and make the systems resistant or adaptive to potentially unfavorable internal or external factors so that the system performance does not degrade at a high rate. In addition to the design stage, for repairable systems, engineers also need to consider the ability to recover the systems to achieve desired performance in a short time. Improving the recovery ability of the system means that the system can recover to a desired state under limited resources as soon as possible after failures or degradations. Therefore, for large and complex systems, using a quantified indicator to assess system robustness and the recovery ability enables the designers and engineers to design robust and effective systems.

In engineering fields, reliability and its related metrics are most frequently used for system performance assessment for a specified period of time (design life) under the design operating conditions without failures (system normal failures), which are affected by its inherent characteristics such as system's design and configurations, reliability of its components, the environmental factors and their interactions and manufacturing defects. However, when systems are subjected to external disruptive events such as natural or manmade hazards, conventional reliability metrics fail to take into account the severity of the system damage and the recovery ability which implies the time and resources needed for the system to achieve a specific performance level

after the failure. This has given rise to extend the reliability metrics to “resilience” of the system, which combines conventional reliability metrics with the system robustness (design stage) and system recovery (maintenance stage) during the post-hazard period. Moreover, under most circumstances in real life, natural and manmade hazards may either be induced by some common causes or interact with each other instead of occurring independently, which has prompted the need to investigate system resilience under multi hazard.

In order to design highly reliable and repairable systems, it becomes necessary to identify how a component affects the performance of the system and to evaluate the relative importance of a component in contributing to system reliability and resilience. Specifically, importance measures (IMs) are quantitative measures of the importance of the component and are commonly defined as the rate at which system reliability improves as the component-reliability improves. These IMs enable the engineers to identify design weaknesses and determine which component merits additional research and development and take proper actions to improve system reliability at minimum cost or effort, such as adding redundancies or standbys (systems or components), cloud backup (data) and improving the reliability of some components. In repairable systems, when hazards occur, system performance does not ideally recover immediately to its pre-hazard level due to the limited recovery resources and recovery time needed to restore the failed or degraded components to their operational levels. IMs suggest the most efficient way to generate a repair checklist by prioritizing components in order of

their importance to the system functions and to optimize the maintenance resources in order to recover system performance to a desired level within the shortest period.

### 1.2 Problem Statement

Resilience means “leap back” and is used as a mechanical property of materials, namely modulus of resilience. For example, when a specimen of a ductile material is subjected to a tensile or compressive load, its stress-strain relationship shown in Figure 1 exhibits linear relationship until it reaches the elastic limit (point B). When the load is removed at this point, the specimen returns to its original condition without residual deformation. The area of the triangle ABC in Figure 1 is referred to as the modulus of resilience, which can be regarded as the ability of this specimen to absorb external energy and recover to its original condition upon the release of the load. Clearly, the specimen recovers to its original condition without repair. Therefore, the ability of a component (system) to absorb external load (stress, disruption, …) without causing damage might be defined as system resilience in terms of its design robustness. Meanwhile, when the systems need to be repaired, the recovery time, which depends on the severity of the damage and the repair resources, is another important indicator of resilience.

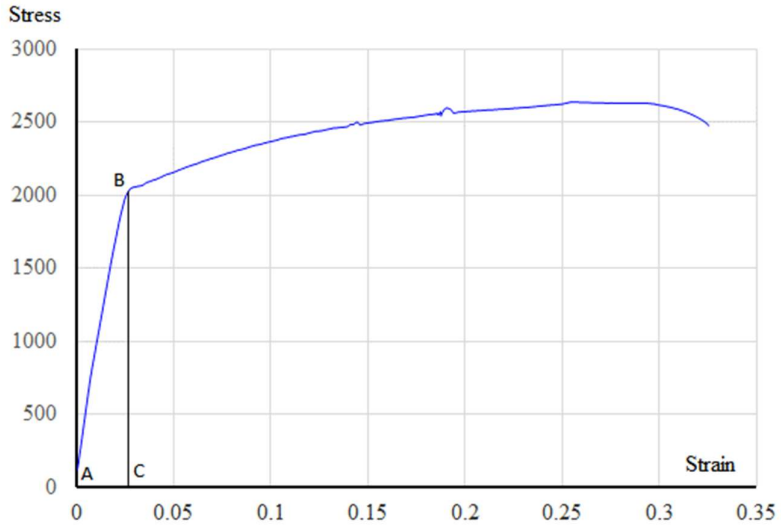



**Figure 1** Stress-strain relationship under tensile load.

In addition to resilience being a mechanical property of materials, substantial efforts have been made to improve the theories and applications of resilience of systems. However, most of the current definitions of resilience either ignore system performance recovery or system design robustness. In addition, most of the research addresses qualitative and semi-quantitative framework of resilience, which result in a limited number of quantitative methods. More limited is that most of the definitions can be only applied to specific scenarios and some even do not specify the scenarios where they can be applied, which further leads to a narrow application range. Therefore, we intend to propose a general quantified definition of resilience which considers the impact of hazards on system performance change (both magnitude and speed) during the hazard in non-repairable systems. Besides, the recovery process implemented to repairable system is a complicated process which depends on not only the system configuration and the quality and the reliability of its components but also the repair resources. In

order to more accurately define the resilience in repairable systems, we then propose another resilience quantification measure which considers the system design robustness as well as its recovery ability by incorporating the exact recovery process. Similar to reliability, the proposed definitions of resilience bound their values between 0 and 1.

Similar to resilience, IMs have been extensively studied and are already mature and can be applied to different system configurations. However, there are still systems where IMs do not adequately and effectively distinguish the importance of components. Accordingly, we intend to compare representative IMs in non-repairable systems and modify them to be more effective and adaptable to these systems. Then we propose a new IM for repairable systems by introducing availability, which provides a better and more comprehensive guidance for the engineers to design and maintain systems. Moreover, we incorporate other features of a component in the IMs to reflect the criticality of the component in system design and repair.

### 1.3 Thesis Organization

This thesis is organized as follows. Chapter 2 provides a thorough review of literature on multi hazard, resilience definition and quantification, the commonly used IMs and review of the cascading failures. More specifically, we introduce the hazard classification, and prediction of its occurrence frequency and severity; we provide a comprehensive literature review on system resilience definitions and assessment, the

development of IMs and the impact of cascading failures on the overall systems performance. In chapter 3, we propose two general quantifications of system resilience for non-repairable and repairable systems, respectively. In repairable systems, we present the exact recovery process, which demonstrates the improvements of the system performance level (say availability) with time. Chapter 4 addresses IMs for non-repairable and repairable systems by assigning different weights to systems components. Chapter 5 presents applications of the proposed resilience and IMs in non-repairable and repairable cyber networks. In Chapter 6 we provide summary and areas for future research.

# CHAPTER 2

# LITERATURE REVIEW

In this chapter, we provide a detailed overview of multi hazards and related methods of their predictions and quantification. We also discuss the definitions and assessment and the development of resilience and the importance measures of the systems' components. We begin this chapter with the classification and identification of the hazards and proposed measures to obtain the overall system's failure rate in section 2.1. We then provide details of the natural hazard from the views of classifications, prediction of occurrence frequency and severity, system performance assessment, hazards mitigation, and system recovery in section 2.1.1. In section 2.1.2, manmade hazards are discussed especially physical manmade hazards and cyber attacks. Specifically, in section 2.1.2.2, we present the definitions of cyber attack and the prediction of its frequency and severity. Then the dependency between natural hazard and manmade hazard is considered in the system performance analysis in section 2.1.3. In section 2.2, we present several qualitative and semi-quantitative framework of resilience as well as methods of its assessment in different applications. We provide the development of the importance measures in section 2.3. We finally discuss the cascading failure in terms of its definition, prevention and models of their assessment in different scenarios to improve the system resilience in section 2.4. A thorough review of the literature shows that the methods to obtain the overall system's failure rate from different type of hazards needs to be improved and most of the resilience definitions only have qualitative and

semi-quantitative frameworks, which promotes the investigation of a generalized and quantitative definition of resilience. Moreover, the applications of importance measures are limited to specific scenarios and cascading failures which are enough to cause major consequences are necessary to be taken into account when evaluating the system performance.

### 2.1 Multi Hazard

The failure rate of the system depends on its configuration, failure rates of its subsystems or components, external loads and environmental conditions. We refer to this failure rate as the normal failure rate (hazard rate). In general, the normal failure rate varies over the life cycle of the system as demonstrated by the bathtub-shaped failure curve. When the failures occur due to natural phenomena that have negative effects, namely natural hazards, such as earthquakes, volcanic eruption, hurricanes, tornados, floods, torrential rains, solar flares and others, we refer to the failure rate of these sources as a natural failure rate. By contrast, manmade hazards are hazards caused by human actions or inactions such as physical-attacks, manmade fires, cyber attacks and others. We refer to their corresponding failure rate as manmade failure rate.

Therefore, the overall system's failure rate should include all the three types of failure rates: normal, natural and manmade. Meanwhile, the frequency and severity of hazards need to be reflected as well. Moreover, under some circumstances, the hazards are

hierarchical and dependent on each other. Without loss of generality, we express the system's failure rate in the additive form in Eq. (2.1):

$$\begin{aligned}\lambda_{\text{system}} = \lambda_{\text{normal}} &+ \sum_{i=1}^{n_i} (I_i^{\text{natural}} \cdot \lambda_i^{\text{natural}}) + \sum_{j=1}^{n_j} (I_j^{\text{manmade}} \cdot \lambda_j^{\text{manmade}}) \\ &+ \sum_{i=1}^{n_i} \sum_{i'=i}^{n_i} (I_{i,i'}^{\text{natural}} \cdot \lambda_{i,i'}^{\text{natural}}) + \sum_{j=1}^{n_j} \sum_{j'=j}^{n_j} (I_{j,j'}^{\text{manmade}} \cdot \lambda_{j,j'}^{\text{manmade}}) \\ &+ \sum_{i=1}^{n_i} \sum_{j=1}^{n_j} (I_{i,j}^{\text{natural·manmade}} \cdot \lambda_{i,j}^{\text{natural·manmade}})\end{aligned} \tag{2.1}$$

where

$\lambda_{\text{system}}$ is the overall system's failure rate;

$\lambda_{\text{normal}}$ is the system's normal failure rate;

$I_i^{\text{natural}}$ is the index indicating the occurrence of the $i^{th}$ natural hazard;

$I_i^{\text{natural}} = 1$ if the hazard occurs and 0 otherwise;

$I_j^{\text{manmade}}$ is the index indicating the occurrence of the $j^{th}$ manmade hazard;

$I_j^{\text{manmade}} = 1$ if the hazard occurs and 0 otherwise;

$I_{i,i'}^{\text{natural}}$ is the index indicating the occurrence of the $i^{th}$ and $i'^{th}$ natural hazards;

$I_{i,i'}^{\text{natural}} = 1$ if both $i^{th}$ and $i'^{th}$ hazards occur and 0 otherwise;

$I_{j,j'}^{\text{manmade}}$ is the index indicating the occurrence of the $j^{th}$ and $j'^{th}$ manmade hazard;

$I_{j,j'}^{\text{manmade}} = 1$ if both $j^{th}$ and $j'^{th}$ hazards occur and 0 otherwise;

$I_{i,j}^{\text{natural·manmade}}$ is the index indicating the occurrence of the $i^{th}$ natural hazard and $j^{th}$ manmade hazard; $I_{i,j}^{\text{natural·manmade}} = 1$ if both the $i^{th}$ and $j^{th}$ hazards occur and 0 otherwise;

$\lambda_i^{\text{natural}}$ is the system's failure rate due to the $i^{th}$ natural hazard, which reflects the severity of the hazard;

$\lambda_j^{\text{manmade}}$ is the system's failure rate due to the $j^{th}$ manmade hazard, which reflects the severity of the hazard;

$\lambda_{i,i'}^{\text{natural}}$ is the system's failure rate due to the occurrence of $i^{th}$ and $i'^{th}$ natural hazards; $\lambda_{i,i'}^{\text{natural}}$ reflects the joint severity of the $i^{th}$ and $i'^{th}$ hazards;

$\lambda_{j,j'}^{\text{manmade}}$ is the system's failure rate due to the occurrence of $j^{th}$ and $j'^{th}$ manmade hazards; $\lambda_{j,j'}^{\text{manmade}}$ reflects the joint severity of the $j^{th}$ and $j'^{th}$ hazards;

$\lambda_{i,j}^{\text{natural·manmade}}$ is the system's failure rate due to the occurrence of the $i^{th}$ natural hazard and the $j^{th}$ manmade hazard; $\lambda_{i,j}^{\text{natural·manmade}}$ reflects the joint severity of the $i^{th}$ and $j^{th}$ hazards;

$n_i$ is the total number of natural hazards under consideration;

$n_j$ is the total number of manmade hazards under consideration.

Generally, system's normal failure rate is predominantly determined by the system design and configuration and can be obtained by failure rates of system's components and engineering experience. The occurrence frequency of natural and manmade hazards are influenced by the geographical location, time (e.g., season), population density and others. Natural and manmade failure rates, depending on specific circumstances, are unstable and vary with time. Thus, it can be seen that hazards are complex and vary greatly in their frequency, severity, duration and the affected area. For example, earthquakes occur with low frequency while heavy rainfall is one of the most frequent

and widespread weather hazard; earthquakes occur only in few seconds while heavy rainfall takes place over a period of weeks or longer; heavy rainfall has local impacts with little damage whereas earthquakes cause impacts over a large region with tremendous loss. Moreover, the speed of recovery varies in different areas: for example, the recent hurricane Harvey caused severe damage but the city of Houston began the recovery immediately whereas hurricane Maria "destroyed" the entire island of Puerto Rico which was unable to begin the recovery process for weeks. Therefore, occurrences of these hazards may result in a catastrophic damage to the system and degradation of its performance, which impact the design of system that can withstand such hazards with minimal interruptions to its functions and rapidly recover its performance to the desired level. Accurate predictions of occurrence frequency and severity of these types of hazards are critical in the estimation of the overall failure rate of a system. Besides, identifying the interdependency among hazards is necessary, i.e., the probability that one hazard triggers another and the system's failure rate induced by the occurrence of two interdependent hazards. Currently, hazard identification is mainly based on experience, historical data, forecasting, subject matter expertise, and other available resources.

### 2.1.1 Natural Hazards

The natural hazards are classified by Department of Regional Development and Environment *et al.* (1990), Burton (1993) and Kusky (2003) and given as

1) geophysical such as avalanches, earthquake, coastal erosion, lahar, landslide, sinkholes, tsunamis and volcanic activity;
2) hydrological such as floods;
3) climatological such as extreme temperatures, drought and wildfires;
4) meteorological such as blizzard, hailstorm, cyclones and storms/wave surges, tornado;
5) biological disease such as epidemics and insect/animal plagues.

More detailed classifications, descriptions, connections, damages, impacts, and responses are presented in references by White (1974), Alexander (1993), Godschalk *et al.* (1998), Lewis (2014), Islam and Ryan (2015), Willis *et al.* (2016), Krausmann *et al.* (2016), Montz *et al.* (2017), Montz *et al.* (2017), Haddow *et al.* (2017), Nigg and Mileti (1997) and Preston *et al.* (2016).

The sudden occurrences of hazards interrupt the normal functioning of the systems, which urge the designers of such systems to provide safeguards that prevent these risks as much as possible. Accordingly, the catastrophic consequences of the natural hazards have motivated researchers to develop prediction models for the occurrence frequency and severity of the hazard. A contextual model is proposed by Mitchell *et al.* (1989) and shows that the frequency and severity of the natural hazard are strongly influenced by environmental, sociocultural, economic, and political contexts in which the hazard occurs. Coppola (2006) states that physical location is the primary factor dictating what

natural hazards a nation faces; while economic, industrial, and sociopolitical factors dictate manmade hazards origin. Bonaiuto *et al.* (2016) find that the attachment of individuals to a place plays a more significant role in natural hazard risk management and conclude that (1) strongly attached individuals perceive natural environmental risks but underestimate their potential effects; (2) strongly attached individuals are unwilling to relocate when facing natural environmental risks and are more likely to return to risky areas after a natural environmental disaster and (3) place attachment acts both as a mediating and moderating variable between risk perception and coping. Preston *et al.* (2016) propose that seasonal predictions of hurricane activity based on three basic methods: statistical methods, analog methods, and dynamical methods. Quantitatively, Di Mauro *et al.* (2006) assess multi-risks situations by using multi-risk maps and provide a consistent response to the emerging concern of public authorities and stakeholders involved in regional risk management.

Specific hazards such as volcanic hazards are investigated individually. For example, Marzocchi *et al.* (2004) estimate eruption probability of volcanic hazard in both long-term and short-term via an event tree by using the Bayesian approach. Marzocchi and Zaccarelli (2006) analyze the statistical distribution of eruptive frequency and volume (both “open” and “close” conduit systems) and build a general probabilistic model to assess volcanic hazard and to constrain the physics of the eruptive process. Marzocchi and Woo (2007) propose a strategy to integrate a probabilistic scheme for volcanic eruption forecasting and cost-benefit analysis. Marzocchi *et al.* (2010) present a

Bayesian event tree to estimate volcanic hazard, which shows the intrinsic stochastic nature of volcanic eruptions and enables the calculation of the probability of any kind of long-term hazards. Marzocchi and Bebbington (2012) review probabilistic eruption forecasting which quantifies inherent uncertainties of volcanic systems for planning rational risk mitigation actions during a short-term (hours to weeks or months) and long-term (years to decades). Garcia-Aristizabal *et al.* (2013) propose a quantitative framework to calculate the probabilities of volcanic unrest by integrating the stochastic models of eruption occurrence into a Bayesian event tree scheme. Bebbington (2013) proposes a method to assess the quality of a suite of eruption forecasts by converting the forecast of the next eruption onset into a probability distribution for the elapsed time since the forecast is made. Moreover, for some other types of hazards. Temesgen *et al.* (2001) evaluate the occurrence rate of landslide and their statistical relationship with various event controlling parameters which are converted into risk susceptibility priority numbers (between 0 and 1) by using geographic information system (GIS) and remote sensing techniques. Poelhekke *et al.* (2016) develop a method to construct a probabilistic Bayesian Network to be used as part of an Early Warning System to predicate coastal hazards for sandy coasts.

Once the inevitable natural hazards occur, system performance assessment, hazards mitigation, and system recovery become the main problems of concern. Therefore, it becomes critically important to design systems that can withstand such hazards with minimal interruptions to its functions and are capable to rapidly recover its performance

to the desired functioning level. Variety of measurements are adopted to describe system's performance in different domains. For example, the number of normal working components (stations) is a measure the performance of an electric power system and the number of passengers delivered in airport terminals is a performance measure for an airport. Unesco (1972) first quantitatively defines risk as the possibility of a loss (including loss of life, loss of property, or loss of productive capacity, etc.), which consists of factors in Eq. (2.2)

$$\text{Risk} = (\text{Value}) \cdot (\text{Vulnerability}) \cdot (\text{Hazard}) \tag{2.2}$$

where "Value" represents the number of human lives at stake, or capital value (land, buildings, etc.), or productive capacity (factories, power plants, agricultural land); "Vulnerability" is a measure of the proportion of the value, which is likely to be lost as a result of a given event; "Hazard" in the estimation of risk is the type of hazards, e.g. volcanic hazard, which is the probability of any particular area being affected by a destructive event within a given period of time. The impact of the natural hazard on system performance is modeled quantitatively and qualitatively by Bebbington *et al.* (2008) and McColl *et al.* (2012). Schmidt *et al.* (2011) develop a generic software framework for modeling risks from different natural hazards and for various elements at risk. Similarly, Bell and Glade (2011) develop a general methodology to analyze natural risk for multiple processes. Krausmann *et al.* (2016) provide a comprehensive introduction to qualitative and quantitative risk assessment of natural hazard. Clarke

and Obrien (2016) develop a reliability stress test framework for critical transport infrastructure to predict the response of transportation networks to natural hazard. Artioli *et al.* (2017) suggest that system performance can be improved in the design stage. Moreover, The natural hazard mitigation is discussed by Godschalk *et al.* (1998), followed by its validation in Gall *et al.* (2011) and Chang (2003).

The quantification of risk assessment and management under natural hazard have gained importance in many disciplines. For example, Duenas-Osorio and Vemuru (2009) study the impact of cascading failures due to natural hazard on complex power infrastructure systems. Specifically, Billinton and Singh (2006) and Liu and Singh (2010a) analyze the weather-associated impact on power systems in terms of reliability, where it is assumed that no repair is conducted during the hazard. Liu and Singh (2010a) analyze the impact of hurricane on composite power system reliability using common cause failure; similar to Billinton and Kumar (1981). Additional research on the evaluation of power system reliability under weather-related hazard is conducted by Billinton and Bollinger (1968), Liu and Singh (2010b), Billinton *et al.* (2002), Billinton and Cheng (1986), Billinton and Acharya (2005) and Bhuiyan and Allan (1994). Moreover, Van Westen *et al.* (2006) conclude a number of new advances and challenges for quantifying landslide risk over larger areas. Steinberg *et al.* (2008) provide an overview of the state of the art in Natech risk assessment and management under natural hazard. National Research Council *et al.* (2011) and National Research Council *et al.* (2014) examine risk reduction strategies to address coastal storms (hurricanes, tropical

storms, and extratropical storms) and associated storm surges, including reducing the probability of flooding or wave impact and the number of people or structures in areas at risk or making them less vulnerable to coastal storms. In addition, there are other natural hazards studies such as dam and levee failures (National Research Council (2012)), volcanic hazard (National Academies of Sciences Engineering and Medicine (2017)) and the earthquake (National Research Council (2011)). More studies on multi-risk assessment and management under natural hazard are presented in Temesgen *et al.* (2001), Pitilakis *et al.* (2014), Lee and Ellingwood (2017), Dindar *et al.* (2016), Gallina *et al.* (2016), Ran and Nedovic-Budic (2016), Eidsvig *et al.* (2017), Dindar *et al.* (2016), Thierry *et al.* (2008), Asprone *et al.* (2010), Perry and Lindell (2008), and Granger *et al.* (1999).

Although mitigating the damage of the disaster is important, the recovery after the disaster is also critical, and they jointly make up the resilience of the system. Institute of Medicine (2015) focuses on the recovery process after the disaster. Hanfling *et al.* (2012) investigate the care that the state and local governments, the hospital and alternate care systems should provide after the disaster. Barben (2010) assumes a repair rate equal to the one during normal weather condition and Billinton and Singh (2006) assume that the repair rate is higher than that under normal weather condition. In many fields, researchers have spent significant effort to improve the system resilience. Cutter *et al.* (2008) provide a new framework, the disaster resilience of place (DROP) model, designed to improve comparative assessments of disaster resilience at the local or

community level. Cutter *et al.* (2013) discuss the natural hazard risk, the necessity and measures of resilience improvement in terms of policy and actions. Power infrastructure, in particular, Panteli and Mancarella (2015) assess the resilience of critical power infrastructure under severe weather events by introducing Sequential Monte Carlo based time series simulation model to quantify the random nature and impact of weather. Espinoza *et al.* (2016) first present a four-phase resilience assessment framework of critical infrastructures and estimate the windstorm and rainfall frequency and severity by taking the effect of time and location into consideration. Preston *et al.* (2016) analyze the risk and resilience of the U.S. electricity system and synthesize different natural and manmade hazards to the electricity system including information on known trends, predictability, and mitigation options to assess the risk to various system components and identify key opportunities and constraints for enhancing resilience. An introduction to the resilience of electricity systems under multi hazard and a framework of system resilience protection strategies are provided in Preston *et al.* (2016).

In fact, many examples suggest that one natural hazard usually triggers or increases the probability that more other natural hazards and many hazards are related (Gill and Malamud (2014)). For example, submarine earthquakes can cause tsunamis, and hurricanes can lead to coastal flooding and erosion; heavy rainfall may induce both flood and mudslide in the same region; floods and wildfires can result from a combination of geological, hydrological, and climatic factors; and of course, there may also be interactions between natural hazards and anthropic processes. For example,

groundwater abstraction may trigger groundwater-related subsidence (Galloway *et al.* (1999)). Therefore, it is realistic and practical to consider multiple hazards and their interactions in risk estimation. Kappes *et al.* (2012) present an outline of the challenges each step of a multi-hazard (risk) analysis poses and present current studies and approaches that face these difficulties. Gill and Malamud (2014) present the importance of constraining hazard interactions and reinforce the importance of a holistic (or multi hazard) approach to natural hazard assessment by synthesizing and using accessible visualization techniques, large amounts of information drawn from many scientific disciplines to (1) identify ninety interactions among multiple natural hazards; (2) subdivide the interactions into three levels, based on secondary hazards, given information about the primary hazard; (3) determine the spatial overlap and temporal likelihood of the triggering relationships occurring; and (4) examine the relationship between primary and secondary hazard intensities for each identified hazard interaction and group these into five possible categories. Liu *et al.* (2016a) develop a systematic hazard interaction classification by dividing geophysical environmental factors in the hazard-forming environment into (1) factors that are relatively stable which construct the precondition for the occurrence of natural hazards and (2) trigger factors which determine the frequency and magnitude of hazards. This classification not only fills the gap in current multi hazard risk assessment methods which not only consider domino effects, but also can effectively calculate the probability and magnitude of multiple interacting natural hazards occurring together. Indeed, it is realistic and practical to consider multiple natural hazards and their interactions as some of them are induced by

common causes. More research on natural hazard modeling with interactions between multiple natural hazards are presented in Gill and Malamud (2017), Poursanidis and Chrysoulakis (2017), Marzocchi *et al.* (2009), Tarvainen *et al.* (2006), Marzocchi *et al.* (2012), Carpignano *et al.* (2009), Di Mauro *et al.* (2006), Frolova *et al.* (2012), Gill and Malamud (2014), Eshrati *et al.* (2015), and Flanagan (2001).

### 2.1.2 Manmade Hazards

In contrast to natural hazards, manmade hazards are the results of human actions (intent, negligence or error). For example, the physical infrastructure may be subjected to manmade hazard of terrorism (Stewart *et al.* (2006)) and the fossil energy chains are under the risk of energy interruption by human actions (Burgherr and Hirschberg (2008)). Specifically, manmade hazards can be classified as physical manmade hazards and cyber attacks. Similarly, the frequency and subsequent damage of these hazards are necessary to be analyzed.

#### 2.1.2.1 Physical Manmade Hazards

Tansel (1995) presents that typical types of physically manmade hazards include fire, energy interruption, nuclear accidents and terrorism. For example, Buchanan and Abu (2017) consider the fire hazard in the design stage of structures and infrastructures. More specifically, the fire hazard in bridges is comprehensively reviewed in terms of

its frequency, its impact on bridge structure design, fire hazard preparedness, damage assessment and recovery and is presented by Kodur *et al.* (2010). The bridge structure is investigated under extreme events such as ship collision (Ghosn *et al.* (2003)). Bridge replacement under and after the emergency is also proposed by Bai *et al.* (2006). Bridge importance factor under fire hazard is analyzed to determine its critical parts and assess its vulnerability during the hazard (Kodur and Naser (2013)). More theoretical and numerical approaches for evaluating bridge performance and damage under fire hazard are presented in Aziz and Kodur (2013), Bennetts and Moinuddin (2009), Alos-Moya *et al.* (2014), Mendes *et al.* (2000) and Payá-Zaforteza and Garlock (2012).

Since most of the network systems such as power grid, telecommunication, information technology, air traffic control systems, air defense systems and others are subject to manmade hazard; more specifically cyber attacks, we highlight this hazard in details below.

#### 2.1.2.2 Cyber Attack Hazard

With the rapid development of technology, cyber is becoming increasingly important to human's daily life and the national security. However, as attackers maliciously manipulate or attack the cyber to access information and destroy specific targets, cyber attacks start to attract researchers' attention. The Joint Chiefs of Staff provide a military definition of cyber attack as "a hostile act using computer or related networks or

systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions" (Cartwright (2011)). Similarly, Hathaway *et al.* (2012) define that cyber attack mainly targets national and political security, i.e., cyber attack is "any action taken to undermine the functions of a computer network for a political or national security purpose". Lin (2015) defines cyber attack as "any type of offensive maneuver employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system". More definitions on cyber attacks are provided in Zhu *et al.* (2011), Li *et al.* (2012), Waxman (2011), Shackelford (2009), Mowbray (2013), Kovacevic and Nikolic (2014), Mezher *et al.* (2016), Pan *et al.* (2015), Gandhi *et al.* (2011), Kumar (1995), and Li *et al.* (2012).

Statistical data reveals that cyber attack occurs with high-frequency and typically causes serious loss. The targets of cyber attack range from direct personal assaults, monetary theft and trade secrets from companies, to national infrastructures or political secrets. For example, approximately 77 million accounts in Sony's PlayStation were hacked in 2011, resulting in that massive personal information theft and a loss of approximately 171 million dollars. The most famous cyber attack is that the joint U.S.-Israel project, "Stuxnet", in 2010, which is a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not

destroy, Tehran's ability to make its first nuclear arms (Times (2011)). In 2013, the Deseret News reported Utah's secure government networks face as many as 20 million cyber attacks each day. Therefore, cyber security has become a matter of global interest and has become part of worldwide security issue. More than 50 countries such as Canada (Government of Canada (2010), USA (White House Office United States (2011)), UK (MOD (2011)), China (Dreyer (2015)) have outlined their official stances on cyber security (Klimburg (2012)).

Cyber attack prediction is one of the critical factors in cyber security in order to avoid and prepare for cyber attacks. In the following, we introduce representative studies on cyber attack prediction in terms of frequency and severity.

Passeri (2018) analyzes cyber attack statistically in 2017. A comprehensive comparison between the cyber attack (and cyber security) data in 2017 and 2016 is conducted from different aspects. Detailed comparisons presented in Figures 2.1 and Figure 2.2, show that prediction of cyber attack occurrence is critical to cyber security. Both recurrent and perceptron neural networks have been used to predict the cyber attack from historical data as presented in Debar *et al.* (1992) and Ghosh *et al.* (1999). Qin and Lee (2004) propose an approach to predict the potential attacks based on observed attack activities. Liu (2005) develops an automatic game-theory-based attack prediction method, which quantitatively predicts the likelihood of (sequences of) attack actions. Arora *et al.* (2006) empirically link the cyber attack frequency with vulnerability

disclosure and state that patched vulnerabilities attract more attacks than unpatched ones. Kim *et al.* (2008) propose a statistical method for prediction and modeling of cyber attack signal. Yang *et al.* (2009) introduce an information fusion approach to provide situation awareness and threat prediction from massive volumes of sensed data. Khalili *et al.* (2010) present methodologies for understanding the mission risks based on Information Technology (IT) infrastructure to predict the occurrence of cyber attacks and assess its impact. Knowing the vulnerability paths, Jajodia and Noel (2010) predict cyber attacks origin and impact. Kim and Hong (2011) use early warning model to predict politically motivated cyber attack before that attack happens with online and offline patterns. Wu *et al.* (2012) propose a cyber attack prediction model based on the Bayesian network. Kotenko and Chechulin (2013) suggest a framework for cyber attack modeling and impact assessment as well as predict cyber attack actions. Zhan *et al.* (2013) propose a statistical framework and use the gray-box prediction to predict the incoming cyber attack based on a stochastic process. As a generalization, Zhan *et al.* (2015) use extreme value theory for long-term cyber attack predictions (twenty-four hours ahead) and gray-box time series theory for short-term prediction (one hour ahead) with an accuracy of 86%–87.9%. Das *et al.* (2013) propose an i-HOPE framework to predict the likelihood of a cyber breach. Silva *et al.* (2014) propose One Point Analysis (OPA) for aggregating peaks of a burst-specifically for the brute force attack at a single point. Chen *et al.* (2016) describe a Proactive Cybersecurity System (PCS), using big data and processing tools to identify potential cyber attacks.

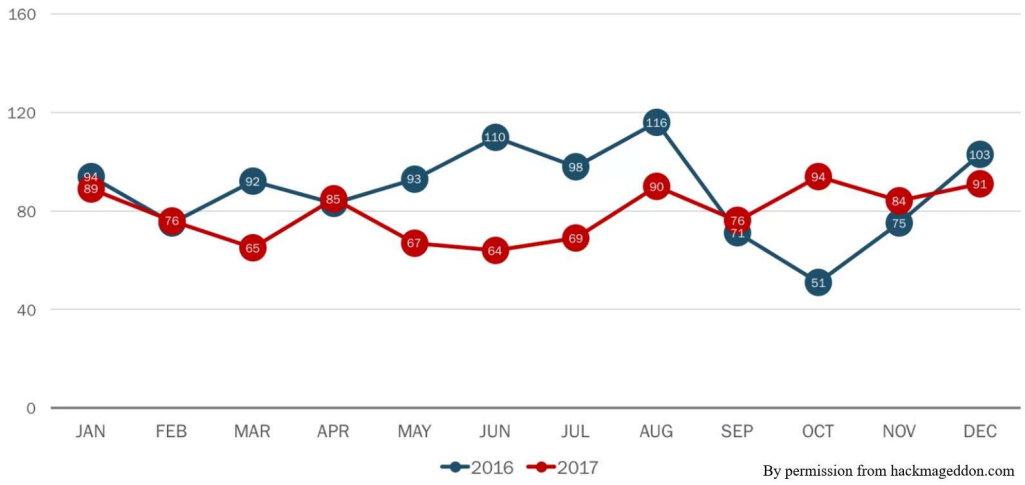



**Figure 2.1** Monthly cyber attacks (2017 vs 2016) (Passeri (2018)).

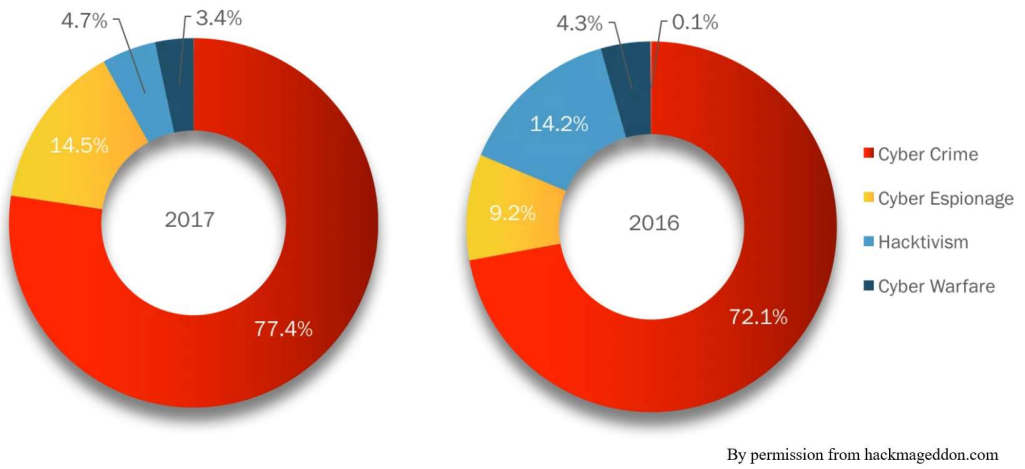



**Figure 2.2** Motivations behind cyber attacks (2017 vs 2016) (Passeri (2018)).

Besides frequency, the severity (impact) of cyber attack is also worthy of discussion to take effective measures and strategies to mitigate the cyber attack damage. Shaw (2003) presents perturbation analysis and develops a workflow model to predict the impact of cyber attacks on Battle Management/Command, Control, and Communications (BMC3) systems. Shen *et al.* (2007) compare different defense strategies to defend various types

of cyber attacks and assess its impact, utilizing a dynamic game theoretic data fusion framework. Argauer and Yang (2008) analyze correlated or grouped alerts induced by cyber attack and determine their "impact" on services which is modeled as "virtual terrain". Stamp *et al.* (2009) analyze the development of a Cyber-to-Physical (C2P) bridge and addresses the issue of grid impacts of cyber attack. Masi *et al.* (2010) analyze the impact of cyber attacks and other events that affect telecommunications networks performances. Musman *et al.* (2010) develop techniques to estimate the mission impact of potential cyber attacks. Esfahani *et al.* (2010) develop a new framework and define a systematic methodology based on reachability to identify the impact that a cyber intrusion might have on the Automatic Generation Control Loop. Khalili *et al.* (2010) present methodologies for understanding the mission risks based on IT infrastructure to predict and model the impact of cyber attacks. Saini *et al.* (2012) provide the understanding of cyber crimes and its future impacts on society. Kotenko and Chechulin (2013) suggest a framework for cyber attack impact modeling and prediction. Cavelty (2013) explores the constitutive effects of different threat representations in the broader cybersecurity discourse. Hurst *et al.* (2015) present an approach for predicting the impact of a cyber attack on a critical infrastructure network, focusing on distributed denial-of-service attack (DDoS) attacks.

### 2.1.3 Multi Hazard

Some of the infrastructure systems, such as electricity power systems and

telecommunication systems are exposed to multi hazard (either natural or manmade hazard). Therefore, the natural and manmade hazard together are considered in the system performance analysis. Haddow *et al.* (2017) discuss a full range of natural and manmade hazards and illustrate these hazards by recent disaster events such as Boston Marathon Bombing, Hurricane Sandy, the Joplin Tornado, the Haiti Earthquake, and the Great East Japan Earthquake. Bullock *et al.* (2017) classify natural and manmade hazard, discuss cybersecurity and critical infrastructure protection under natural and manmade hazard; the desired response and mitigation strategies are provided. Ettouney and Alampalli (2016) investigate the civil infrastructure under multi hazard, resilience monitoring and acceptance and treatment under multi hazard is analyzed from different aspects.

The U.S. Department of Energy (2014) and North American Electric Reliability Corporation (2010) identify a range of risks to the electricity power systems from natural and manmade hazard. Preston *et al.* (2016) summarize the frequency (number of events) and severity (number of people affected) of bulk power emergencies due to a host of natural and manmade hazard, and introduce commonly used approaches for hazard occurrence prediction. They also point out that the natural hazard could be the trigger factor of manmade hazards. Haddow *et al.* (2017) discuss the full range of both natural and manmade hazard and provide a brief description of each hazard as well as information on hazard detection and classification. Cutter *et al.* (2010) provide a set of resilience indicators for measuring baseline characteristics of communities under

natural and manmade hazard, pointing out that metropolitan areas have higher levels of resilience than rural counties. Similarly, Islam and Ryan (2015) identify and provide mitigation strategies for a variety type of natural and manmade hazard. Coppola (2006) states that physical location is the primary factor dictating what natural hazards a nation faces, while economic, industrial, and sociopolitical factors dictate manmade hazards origin.

## 2.2 Resilience

### 2.2.1 Resilience Definitions

As stated earlier, natural and manmade hazards may cause significant damage to the system's performance (either immediately dropping or gradually deteriorating to an unacceptable level). The system's ability to minimize the negative impact of the hazard (e.g., system performance loss and the deterioration period) is generally understood as system robustness; and the ability of system to adapt to the degraded environment and still maintains (at least partial) its functionality can be interpreted as system's adaptive ability. From these two perspectives, some studies consider system resilience as one or more of the following abilities.

1) Accurately forecast the hazard;
2) Defend against the hazard before adverse consequences occur;
3) Absorb external stresses;
4) Adapt to the environmental requirements;

5) Maintain the desired performance level.

It is worth noting that these abilities are mainly considered and improved during system design stage.

Chen *et al.* (2008) define resilience under natural hazards as "the capability of a community to survive following a disaster". As an extension, Hollnagel *et al.* (2007) define resilience as "the ability to sense, recognize, adapt and absorb variations, changes, disturbances, disruptions and surprises". The static resilience of an economic organization is defined as "the ability of an entity or system to maintain function (e.g., continue producing) when shocked" (Pant *et al.* (2014b)), which is applicable to engineering systems. Similarly, Pregenzer (2011) considers resilience as "a measure of a system's ability to absorb continuous and unpredictable change and still maintain its vital functions"; while Klein *et al.* (2003) present a similar but more general concept of resilience under natural hazards. Comfort (2007) considers resilience as "the capacity to adapt existing resources and skills to new situations and operating conditions", i.e., system's adaptability. Overbye *et al.* (2012) propose that for a power grid, resilience is the ability to "maintain or gradually degrade its performance under hazards". Similar definitions of resilience with ignorable consideration of system recovery ability are found in ecological and socio-ecological systems in Holling (1973), Walker *et al.* (2004), Easterby-Smith *et al.* (2012), and Gunderson (2000). Specifically, the resilience of passenger traffic in roadway networks is defined as "the network's ability to resist and adapt to disruption" (Faturechi and Miller-Hooks (2014b)).

A substantial number of studies on resilience of service-oriented network (such as

supply chain, transportation network systems) consider resilience as the ratio between the system performance level after and before the hazard ((Omer *et al.* (2009), Omer *et al.* (2014), Miller-Hooks *et al.* (2012), Fotouhi *et al.* (2017), and Jin *et al.* (2014)), where the system recovery ability after the hazard is not considered. Alternatively, resilience is simply considered as the system performance (Janić (2015a)).

Though system's robustness, vulnerability and adaptive ability are widely used as measures of resilience; they ignore the ability of the repairable system to recover to the desired performance level and therefore are not inclusive. For repairable systems, when its performance deteriorates to a predefined threshold, recovery action is performed until system performance is restored to a desirable level. Geis (2000) and Campanella (2006) use system's recovery ability (i.e., the recovered system performance level and the recovery time) as resilience. Hollnagel *et al.* (2007) modify the resilience definition to "the ability that a system or an organization to react to and recover from disturbances at an early stage, with minimal effect on the dynamic stability". Recovery ability is also interpreted as "the ability to 'bounce back' after suffering a damaging blow" (Wildavsky (1988) and Boin and McConnell (2007)). Logistic network considers the resilience as the ability to return to a stable or normal operating state after a strong perturbation or shutdown due to serious failure or outside attack (Wang and Ip (2009)).

A substantial number of studies define system resilience by combining abilities 1) through 5) and recovery ability. As an example, Cabinet Office (2011) defines resilience as "the ability of assets, networks and systems to anticipate, absorb, adapt to and/or rapidly recover from a disruptive event". The National Infrastructure Advisory Council (NIAC) provides a generic definition of resilience in terms of robustness,

resourcefulness, rapid recovery and adaptability when critical infrastructure (CI) is exposed to a host of natural hazards. Similar definitions of the resilience of CI under natural hazards are provided by (Tran *et al.* (2017), Berkeley III *et al.* (2010), Haimes (2009), and Keogh and Cody (2013)), where resilience is more general and distinguished from vulnerability, risk and preparedness.

The seismic resilience is defined as "the ability of a system to reduce the chances of a shock, to absorb such a shock if it occurs (abrupt reduction of performance), and to recover quickly after a shock (reestablish normal performance)" (Bruneau *et al.* (2003)). This resilience definition has been generally adopted for a variety of systems under different scenarios. Similar definitions of resilience are also found in Chang and Shinozuka (2004), Ayyub (2014), Nan and Sansavini (2017) and Tilman and Downing (1994). Lu *et al.* (1996) classify the power system's resilience into short-term and long-term, where the latter one focuses on the adaptability of the system to the changing conditions and new threats in a long run. Generally, for an energy system, resilience is "the capacity of an energy system to tolerate disturbance and to continue to deliver affordable energy services to consumers, and speedily recover from shocks and can provide alternative means of satisfying energy service needs in the event of changed external circumstances" (Chaudry *et al.* (2011)).

Conceptually, system resilience needs to consider the impact of hazards on system performance change (both magnitude and speed) during the hazard and recovery phase; therefore we demonstrate system recovery time in our proposed definition later.

### 2.2.2 Qualitative and Semi-quantitative Framework of Resilience

Bruneau *et al.* (2003) describe resilience for both physical and social systems that should consist of robustness, redundancy, resourcefulness and rapidity; similar assessment of resilience is found in Keogh and Cody (2013), which is used for the resilience assessment of critical electrical power infrastructure under extreme weather events (Panteli and Mancarella (2015)). Sterbenz *et al.* (2011) measure system resilience using its ability in a time series as: defend, detect, diagnose, remediate, refine, and recovery; which is similar to the resilience assessment of cyber systems. A conceptual framework for system resilience is proposed by Kahan *et al.* (2009) as: threat and hazard assessment, robustness, consequence mitigation, adaptability, risk-informed planning, risk-informed investment, harmonization of purposes, and comprehensiveness of the scope. The resilience of CI is classified into internal and external resilience; where the internal resilience refers to the inherent resilience of the CI, and external resilience refers to the resilience associated with external agents (Labaka *et al.* (2015)). A qualitative what-if analysis is performed on the resilience assessment of heterogeneous systems by Filippini and Silva (2014), assuming the entire system state is dependent on the states of the components in the system.

In real-time sequence, system's resilience can be qualitatively assessed in four stages: (i) threat characterization, (ii) vulnerability of system's components, (iii) system reaction or operation and (iv) system's restoration (Espinoza *et al.* (2016)); where the four stages can be alternatively interpreted as 1) prediction and preparedness, 2) vulnerability, 3) robustness and adaptability and 4) recovery. Similarly, the qualitative framework to assess resilience is suggested to be divided into five steps as: system description, potential disruptions analysis, recovery actions analysis, system performance measurement, and system resilience calculation.

Sterbenz *et al.* (2011) use a two-phase strategy "D2R2+DR" for cyber network resilience assessment. The first strategy phase D2R2 consists of a cycle of four steps (defend, detect, remediate, recover) which are performed in time sequence; based on the first strategy, the second strategy DR consists of diagnosis of faults and refinement of future behavior. For example, Gillani *et al.* (2015) propose to defend against attacks by proactively changing the footprint of critical resources in an unpredictable fashion to invalidate an adversary's knowledge and plan of attack against critical network resources. Singh and Silakari (2009) define cyber-attack detection as "the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges" and suggest that cyber detection identifies attacks mainly based on three basic approaches: misuse detection, anomaly detection and specification-based detection. Mayer *et al.* (2012) develop a method to prioritize remediation actions when computer system is under cyber attacks; specifically, remediation action with the highest impact on the security value improvement is assigned the highest priority. Goldman *et al.* (2011) propose that it is unrealistic to completely defend against the cyber attack; instead, more efforts should be spent on ensuring and recovering mission success even in a degraded or contested environment. Recovery methods after the cyber attacks vary in different domains. Tran *et al.* (2016) present the implementation of dynamic cyber resilience recovery model (CRRM) to combat a zero-day outbreak within a closed network and minimize disruptions of cyber attacks to business operations. General actions for cyber resilience refinements in the long term are recommended in Choudhury *et al.* (2015). A Bayesian algorithm is proposed to enhance the resilience of Wide Area Monitoring System (WAMS) applications against cyber attacks (Khalid and Peng (2016)). Specifically, suggestions on refining resilience in different domains are provided such

as industrial control systems (Chaves *et al.* (2017)), critical infrastructures (Bologna *et al.* (2015)), power grid systems (Ashok *et al.* (2017)) and communication networks (Sterbenz *et al.* (2010)).

In some studies, system reliability is considered as important factors in system resilience. For example, Vlacheas *et al.* (2013) propose that the most important factors in resilience are reliability, safety, availability, confidentiality, integrity, maintainability and performance; where both non-repairable and repairable systems are included. Wang and Ip (2009) propose that a logistic system with redundancy has a quick recovery (and therefore high resilience) when the system functionality is down. Similarly, Panteli and Mancarella (2015) suggest effective measures (such as accurate hazard prediction and comprehensive plans in advance, use of highly-reliable components, locating facilities to safe regions, and designing redundant transmission lines) to improve the resilience of critical electrical power infrastructure. More suggestions for improving electricity system resilience and reducing power outage by considering either redundancy or reliability are proposed by Campbell (2012), Northern PowerGrid (2013) and Energy Networks Association (2011).

As stated earlier, systems are subjected to a host of natural and manmade hazards. Cutter *et al.* (2008) provide a disaster-resilience-of-place model to improve disaster resilience assessment accuracy at a local level. A host of natural hazards types are described and the performance of sanitation systems under these hazards are scored and weighted by experts for system resilience semi-quantitative analysis (Luh *et al.* (2017)); it is proposed that difficulty and challenge exist in accurately scoring the hazards. More semi-quantitative analysis on system resilience assessment is performed on supply

chain resilience (Pettit *et al.* (2010)) and industry system resilience (Shirali *et al.* (2013)). The contributions and advantages of qualitative analysis to resilience research are summarized in Ungar (2003).

We use Table 2.1 to summarize system's various abilities that are considered in the system's resilience definition and qualitative assessment.

**Table 2.1** Abilities related to system's resilience definition and assessment.

| | Sense the hazard | Adapt to the environment | Absorb negative energy | Maintain System's functionality | Recover quickly | Resist the hazard |
|---|---|---|---|---|---|---|
| Hollnagel *et al.* (2007) | √ | √ | √ | | √ | |
| Pant *et al.* (2014b) | | | | √ | | |
| Pregenzer (2011) | | | √ | √ | | |
| Klein *et al.* (2003) | | | √ | √ | | |
| Comfort (2007) | | √ | | | | |
| Overbye *et al.* (2012) | | | | √ | | |
| Holling (1973) | | | √ | √ | √ | |
| Walker *et al.* (2004) | | | √ | √ | | |
| Gunderson (2000) | | | | | √ | |
| Faturechi and Miller-Hooks (2014b) | | √ | | | | √ |
| Geis (2000) | | | | | √ | |
| Campanella (2006) | | | | | √ | |
| Wildavsky (1988) | | | | | √ | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Boin and McConnell (2007) | | | | | √ | |
| Wang and Ip (2009) | | | | | √ | |
| Cabinet Office (2011) | √ | √ | √ | | √ | |
| Bruneau *et al.* (2003) | √ | | √ | √ | √ | |
| Ayyub (2014) | √ | | √ | | √ | |
| Nan and Sansavini (2017) | √ | | √ | | √ | |
| Tilman and Downing (1994) | √ | | √ | | √ | |
| Chaudry *et al.* (2011) | √ | | √ | √ | √ | |
| Sterbenz *et al.* (2011) | √ | | | | √ | |
| Kahan *et al.* (2009) | | √ | | √ | | √ |
| Espinoza *et al.* (2016) | √ | √ | | √ | √ | √ |
| Keogh and Cody (2013) | √ | √ | | √ | √ | √ |
| Tran *et al.* (2017) | √ | √ | | √ | √ | √ |
| Berkeley III *et al.* (2010) | √ | √ | | √ | √ | √ |
| Haimes (2009) | √ | √ | | √ | √ | √ |
| Omer *et al.* (2009) | | | | √ | | √ |
| Omer *et al.* (2014) | | | | √ | | √ |
| Miller-Hooks *et al.* (2012) | | | | √ | | √ |
| Fotouhi *et al.* (2017) | | | | √ | | √ |
| Jin *et al.* (2014) | | | | √ | | √ |

## 2.3 Importance Measure

Importance measure (IM) is beneficial not only for the designer's insight into a system but also for system optimization. By now, various efforts have been made to improve the theories and applications of IMs, but in different domains, there are different methods for measuring the importance of components.

Birnbaum (1968) first proposes the IM that deals with the effects of changes in the unreliability of a given component by taking the partial derivative of system unreliability with respect to components unreliability. In other words, a component whose variation of the unreliability results in the largest variation of the system unreliability has the most impact on system failure.

As a seminal work, Birnbaum IM has been extensively studied and applied. For example, Papastavridis (1987) drives Birnbaum IM for components in consecutive-*k*-out-of-*n: F* system (consisting of an ordered sequence of $n$ components such that the system fails if and only if $k$ or more consecutive components fail, such as telecommunication and pipeline systems) with i.i.d. components and concludes that the most important components are in the middle of the sequence. Xie and Shen (1989) propose a general IM whose system reliability depends on the reliability of the component to improve the Birnbaum IM. Leemis (1995) proposes an IM which considers system reliability instead of unreliability. Chadjiconstantinidis and Koutras

(1999) apply Birnbaum IM for Markov chain imbeddable systems. Chang *et al.* (1999) introduce some new techniques to explain some unproven results Birnbaum IM and extend the measure to the 2-out-of-*m*-out-of-*n* systems. Yao *et al.* (2011) propose five new Birnbaum IM based heuristics and their corresponding properties in Component Assignment Problem (CAP). Zhu *et al.* (2012) analyze certain patterns of the component Birnbaum IM for linear consecutive-*k*-out-of-*n* systems when all components have the same reliability. Wu and Coolen (2013) develop a cost-based extension of Birnbaum IM, which considers costs incurred by maintaining a system and its components within a finite time horizon. Liu *et al.* (2014) derive the expression of the Birnbaum IM under deterministic environmental conditions and utilize Birnbaum IM in components subjected to competing degradation modes under time-variant conditions. Zhu *et al.* (2017) present the Birnbaum IM based local search methods and the Birnbaum IM based genetic algorithms for addressing the multi-type component assignment problem (MCAP). Birnbaum IM is the most fundamental, and most of the alternative IMs are developed and extended based on it.

The reliability importance of a component usually is insufficient to determine how components affect the system reliability, in particular, it gives very little information about how the dependent components' reliabilities affect system performance jointly. Hong and Lie (1993) first propose joint reliability importance (JRI) defined as the rate at which the system reliability improves as the reliabilities of the two components improve to indicate how components interact in contributing to system reliability.

Armstrong (1995) further improves JRI by considering component states dependently. Wu (2005) extends the joint importance measure (JIM) from the binary systems to multi-state systems by considering the performance utility of the system with JRI and joint structural importance (JSI). Gao *et al.* (2007) extend the JRI from two components to multi components, and investigate the concept of Conditional Reliability Importance (CRI) while the working states of certain components are known. Furthermore, Si *et al.* (2012b) extend the JRI from multi-state systems to multi-state transition systems. Applications on JIM are also presented in Hong *et al.* (2000) on fault-tree, Hong *et al.* (2002) in *k*-out-of-*n* systems, Eryilmaz (2013) in linear *m*-consecutive-*k*-out-of-*n*: *F* systems and Pan and Nonaka (1995) in common cause failures. Borgonovo (2010) presents a unified framework for the utilization of JIM and DIM in both coherent and non-coherent systems, and develops a total order IM that synthesizes the Birnbaum IM, JIM and DIM of all orders in one unique indicator.

Most IMs mentioned above rank components from reliability as a performance measure of the system, which not only considers the probability that a component functions properly during the mission time or at a fixed time point, but also considers system structure. However, some of IMs are evaluated only from the structure importance, which considers the relative importance of various components with respect to their positions in a system. Although the reliability IMs are generally superior to the structural ones and are of primary concern, their calculations might not be available in practice. For example, in large complex systems, the computations involved in

quantifying IM can become prohibitively extensive. Therefore, structural IMs can be used to provide a fair basis to compare the relative importance among system components. According to the Fussell-Vesely measure, the importance of a component depends on the number and on the order of the cut-sets in which it appears. Butler (1977) proposes a cut-importance ranking based on the minimal cut-sets of the system, Aven (1985) provides a computer program ERAC to calculate (un)reliability ((un)availability) and some IMs based on the minimal cut-sets, Boland *et al.* (1987) develop a procedure for optimally allocating components by introducing the notion of structural criticality of components. Page and Perry (1994) develop an IM to assess the relative importance of edges in a graph based on reliability polynomials. Later Meng (1994) and Meng (1995) characterize the criticality ordering from minimal cut-set (minimal path-set) introduced by Butler (1977) and Boland *et al.* (1987) and derive a relationship between the criticality ordering and Birnbaum IM of components. Meng (1996) and Meng (2000) compare the relative importance of system components ordered by their structural criticality instead of calculating their Birnbaum and Fussell-Vesely IM, and propose a new IM to improve Fussell-Vesley IM and a new method to compute Birnbaum IM.

More comprehensive reviews concerning the topic of IMs for components in binary coherent systems whose components and/or the system performance only have two states, i.e., functioning/not-functioning are presented by Boland and El-Neweihi (1995), Aven and Nøkland (2010), Kuo and Zhu (2012), and Borgonovo *et al.* (2016).

Although binary systems have many practical applications, a model based on two states is often over-simplified and insufficient for describing many commonly encountered situations in real life. Accordingly, multi-state systems whose components and/or the system performance have more than two states are more realistic and frequently required. For example, multi-state systems appear in a gas transportation systems, which usually operate in intermediate states (the state of the system is defined as the rate of delivered gas (0%, 100%)), similar as in supply chain systems, communication networks, production systems, manufacturing systems, power generation, computer systems and so on. When applied to multi-state systems, the concept of unavailability is used as a function of the individual components' performances as well as of the demand required of the system (system performance). Consequently, a component can be regarded as more important one if it improves system availability by achieving a required performance level and less important for another. Research efforts have been focused on generalizing frequently used binary importance measures to accommodate the multi-state behavior. Research on extending binary systems to multi-state systems with multi-state components (MSMC) and assessing their reliability (performance measures) are presented by Hirsch *et al.* (1968), Postelnicu (1970), El-Neweihi *et al.* (1978), Barlow and Wu (1978), Ross (1979), Natvig (1982b), Block and Savits (1982), Wood (1985), Garribba *et al.* (1985), Gandini (1990), Aven (1993), Levitin and Lisnianski (1999), Lisnianski and Levitin (2003), Levitin (2005) and Li *et al.* (2014). In particular, El-Neweihi *et al.* (1978) analyze the relationships between multi-state coherent system's reliability behavior and multi-state component's performance under

deterministic and stochastic scenarios, where this work is developed based on the structure function. Barlow and Wu (1978) extend binary coherent structures to the system state function for coherent systems with multi-state components, and investigate its properties which can be extended to an increasing but otherwise arbitrary state function. Lisnianski and Levitin (2003) address the details of multi-state system reliability analysis and optimization.

Kim and Baxter (1987) extend the importance measures from discrete-state systems to continuous-state systems. Bueno (1988) uses decomposition to obtain an extension of the Barlow-Proschan IM in multistate monotone systems. Gandini (1990) develops a new IM by using the heuristically-based generalized perturbation theory (GPT) and compares it with Birnbaum IM and Barlow-Proschan IM. Armstrong (1997) extends importance measures to cover reliability models where the components have two failure-modes rather than the conventional one failure-mode. Levitin and Lisnianski (1999) propose importance and sensitivity measures for multi-state systems with binary capacitated components, which account for both the multi-state system performance caused by the capacitated components and stochastic system demand. Levitin *et al.* (2003) study the generalized IMs for multi-state components based on the restriction that component's performance is only reachable to certain states. Zio and Podofillini (2003b) present multi-state extensions for risk achievement worth (RAW), risk reduction worth (RRW), Fussell-Vesley IM and Birnbaum for MSMC. Zio and Podofillini (2003a) generalize some of the most frequently used IMs to MSMC, which

characterize the importance of a component achieving a given level of performance with respect to the overall mean system unavailability and performance. Vaurio (2011) develops new IMs for repairable systems under multiple phases of the mission. Peng *et al.* (2012) and Liu *et al.* (2014) analyze IM for components subject to degradation, where the latter work considers the interdependency among components' performance.

Traditional IMs mainly concern the change of the system reliability (availability) caused by the change of the reliability (availability) of the component without considering the joint effect of the probability distributions, transition intensities of the object component states, and the system performance. In order to describe the reliability, structure and causality characteristics of components comprehensively, integrated IM (IIM) is first presented by Si *et al.* (2010) to evaluate the integrated effect of components on the MSMC under uncertainty, which introduces the probability distribution change of system under the conditions of different component states and the failure state distributions of the component. Further, Si *et al.* (2012c) study the IIM of component states in multi-state systems based on loss of system performance related to the expected number of component failures, and the effect of system structure, then evaluate IIM by using the UGF method. Si *et al.* (2012a) discuss the IIM of component states based on the system maintenance cost. Si *et al.* (2013) extend the IIM to estimate the effect of a component residing at certain states on the performance of the entire multi-state systems. Dui *et al.* (2014) apply IIM to multi-state system with renewal functions and later Dui *et al.* (2015) apply IIM to semi-Markov processes.

Obviously, most of IMs in MSMC focus on investigating how a particular component state or set of states affects multi-state system reliability instead of a specific component. It is not clear to prioritize system component importance for some systems whose the most critical component state may not correspond to the most critical system component. Accordingly, Ramirez-Marquez and Coit (2005) propose composite importance measures (CIM) with the aim of identifying how a specific component affects multi-state system reliability by considering all of its prospective states. Ramirez-Marquez *et al.* (2006) generalize the work in Ramirez-Marquez and Coit (2005) by discussing IMs for measuring the criticality of both "specific component" and "a specific state or sets of states of a component". Ramirez-Marquez and Coit (2007) further evaluate and implement CIM for MSMC and develop a component allocation heuristic to maximize system reliability improvements. Peng *et al.* (2012) use CIM for components that are subjected to degradation under one-dimensional time-invariant environment.

Besides reliability and availability, a variety of system performance measurements are adopted for component's IM calculation such as resilience (Fang *et al.* (2016), Baroud *et al.* (2014) and Whitson and Ramirez-Marquez (2009)), vulnerability (Murray-Tuite and Mahmassani (2004) and Jenelius *et al.* (2006)) and survival signature (Feng *et al.* (2016)).

Majority of the IMs mentioned above are strictly for coherent system (each component

is relevant, the structure function is increasing (non-decreasing), and the failure only caused by component failure event) analysis. Non-coherent systems (whose failure can be caused not only by component failure (coherent systems) event, but also by component repair event) can occur and accurate importance analysis is essential. Jackson (1983) first enables analysis of non-coherent systems by using extended Birnbaum IM and Andrews and Beeson (2003) improve its consistency. Beeson and Andrews (2003) extend four commonly used IMs, using the non-coherent extension of Birnbaum's measure of component reliability importance. Andrews and Beeson (2003) propose an extension of Birnbaum IM for non-coherent importance analysis, which calculates the average number of system failures in a given interval more efficiently. Borgonovo (2010) builds a unified framework for the utilization of JIM and DIM in both coherent and non-coherent systems. Borgonovo *et al.* (2016) propose a new importance measure for time-independent reliability analysis, for both coherent and non-coherent systems and has an intuitive probabilistic and also geometric interpretation. Alternate extensions are recently offered by Vaurio (2016) and Aliee *et al.* (2017), as they introduce a Boolean expression in the non-coherent system.

## 2.4 Cascading Failure

The normal operation of a system shows that the system carries a flow of some certain resource, such as information, electricity, water, data packages and so on, where components individually share a load which does not exceed the capacity of that

component. In general, when the total flow of the system changes or components are added or removed, system will dynamically adjust the loads on the individual components to maintain the load below the capacity of the component. For example, when a component fails, the loads are recalculated and the components whose loads exceed their capacity are removed from the system. The process is repeated until loads of all remaining components are below their capacity. However, this dynamic adjustment of redistributing the loads causes the "removing" (referred to as "failure") of the components, which results in the cascading failure.

A cascading failure is a process in a system of interconnected subsystems in which the failure of one or few components can trigger the failure of other components. It is initiated when a component fails, and other components must compensate to share the load of the failed component. In turn, this redistribution may overload other components causing them to fail as well. Thus, the number of failed components increases, propagating throughout the system and causing additional components to fail one after the other. In particularly serious cases the entire network is affected. Therefore, it can be seen the failure of a single component is sufficient to cause the failure of the entire system if the component is among the ones with the largest load.

Many systems can experience random and systematic failures of their components, and there are numerous examples showing that these local failures can lead to the global failure of the system and consequently the break down of the system. Large cascades

triggered by small initial failures are present in many types of systems, including power transmission, computer networking, finance, human body systems, bridges, epidemic infection, and production systems and others. The modern society is dependent on large-scale infrastructure systems to deliver resources to homes and businesses in an efficient manner (Ash and Newth (2007)). For example, cascading failures are common in most of the complex communication and/or transportation networks that are the basic components of our lives and industry (Dorogovtsev and Mendes (2002)).

Cascading failures in power grids are also well documented. It is common when one of the components fails and shifts its load to nearby components. If those nearby components are overloaded, they will shift their load onto other components. This surge current can induce the already overloaded components into failure, setting off more overloads and thereby taking down the entire system in a very short time (a large number of transmission lines are overloaded and malfunction at the same time). For example, on November 9, 1965, a small variation of power originating from one of the generating plants in New York caused the relay to trip. Instantly, the power that was flowing on the tripped line transferred to the other lines, causing them to become overloaded. Their own protective relays, which are also designed to protect the line from overload, tripped. Within five minutes, the power distribution system in the Northeast was in chaos as the effects of overloads and the subsequent loss of generating capacity cascaded through the network, breaking the grid into "islands". Station after station experienced load imbalances and automatically shut down, affecting parts of

Ontario in Canada and Connecticut, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island, Pennsylvania, and Vermont in the United States. Over 30 million people and 80,000 square miles were left without electricity for up to 13 hours (Vassell (1990)). On 10 August 1996, when a 1300-mw electrical line in southern Oregon sagged in the summer heat, initiating a chain reaction that cut power to more than four million people in eleven Western States (Sachtjen *et al.* (2000)). On 14 August 2003 when an initial disturbance in Ohio triggered the largest blackout in the U.S.'s history in which millions of people remained without electricity for as long as 15 hours (Glanz *et al.* (2003)).

Cyber networks are also such examples that should be protected against cascading failures (Mei *et al.* (2008), Ren and Dobson (2008), Jacobson (1988b) and Guimerà (2003)), which are caused by failing or disconnected hardware or software. Specifically, if a few important cables break down, the traffic should be rerouted either globally or locally towards the destination. When a line receives extra traffic, its total flow may exceed its threshold and cause congestion. As a result, an avalanche of overloads emerges on the network and cascading failure might occur (Mirzasoleiman *et al.* (2011)). For instance in October 1986, during the first documented Internet congestion collapse, the speed of the connection between the Lawrence Berkeley Laboratory and the University of California at Berkeley, two places separated only by 200 meters, dropped by a factor 100 (Jacobson (1988a) and Guimera *et al.* (2002)). In particular, a cyber network comprising small devices includes thousands of sensors, transmitters,

actuators, and monitors. Hence, connectivity is the most crucial factor to determine the service quality in a network; thus, network flows should be carefully distributed in terms of load balance among devices. However, a small fraction of overloaded nodes extremely accelerates the propagation of failures as discussed in Sun and Han (2005), Zhao *et al.* (2007) and Ash and Newth (2007). In a wireless sensor cyber network, a sensor node which must communicate with a large number of neighbors may be more likely to deplete its energy reserve and fail. Alternatively, a node directly connected to many other nodes may be also more likely to be attacked by an adversary seeking to break down the whole network. For example, virus and worms which originate at a small number of nodes can propagate themselves by infecting nearby cell phones and laptops via short-range communication, thereby potentially creating a "wireless epidemic" (Kleinberg (2007)).

These severe incidents such as blackouts and internet congestion mentioned above have been investigated quite intensively (Boccaletti (2006)). Although most of studies are mainly focused on the cascading failures on a single or isolated system, many complex systems are interdependent and failures occurring in one system are likely to have impacts on others in real world. The operations of many modern cyber-physical systems are based on increasingly interdependent networks, and diverse infrastructures such as water supply, transportation, fuel and power stations are coupled together. Due to this coupling relationship, they are extremely sensitive to random hazards so that a failure of a small fraction of components from one system can produce an iterative cascade of

failures in several interdependent systems (Foster Jr *et al.* (2004) and Rinaldi *et al.* (2001)). For example, the September 28, 2003 blackout in Italy resulted in a widespread failure of the railway network, health care systems, and financial services and, in addition, severely influenced communication networks. The partial failure of the communication system in turn further impaired the power grid management system, thus producing a positive feedback on the power grid (Rosato *et al.* (2008)).

In addition, the small-world and scale-free properties are ubiquitous in nature and human society (Albert (2002)), which operate with a high tolerance of random failures but are susceptible to cascading failures (Motter and Lai (2002)). Thus the impact of cascading failures and the robustness characteristic on independent and dependent systems have received significant attention in the past decade (Albert (2002), Dorogovtsev (2002), Newman (2003), Boccaletti (2006), and Gallos (2005)). From the viewpoint of system resilience, a key question is whether the system facing these dependent and correlated failures can retain its functionality in terms of maintaining some sense of global communication. Specifically, the network may be considered to be resilient if the size of the largest connected component of operational nodes (after the failures) is proportional to the size of the whole network (Kong and Yeh (2010)). For instance, if a power grid still collects electricity from a constant fraction of some nodes even after a substantial number of node and wire failures, then the power grid is resilient. On the other hand, after some node and wire failures, the power grid breaks down into isolated parts where even the most important node can receive only a

vanishingly small fraction of the electricity, then the power grid is not considered to be resilient. Several studies are devoted to the concept of controlling cascading failures (Adibi *et al.* (1987), Talukdar *et al.* (2003) and Kundur *et al.* (1994)). For example, islanding or separating the survivable parts of a grid has long been used to allow a transmission grid to continue its functionality, and building a system for allocating competing resources during an extended failure is another solution for controlling such failures (Talukdar *et al.* (2003)).

Up to now, a large number of important impacts of cascading failures have been investigated, dynamical approaches are developed, and many system models are proposed and studied, such as the sandpile model (Bak (1987), Goh and Lee (2003) and Huang *et al.* (2006)), the global load-based cascading model (Motter and Lai (2002), Moreno (2003), Motter (2004), Zhao *et al.* (2004), and Zhao *et al.* (2005b), Crucitti *et al.* (2004a), Schäfer *et al.* (2006), Mirzasoleiman *et al.* (2011), Holme and Kim (2002), Moreno *et al.* (2003), Crucitti *et al.* (2004b), and Carreras *et al.* (2003)) and the fiber bundle model (Moreno *et al.* (2002), Kim (2004) and Kim *et al.* (2005)). In addition, the influence of the cascaded failure in the size of the largest connected component is investigated in a number of system models including preferential attachment scale-free (Zhao *et al.* (2004)), Watts-Strogatz small-world (Xia *et al.* (2010)), and modular networks (Babaei *et al.* (2011)). Based on these models, some protection strategies are proposed (Motter (2004), Moreira *et al.* (2009), Zhao *et al.* (2004), Zhao *et al.* (2005a), Zhao *et al.* (2005b), Schäfer *et al.* (2006) and Wang and Kim (2007)). Ash and Newth

(2007) and Simonsen *et al.* (2008) compare the different control and defense strategies.

From the perspective of system resilience, Newth and Ash (2004) and Ash and Newth (2007) use an evolutionary algorithm to evolve complex networks that are resilient to such cascading failure and apply network statistics to identify topological structures that promote resilience to cascading failure. Kinney *et al.* (2005) model the power grid using its actual topology and plausible assumptions about the load and overload of transmission substations, and study the damage inflicted by the loss of single unit. They find three universal behaviors, suggesting that 40% of the transmission substations lead to cascading failures when disrupted. While the loss of a single unit can inflict substantial damage, subsequent removals have only incremental effects, in agreement with the topological resilience to less than 1% unit loss. Kong and Yeh (2010) analyze the problem of resilience to dependent unit (node) failures in large-scale networks modeled by random geometric graphs from a percolation-based perspective, and show that the cascading failure problem is equivalent to a degree-dependent percolation process. Zeng *et al.* (2013) construct a novel cascading failure model with tunable parameters and propose an evaluation method of node importance according to the features of symbiosis networks of eco-industrial parks. Based on the cascading model, an effective new method, the critical threshold, is put forward to quantitatively assess the resilience of symbiosis networks of eco-industrial parks. Moon and Jeon (2015) propose a load-dependent cascading failure model according to sandpile principle, which is effective in evaluating the overall aspect of resilience capacity in terms of

connectivity efficiency against the spreading of large collapse. Chai *et al.* (2016) study the resilience and robustness of interdependent networks consisting of an electric power grid and a communication network against cascading failures

From the viewpoint of weighted system, Wang and Chen (2008) propose a cascading model inducing the weight of a network edge $(k_i k_j)^{\theta}$ with a local weighted flow redistribution rule (LWFRR) on weighted networks, which combines the cascading process and the weighted characteristics of the network. The weighted complex network reaches the highest robustness level when the weight parameter $\theta = 1$, which indicates the significant roles of weights in complex networks for designing protection strategies against cascading failures. Moreover, Mirzasoleiman *et al.* (2011) investigate the profile of the robustness against cascading failures in weighted networks and three weighting strategies including the betweenness centrality of the edges, the product of the degrees of the end nodes, and the product of their betweenness centralities. They find that the load of the links is considered to be the product of the betweenness centrality of the end nodes is favored for the robustness of the network against cascading failures.

In interdependent systems, Vespignani (2010) studies the failures in interconnected networks and highlights the vulnerability of tightly coupled infrastructures and shows the need to consider mutually dependent network properties in designing resilient systems. Parshani *et al.* (2010) propose a theoretical framework for studying the

impacts of coupling probability on interdependent networks. It is found that reducing the coupling leads to a change from a first order percolation phase transition to a second order percolation transition. Buldyrev *et al.* (2010) analyze the blackout in Italy and generalize a model to capture the phenomenon of cascading failures in interdependent networks. They present analytical solutions for the critical fraction of nodes and find that interdependent links make interdependent networks more vulnerable to random failures. Brummitt (2012) investigates the sandpile model on modular random graphs and power grids and find that some connectivity is beneficial but extensive interconnectivity becomes detrimental. Tan *et al.* (2013) investigate the effect of coupling preference on cascading failures in interconnected networks and found that assortative coupling is more helpful to resist the cascades. Chen *et al.* (2015) investigate cascading failures and the coupling preference on systems robustness in interdependent scale-free networks under targeted attacks and find that disassortative coupling is more robust for sparse coupling while assortative coupling performs better for dense coupling. More detail about interdependent networks can be found in Kivelä *et al.* (2014) and Gao *et al.* (2014).

Since most of studies focusing different scenarios are based on the seminal model proposed by Motter and Lai (2002) and Crucitti *et al.* (2004a), we provide details of this model in the following.

The model assumes that each node has certain capacity and initially the load at each

node is smaller than its capacity. The failure (removal) of a node changes the balance of flows and leads to a redistribution of loads over other nodes. If the capacity of these nodes cannot handle the extra load a cascade of overload failures is triggered and eventual network failure. The model follows:

1) Overloaded nodes are not removed from the network;
2) The damage caused by a cascade effect is quantified in terms of the decrease in the network efficiency (Latora and Marchiori (2001)).

The average efficiency of the network $E(\mathbf{G})$ can be expressed as in Eq. (2.3)

$$E(\mathbf{G}) = \frac{1}{N(N-1)} \sum_{i \neq j \in \mathbf{G}} \varepsilon_{ij} \tag{2.3}$$

where $N$ is total number of nodes in network; $\mathbf{G}$ is the network described by the $N \times N$ adjacency matrix $\{e_{ij}\}$ in which $e_{ij}$ is a measure of the efficiency in the communication along the link: if there is a link between node $i$ and node $j$, the entry $\mathrm{e}_{ij}$ is a value in the range (0,1]; otherwise $\mathrm{e}_{ij} = 0$; $\varepsilon_{ij}$ represents the efficiency of the most efficient path between node $i$ and node $j$. The initial removal of a node starts the dynamics of redistribution of flows on the network, which changes the most efficient paths between nodes. $\varepsilon_{ij}$ can be calculated by using the information contained in adjacency matrix $\{e_{ij}\}$ which can be obtained by following iterative rule as shown in Eq. (2.4)

$$e_{ij}(t+1)=\begin{cases} e_{ij}(0)\dfrac{C_i}{L_i(t)} & \text{if } L_i(t)>C_i \\ e_{ij}(0) & \text{if } L_i(t)\le C_i \end{cases} \tag{2.4}$$

where $j$ extends to all the first neighbors of $i$; $L_i(t)$ is the load on node $i$ at time $t$ ( the total number of the most efficient paths passing through node $i$ at time $t$ ) and; $C_i$ is the capacity of node $i$, which is proportional to its initial load. Therefore, if node $i$ is congested at time $t$, the efficiency of all the links passing through it will be reduced so that eventually the flow will take the new most efficient paths.

In addition, Elsayed (2012) presents a conditional reliability by using joint density function (*jdf*) to analyze the general systems whose components experience cascading failures which also can be considered as dependent failures of the components. This approach requires that the *pdf* of the failure-time distribution of each component in the system as well as the *jdf*'s of all components be known. For example, if two identical components are in parallel with constant failure rates of $\lambda_s$ when they operate singularly and $\lambda_b$ when both operate simultaneously. Let $\tau$ be the time of the first failure and $g_1(\tau)$ be the density function for the first failure as shown in Eq. (2.5); the time of the second failure is $t$ $(0<\tau<t)$ and its dependent function, $g_2(t\mid\tau)$ as shown in Eq. (2.6).

$$g_1(\tau)=2\lambda_b e^{-2\lambda_b\tau} \qquad 0<\tau<t \tag{2.5}$$

$$g_2(t \mid \tau) = \begin{cases} \lambda_s e^{-\lambda_s (t-\tau)} & 0 < \tau < t \\ 0 & t < \tau \end{cases} \tag{2.6}$$

The pdf, $\phi\ (\tau, t)$, can be expressed in Eq. (2.7)

$$\phi\ (\tau, t) = g_1(\tau) g_2(t \mid \tau) \qquad 0 < \tau < t \tag{2.7}$$

The marginal density function, $f(t)$, can be obtained in Eq. (2.8)

$$f(t) = \int_0^t \phi\ (\tau, \xi)\ d\xi \tag{2.8}$$

Therefore, the reliability of this system can be obtained as given in Eq. (2.9)

$$R(t) = 1 - \int_0^t f(\xi)\ d\xi \tag{2.9}$$

**2.5 Summary and Conclusions**

In this chapter, the literature of the multi hazard is reviewed in details. We propose an additive form to obtain the overall system's failure rate by integrating the occurrence frequency and severity of the different types of hazards; where all the failure rates are assumed to be constant. However, under most circumstances, system normal failure rate is time-dependent (such as Weibull and Lognormal). Likewise, the factors that affect the natural and manmade hazards vary dynamically and randomly and the proposed

system failure rate needs to be modified accordingly. Through a comprehensive review of natural hazard, manmade hazard, and multi hazard that considers the dependency between hazards, the methods to predict and mitigate the damage of the hazards and the guide to restore from hazards are suggested. Although substantial studies have been conducted on simulation-based hazard assessment, little progress is achieved in understanding the inner pattern of the hazards. Moreover, lacking quantitative modeling of the interaction among different types of hazards and determining the occurrence sequence of hazards, appropriately incorporating the three types of failure rates into overall system's failure rate becomes a challenge. We also examine the qualitative and semi-quantitative framework of resilience definitions and their characteristics in different scenarios and summarize various abilities that are considered in system's resilience definitions and qualitative assessments in Table 2.1. Most researchers initially focus solely on system robustness, while ignoring the system recovery after the hazards, which is also an indispensable factor to assess the resilience of the system. We then present a thorough review of literature of the importance measure. Specifically, importance measures are developed from binary systems to multi-state systems, from discrete-state systems to continuous-state systems and from non-repairable systems to repairable systems. However, the applications of importance measures are limited to specific scenarios. Most of large complex systems include cascading failures may lead to the failure of the entire system due to a minor failure. Finally, we discuss the cascading failures in different type of systems and corresponding methods of their mitigation or avoidance in order to improve the system's resilience.

# CHAPTER 3

# RESILIENCE

In chapter 2, we review the qualitative and semi-quantitative resilience definitions. In this chapter, we provide a detailed review of the quantifications of the resilience followed by the proposed resilience quantification. We begin this chapter with general system's resilience scenarios and conclude that most of the current studies on resilience quantification include some of the following factors: (1) system performance loss; (2) system performance recovery; (3) system performance level at arbitrary times after the hazard; (4) system performance loss throughout the hazard and recovery period or arbitrary time period; (5) system performance throughout the hazard and recovery period; (6) length of system recovery period and (7) length of the hazard period. In order to adapt the previous resilience quantifications to more general situations, we propose two resilience quantifications for non-repairable and repairable systems in section 3.2 and section 3.3, respectively.

## 3.1 Resilience Quantification

Figure 3.1 illustrates system's resilience behavior, using $P(t)$ as the system performance function at time $t$. Under normal failures, a system operates with steady system performance $P(t_0)$ (normalized performance level $P(t_0) \leq 1$), from time $t_0$ until the occurrence of the hazard at time $t_h$ (the system performance is $P(t_h)$, which

usually equals $P(t_0)$); the hazard deteriorates system's performance to level $P(t_d)$ at time $t_d$. Then, maintenance actions start restorations (if the system is repairable) until it reaches a desired level of performance $P(t_r)$ at time $t_r$, where we assume without loss of generality that $P(t_r) \le P(t_0)$.

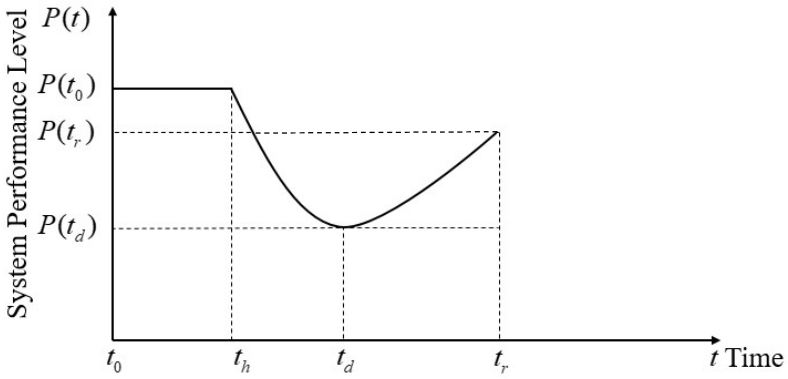



**Figure 3.1** Schematic diagram of the system performance behavior.

Most of the current studies on resilience quantification consider one or more of the following factors:

1) System performance at a specific time point: $P(t)$;
2) System performance loss due to the hazard: $P(t_0) - P(t_d)$;
3) System performance recovery: $P(t_r) - P(t_d)$;
4) System performance loss throughout the hazard and recovery period or arbitrary time period $[t_a, t_b]$: $P(t_0)(t_r - t_h) - \int_{t_h}^{t_r} P(t)\,dt$ or $P(t_0)(t_b - t_a) - \int_{t_a}^{t_b} P(t)\,dt$;
5) System performance throughout the hazard and recovery period or arbitrary time period $[t_a, t_b]$: $\int_{t_h}^{t_r} P(t)\,dt$ or $\int_{t_a}^{t_b} P(t)\,dt$;

6) Length of system recovery period: $t_r - t_d$;

7) Length of the hazard period: $t_d - t_h$.

The above factors are discussed in system resilience quantification as presented in Table 3.1.

**Table 3.1** System's resilience quantification with various factors.

| | Performance at a specific time point | Performance loss at a specific time point | Performance recovery at a specific time point | Performance loss over a period | Performance over a period | Length of recovery period | Length of hazard period |
|---|---|---|---|---|---|---|---|
| Henry and Ramirez-Marquez (2012) | | √ | √ | | | | |
| Baroud *et al.* (2014) | | √ | √ | | | | |
| Hosseini and Barker (2016) | | √ | √ | | | | |
| Barker *et al.* (2013) | | √ | √ | | | | |
| Cutter *et al.* (2008) | | √ | √ | | | | |
| Nan and Sansavini (2017) | | √ | √ | | | | |
| Pant *et al.* (2014a) | | √ | √ | | | | |
| Luo and Yang (2002) | | | | | | √ | √ |
| Wang *et al.* (2010) | | | | | | √ | |
| Cimellaro *et al.* (2010b) | | | | | √ | | |
| Bruneau *et al.* (2003) | | | | √ | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Bruneau and Reinhorn (2007) | | | | √ | | | |
| Ouyang *et al.* (2012) | | | | | √ | | |
| Ouyang and Dueñas-Osorio (2012) | | | | | √ | | |
| Ouyang and Dueñas-Osorio (2014) | | | | | √ | | |
| Ouyang and Wang (2015) | | | | | √ | | |
| Cimellaro *et al.* (2010a) | | √ | √ | √ | √ | √ | √ |
| Attoh-Okine *et al.* (2009) | | | | | √ | | √ |
| O'Rourke (2007) | | | | | √ | | |
| Reed *et al.* (2009) | | | | | √ | | |
| Adams *et al.* (2012) | | √ | √ | | √ | √ | |
| Sahebjamnia *et al.* (2015) | √ | | | | | | |
| Franchin and Cavalieri (2015) | | | | | √ | | |
| Vugrin *et al.* (2014) | | √ | | | | √ | |
| Zobel (2010) | | √ | | | | √ | |
| Zobel (2014) | | √ | | | | √ | |
| Nan and Sansavini (2017) | √ | | √ | √ | | √ | |
| Tran *et al.* (2017) | √ | √ | √ | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Orwin and Wardle (2004) | | √ | √ | | | | |
| Faturechi and Miller-Hooks (2014b) | √ | | √ | | | | |
| Chen and Miller-Hooks (2012) | √ | | √ | | | | |
| Omer *et al.* (2014) | √ | | √ | | | | |
| Miller-Hooks *et al.* (2012) | √ | | √ | | | | |
| Jin *et al.* (2014) | √ | | √ | | | | |
| Sarre *et al.* (2014, Chen *et al.* (2017) | √ | | √ | | | | |
| Janić (2015b) | √ | | √ | | | | |
| Zhao *et al.* (2017) | √ | | √ | | | | |
| Chen *et al.* (2017) | √ | | √ | | | | |
| Faturechi *et al.* (2014) | √ | | √ | | | | |
| Chang and Shinozuka (2004) | | | √ | | | √ | |
| Hashimoto *et al.* (1982) | | | √ | | | √ | |
| Li and Lence (2007) | | | √ | | | √ | |

System resilience at recovery time $t_r$, $\Re(t_r)$, is quantified in Eq. (3.1) as the ratio between system performance recovery and system performance loss (Henry and

Ramirez-Marquez (2012), Baroud *et al.* (2014), Hosseini and Barker (2016), Barker *et al.* (2013), Cutter *et al.* (2008), and Nan and Sansavini (2017)). Pant *et al.* (2014a) extend Eq. (3.1) to obtain system's resilience-related metrics under stochastic conditions.

$$\Re\left(t_r\right)=\frac{P\left(t_r\right)-P\left(t_d\right)}{P\left(t_0\right)-P\left(t_d\right)} \tag{3.1}$$

Other studies take the effect of time into consideration; i.e., system performance change "rapidity", where the "rapidity" could be either used to describe system performance loss or system performance recovery. For example, resilience is quantified as the sum of the time it takes the system to degrade and to recover, i.e., $\Re\left(t_r\right)=t_r-t_h$ (Luo and Yang (2002)); however, the magnitude of system performance recovery is not addressed. Wang *et al.* (2010) propose system resilience based on its maximum recovery ability, i.e., the ratio between system's demand recovery time and actual recovery time.

Combining the effect of time and magnitude of system performance change, Cimellaro *et al.* (2010b) quantify system resilience in terms of system performance level throughout the hazard and recovery period ( $\int_{t_h}^{t_r} P(t)\,dt$ ). Furthermore, system performance under its steady state is adopted in some studies: interpreting $P\left(t_0\right)\left(t_r-t_h\right)$ as system's desired performance level throughout the hazard and recovery phases, resilience can be either considered as $P\left(t_0\right)\left(t_r-t_h\right)-\int_{t_h}^{t_r} P(t)\,dt$

(Bruneau *et al.* (2003) and Bruneau and Reinhorn (2007)) or as $\frac{\int_{t_h}^{t_r} P(t)\,dt}{P(t_0)(t_r - t_h)}$ (Ouyang *et al.* (2012), Ouyang and Dueñas-Osorio (2012), Ouyang and Dueñas-Osorio (2014) and Ouyang and Wang (2015)). These quantifications are similar to Cimellaro *et al.* (2010a), Bocchini and Frangopol (2012) and Attoh-Okine *et al.* (2009).

It is worth noting that in the above quantifications, $P(t_0)$ can be either normalized as 1 (i.e., the system has the highest level of steady-state performance) or any value $P(t_0)<1$. Besides, two generalizations can be made: 1) $\int_{t_h}^{t_r} P(t)\,dt$ could change to $\int_0^T P(t)\,dt$, where the latter can be understood as the system performance over any time period of interest; 2) $P(t)$ could follow a probabilistic process as stated earlier. O'Rourke (2007) defines system resilience at arbitrary time $t_b$ as $\Re(t_b) = \frac{\int_{t_a}^{t_b} P(t)\,dt}{t_b - t_a}$, where resilience is quantified as the average system performance during a period of time $[t_a, t_b]$; this quantification is also adopted in Reed *et al.* (2009). As a simplification, system resilience is assessed by assuming that $P(t)$ in the above resilience quantifications as a linearly decreasing function during the hazard period and a linearly increasing function during the recovery period as presented in Adams *et al.* (2012), Sahebjamnia *et al.* (2015), and Zobel and Khansa (2014). Applications and variations of resilience quantification are presented in Adams *et al.* (2012), Zobel (2011) and Sahebjamnia *et al.* (2015), and Mugume *et al.* (2015).

Other resilience quantifications mainly emphasize system recovery phase. Franchin and

Cavalieri (2015) obtain resilience as the normalization of system recovery performance over the recovery phase, i.e., $\frac{\int_{t_d}^{t_r} P(t)\ dt}{P(t_0)(t_r - t_d)}$. Vugrin *et al.* (2014) link resilience to the optimal recovery sequence of failed parts, where resilience mainly focuses on system recovery ability after the hazard occurrence. Specifically, some studies consider that the shape of a recovery curve provides an indication of a system's recovery ability over time (Cimellaro *et al.* (2010a), Cimellaro *et al.* (2010b), Zobel (2010) and Zobel (2014)), where four types of recovery curves (linear, trigonometric, exponential and inverted exponential) are utilized.

More generally, resilience could also be quantified using different measures during different stages starting from the hazard occurrence to the recovery at desired performance levels. For example, Nan and Sansavini (2017) use robustness, system rapidity, average performance loss, recovery ability (Eqs. (3.2)-(3.5)), to respectively characterize system resilience in the original steady phase, disruptive phase, recovery phase, and steady phase (post-recovery phase). Similarly, Tran *et al.* (2017) include system performance, absorption ability, recovery ability and volatility ability into system resilience calculation.

$$\text{Robustness} = \text{Min}\ \{P(t);\ t_h \leq t \leq t_r\} \tag{3.2}$$

$$\text{Rapidity} = \frac{P(t_h) - P(t_d)}{t_d - t_h} \tag{3.3}$$

$$\text{System Average Performance Loss} = \frac{\int_{t_h}^{t_d} (P(t_0) - P(t))\, dt}{t_d - t_h} \tag{3.4}$$

$$\text{Recovery Ability} = \frac{P(t_r) - P(t_d)}{P(t_h) - P(t_d)} \tag{3.5}$$

Besides the above commonly adopted resilience quantification, factors 1) - 7) are taken into consideration in terms of other forms of mathematical expressions by Orwin and Wardle (2004), Enjalbert *et al.* (2011), Zobel (2011), Franchin and Cavalieri (2015), Chang and Shinozuka (2004), and Attoh-Okine *et al.* (2009). As a generalization, Zobel and Khansa (2014) extend system resilience quantification to multi overlapping hazards. Dessavre *et al.* (2016) quantify system resilience under multiple hazards as an additive form of the resilience under each type of hazard.

As stated earlier, resilience of service-oriented network systems is typically quantified as the expected fraction of total pre-event demand that is met after the recovery action (Faturechi and Miller-Hooks (2014b)), i.e., $\Re(t) = \frac{E\left(\sum_{\forall i} f_i\right)}{\sum_{\forall i} D_i}$; where $f_i$ and $D_i$ are respectively the post-repair performance level and the desired performance level of the $i^{th}$ component/subsystem in the network. Similarly, resilience is considered as the ratio of the delivery ability of the network after and before a hazard by Chen and Miller-Hooks (2012), Omer *et al.* (2014), Janić (2015b), Jin *et al.* (2014), Miller-Hooks *et al.*

(2012), Fotouhi *et al.* (2017), Sarre *et al.* (2014), Faturechi *et al.* (2014), Chen *et al.* (2017) and Zhao *et al.* (2017). Moreover, Ouyang (2017) quantifies the resilience of interdependent network infrastructure as the amount of demand being satisfied at arbitrary time; which can be interpreted as $P(t)$; this quantification is similar to Janić (2015a). Following the qualitative what-if analysis mentioned in section 2.2.2, Filippini and Silva (2014) specifically calculate resilience as the sum of all components' which may result in the overall system's deadlock states.

In addition to the above-stated factors, reliability-related performance measurements such as reliability function and redundancy are used to assess system resilience as introduced earlier. Youn *et al.* (2011) mathematically define resilience as the sum of normalized system reliability and recovery ability; Ayyub (2014) also presents a resilience assessment by prescribing both reliability and recovery duration strategies. Yodo *et al.* (2017) apply the dynamic Bayesian network approach to discuss the general framework of modeling and quantifying system resilience; where the work emphasizes that two basic attributes of resilience are reliability and restoration.

Rose (2007) quantifies economic system resilience under deterministic and dynamic cases, where system's maximum percentage loss under the hazard is taken into consideration. Specifically, system static resilience is quantified as the ratio of the avoided system performance loss and the maximum potential loss; while the dynamic resilience focuses on the speed of the system recovery from a severe shock to achieve

a desired state. These two resilience quantifications consider the worst system potential performance under the hazard.

Game-theoretic approach is used to dynamically model and optimize the resilience of cyber control system in large complex systems (such as transportation systems, smart grid systems and healthcare systems) with multi-layer optimization objectives. Specifically, the profits and strategies of both resilience "defender" and attacker are taken into consideration. For example, He *et al.* (2013) assume both defenders and attackers aim to maximize their individual utility, where the system resilience is formulated as a power-form product of the survival probabilities of cyber and physical subsystems. A game theoretic solution is employed using a game formulation that identifies optimal defense strategy to minimize the maximum cyber risk (Musman and Turner (2017)). Similarly, considering the cascading failures, a game-theoretic approach is used to model the interactions between the cyber level policy maker and physical level robust control design in cyber physical systems (Zhu and Başar (2012)).

Considering resilience as a probability, Chang and Shinozuka (2004) quantify resilience as the likelihood that the system performance loss is less than a given threshold, as well as the likelihood that the recovery time is shorter than a given threshold. Similarly, system resilience at $t$ is considered as the conditional probability that system recovers at $t$, given a system failure at $t_1$ $(t > t_1)$ (Hashimoto *et al.* (1982) and Li and Lence (2007)). Resilience assessments based on a simulation study are presented by

Ouedraogo *et al.* (2013) and Adjetey-Bahun *et al.* (2014). Other review papers on resilience definition, qualitative and quantitative analysis in a variety of domains are given in Bhamra *et al.* (2011), Bhamra *et al.* (2011), Francis and Bekera (2014), Faturechi and Miller-Hooks (2014a), Haimes (2009), Madni and Jackson (2009), Yodo and Wang (2016) and Sarre *et al.* (2014).

Resilience should evaluate systems robustness and its ability to recover to a desired performance level, but most of the current quantifications of resilience either ignore system performance recovery or system design robustness. Therefore, in non-repairable systems, we propose a general quantification of system resilience regarding system robustness; and in the repairable systems, we propose another quantification of resilience which considers system's robustness as well as the recovery ability.

### 3.2 Proposed Resilience Quantification for Non-repairable Systems

Non-repairable Systems include satellite failures and one-shot units such as missiles and airbags. System robustness is an important indicator to assess the ability of the system to resist external disruptive events with no or minimum deterioration of its performance. We extend Chen and Elsayed (2017) resilience quantification. Specifically, system performance deterioration magnitude and rate are included in the resilience quantification as given in Eq. (3.6):

$$\Re(t_d) = \frac{t_d - t_h}{2t_h}\left[P(t_h) + P(t_d)\right] \tag{3.6}$$

It is without loss of generality to assume $t_h > 0$, where $t_h$ is the reference time point at which the hazard occurs. Eq. (3.6) considers the system performance (specifically, robustness) during the hazard period. Specifically, fixing $t_h$ and $P(t_h)$, system resilience is a decreasing function of its performance loss ($P(t_h) - P(t_d)$) and is an increasing function of its performance deteriorating period ($t_d - t_h$).

Reliability is the most important performance criterion of the non-repairable systems, which indicates that we may consider the reliability $R(t)$ as the performance function $P(t)$. Therefore, substituting reliability for system performance function, Eq. (3.6) can be written as Eq. (3.7)

$$\Re(t_d) = \frac{t_d - t_h}{2t_h}\left[R(t_h) + R(t_d)\right] \tag{3.7}$$

### 3.3 Proposed Resilience Quantification for Repairable Systems

Repairable systems include power distribution, water distribution, telecommunications systems and others. Catastrophic failures and damage severity of repairable systems may render such systems as non-repairable such as in the case of the triple meltdown at Fukushima Daiichi nuclear reactor in Japan in 2012 and Chernobyl nuclear power

plant in Ukraine in 1986. Availability is considered to be one of the most important reliability performance measures of maintained systems since it includes both the failure rates and repair rates of the components. It describes the proportion of time that a system functions properly during steady state. Availability is classified either according to (1) the time interval considered or (2) the type of downtime (repair and maintenance). The time-interval availability includes instantaneous (or point availability), average uptime, and steady-state availabilities. The availability classification according to downtime includes inherent, achieved, and operational availabilities (Lie *et al.* (1977)). Other classifications include mission-oriented availabilities. Therefore, it's reasonable to consider instantaneous availability $A(t)$ (the probability that the system is operational at any random time $t$) as the system performance function $P(t)$ in repairable systems.

In non-repairable system, resilience is usually determined by system structural design (explicit and implicit redundancies) and the quality and the reliability of its components. However, resilience in repairable system is not only affected by above factors but also requires the implementation of an effective maintenance and inspection program to maintain the steady-state availability or improve the point availability of the system.

### 3.3.1 Changes of System Availability in Repairable Systems

We assume system availability is a three-stages piece-wise function of time: (1) before

hazards ($t \le t_h$) (normal failure and repair), system has steady-state availability $A(t_h)$ (usually $A(t_h) \le 1$); (2) during random multi hazards ($t_h < t \le t_d$) (no repair or minimal if any), system has decreasing availability; during recovery ($t_d < t$), system has increasing availability corresponding to the repair function (no failure or minor failures). Specifically, when system has time-dependent failure rate and constant repair rate in stage (2), system availability can be obtained by a semi-Markov model or alternating renewal process. In stage (3), the repair function can be described by a stochastic process, which can be modeled as Brownian motion or Gamma process.

In general, each component has a varying degree of degradation and maintenance resources after the hazards and follows its own repair function such as Brownian motion or Gamma process, which shows the amount of the recovery with time. Hence during the repair, we assume that the repair rate of the overall system is the integration of all different repair functions of its components. The details of the Brownian motion and Gamma process are illustrated as follows.

3.3.1.1 Brownian Motion

The Brownian motion, sometimes called the Wiener process, is a continuous-time stochastic process and one of the most useful stochastic processes in pure and applied mathematics, economics, quantitative finance, and physics. A stochastic process $\{X(t),\ t \ge 0\}$ is said to be a Brownian motion if (Ross (2014)):

1) $X(0) = 0$;

2) $\{X(t),\ t \geq 0\}$ has stationary and independent increments; and

3) $X(t)$ is normally distributed with mean 0 and variance $\sigma^2 t$.

When $\sigma^2 = 1$, the process is referred as standard Brownian motion ($\{B(t),\ t \geq 0\}$) which can be easily accomplished for any process. Geometric Brownian motion is the most applicable to actual recovery process, which shows the amount of the recovery of the overall system (or component) availability and is an exponentiated version of the standard Brownian motion as shown in Eq. (3.8)

$$Y(t) = Y_0\ e^{\sigma B(t) + \left(\mu - \frac{1}{2}\sigma^2\right)t} \tag{3.8}$$

Where $\mu$ is the repair rate of the system (or component), $\sigma$ is the diffusion coefficients and $Y(0) = Y_0 > 0$ is the initial value. Specifically, due to the volatility of the geometric Brownian motion, the recovery time that the system (or component) achieves to a targeted availability is usually defined in a range. Therefore, we can consider the "mean time" $\overline{t_r}$ as the alternative recovery time as shown in Figure 3.2.

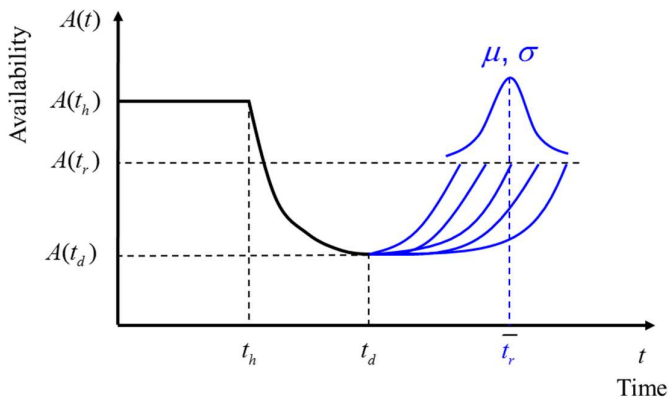



**Figure 3.2** Repair functions of system (or component).

3.3.1.2 Gamma Process

The Brownian Motion is suitable for non-monotone recovery processes. However, this may not be a realistic assumption and it may not be suitable to use in a recovery process that has strictly positive increments. The gamma process can be applied for monotone recovery. Gamma processes play a crucial part in inspection and maintenance of complex systems such as dikes, beaches, steel coatings, berm breakwaters, steel pressure vessels, underground trains, and high-speed railway tracks. Gamma processes are also satisfactorily fitted to real-life data on creep of concrete, fatigue crack growth, corrosion of steel protected by coatings, corrosion-induced thinning, chloride ingress into concrete, and longitudinal leveling of railway tracks (Van Noortwijk (2009)). In the following, we first introduce the gamma distribution and its properties then present the gamma process.

The gamma distribution is characterized by two parameters: shape parameter $\gamma$ and scale parameter $\theta$. The probability density function of a gamma distribution is given by Eq. (3.9)

$$f(t)=\frac{t^{\gamma-1}\theta^{\gamma}}{\Gamma(\gamma)}e^{-\theta t} \tag{3.9}$$

The cumulative distribution function, $F(t)$, can be expressed as in Eq. (3.10)

$$F(t)=\int_0^t \frac{\tau^{\gamma-1}b^{\gamma}}{\Gamma(\gamma)}e^{-\theta\tau}d\tau \tag{3.10}$$

Substituting $\tau\theta=c$, we obtain $F(t)=\frac{1}{\Gamma(\gamma)}\int_0^{\theta t} c^{\gamma-1}e^{-c}dc$ or $F(t)=I(\theta t,\gamma)$, where $I(\theta t,\gamma)$ is known as the incomplete gamma function. The expectation and variance of the gamma distribution are respectively: $E[t]=\frac{\gamma}{\theta}$ and $Var[t]=\frac{\gamma}{\theta^2}$.

We utilize the gamma distribution properties to explain the recovery process since it is a stochastic process with independent, non-negative increments where each increment follows the gamma distribution with the same scale parameter $\theta>0$, and shape parameter $\gamma(t)>0$, which can be expressed as $\Gamma(t;\gamma,\theta)$. The random variable $X(t)-X(s)$ for $0\le s<t$ follows gamma distribution $\Gamma(\gamma(t-s),\theta)$ and is expressed in Eq. (3.11)

$$f_{X(t)}(x;\gamma(t-s),\theta)=\frac{\theta^{\gamma(t-s)}}{\Gamma(\gamma(t-s))}x^{\gamma(t-s)-1}e^{-\theta x} \tag{3.11}$$

where $X(t)\sim\Gamma(\gamma(t-s),\ \theta)$ is the recovery at time $t$ follows the gamma distribution with time dependent shape parameter. The mean and variance of the gamma process are $E\ [x]=\frac{\gamma(t)}{\theta}$ and $Var\ [x]=\frac{\gamma(t)}{\theta^2}$ , respectively, which implies that the mean and variance increase linearly with time.

However, the gamma process introduces intrinsic randomness as shown in Figure 3.3 (Cheng *et al.* (2018)), where the red scatter plot shows a recovery process with higher rate than the blue scatter plot. Using initial recovery time data one can obtain the expected time to reach a specified performance level of the system. The recovery time $T_P$ to achieve performance level $P$ is obtained by finding the value of $T_P$ that satisfies Eq. (3.12)

$$P(X(T_P)\geq t)=P(X(T_P)\geq P)=1-\int_0^P\frac{1}{\Gamma(\gamma t)}\theta^{\theta t}x^{\gamma t-1}e^{-\theta x}dx \tag{3.12}$$

Therefore, initial recovery data can be used to estimate the parameters of the recovery process using the Gamma process and obtain the expected recovery time to reach a specified performance level.

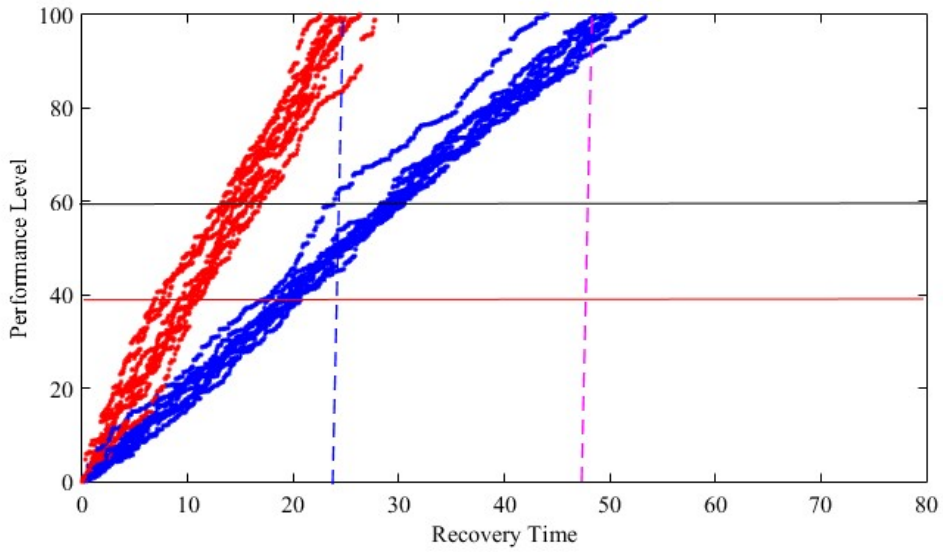



**Figure 3.3** Gamma processes with different mean and variance (Cheng *et al.* (2018)).

### 3.3.2 Proposed Resilience Quantification

In repairable systems, we propose a resilience quantification that focuses on system performance robustness (performance deterioration magnitude and rate) as well as its recovery ability (performance recovery magnitude and rate) after the hazards as given in Eq. (3.13)

$$\Re(t_r) = \frac{P(t_r) - P(t_d)}{P(t_h) - P(t_d)} \cdot \frac{t_d - t_h}{t_r - t_h}, \qquad t_r > t_d \tag{3.13}$$

where the term $\frac{t_d - t_h}{t_r - t_h}$ in Eq. (3.13) is interpreted as the system steady-state availability. Moreover, the system recovery time $(t_r - t_h)$ is taken into consideration.

This general definition is independent of the shape of the degradation and recovery functions as it only includes the time that it takes the system to reach an unacceptable level of system performance as well as the system recovery time to achieve a desired performance level. Substitute the availability for system performance function in Eq. (3.13) to obtain Eq. (3.14)

$$\Re(t_r) = \frac{A(t_r) - A(t_d)}{A(t_h) - A(t_d)} \cdot \frac{t_d - t_h}{t_r - t_h}, \qquad t_r > t_d \tag{3.14}$$

As the resilience of repairable systems depends on its recovery ability, its requires efficient approaches to recover system performance to the desired level in a relatively short time by identifying the repair priorities of the system's components. In chapter 4, we present a detailed discussion on importance measures of the system's components and their role in repair priorities.

### 3.4 Summary and Conclusions

In this chapter, we provide a detailed literature review of resilience quantification and summarize system's resilience quantification with various factors. Then we conclude that most of the current quantifications of resilience either ignore system performance recovery or system design robustness. Therefore, in non-repairable systems, we propose a general quantification of system resilience regarding system robustness, which takes

the reference point $t_h$ when hazard occurs into consideration in order to effectively demonstrate the system's "resistance" to hazards. In repairable systems, by assuming system availability is a three-stages piece-wise function of time, the system availability at any time point can be obtained. We then propose a quantification of resilience that considers both the recovery ability as well as system robustness in repairable systems. It is noted that the two proposed resilience quantifications are applicable when the system is subjected to multi hazard, where the challenge exists in obtaining system's performance indicator under multi hazard based on the system configuration and the type of hazards. For example, the system's performance deterioration under the interactions of multi hazard is not the sum of its performance deterioration induced by every single hazard independently. Likewise, system's performance restoration process under multi hazard is also challenging; for example, one hazard may occur when restoration of previous hazard(s) has not ended; under such circumstance, the overall system restoration process is affected.

Indeed, acceptance and unification of the resilience definition and quantification across disciplines require interdisciplinary interactions and research collaborations. For example, in the proposed resilience quantifications, the knowledge in both reliability engineering and civil engineering are required to appropriately utilize system reliability metrics as effective system performance indicator. Similarly, statistical models are utilized when incorporating the multi hazard in the overall system's failure rate to reflect the effect of the multi hazard on system's resilience.

# CHAPTER 4

# IMPORTANCE MEASURES

In this chapter, we present a comprehensive review of the quantifications of the Importance Measures (IMs) of the systems' components for non-repairable and repairable systems. We begin this chapter with the IMs of non-repairable systems followed by the proposed weighted IM for non-repairable systems in section 4.2, which alleviates the concerns of inability of the current IMs in distinguishing the importance of components in some reliability configurations. We then present a review of IMs for repairable systems in section 4.3. In section 4.4, we present the weighted IM for repairable systems.

## 4.1 IMs for Non-repairable Systems

In the design stage, engineers may use IMs to determine the components that merit additional research and development to improve overall system robustness at minimum cost or effort.

The IM is first proposed by Birnbaum (1968) as BIM, using the structure function to calculate the probability that a specific component is critical to the system performance; specifically, at time $t$, the $i^{th}$ component's importance is calculated by taking the partial derivative of system unreliability function with respect to the unreliability of the

$i^{th}$ component. It is expressed as shown in Eq. (4.1)

$$I_B^i(t) = \frac{\partial G(q(t))}{\partial q_i(t)} = G\left(1_i, q(t)\right) - G\left(0_i, q(t)\right) \tag{4.1}$$

where $q_i(t)$ is the unreliability function of the component $i$; $G(q(t))$ is the unreliability function of the system; $G\left(1_i, q(t)\right)$ is the unavailability of the system when component $i$ is not working and $G\left(0_i, q(t)\right)$ is the unavailability of the system when component $i$ is working (BIM assumes that components are independent and have binary-states, where $1_i$ means $q_i = 1$ and $0_i$ means $q_i = 0$).

Other commonly and widely used IMs include the following. Fussell-Vesley IM is proposed by Vesely (1970) and used by Fussell (1975), which is the probability that the system's life coincides with the failure of a cut-set containing component. It can be expressed as shown in Eq. (4.2)

$$I_{FV}^i(t) = \frac{G_i(q(t))}{G(q(t))} \tag{4.2}$$

where $G_i(q(t))$ is the probability of component $i$ contributing to a cut-set of the system. There are two notable risk IMs proposed by Vesely and Davis (1985) to evaluate a component's importance in further reducing the risk and its importance in maintaining the present risk level. The first is the risk achievement worth (RAW) and

is given in Eq. (4.3)

$$I_{RAW}^{i}(t) = \frac{G\left(1_i, q\left(t\right)\right)}{G(q(t))} \tag{4.3}$$

It is the ratio between the conditional system unreliability given that component $i$ has failed and the system unreliability. It represents the importance of maintaining the current level of reliability with respect to the failure of the component. The second is the risk reduction worth (RRW) importance measure and is given in Eq. (4.4)

$$I_{RRW}^{i}(t) = \frac{G(q(t))}{G\left(0_i, q\left(t\right)\right)} \tag{4.4}$$

It is the ratio between the system unreliability and the system conditional unreliability given that component $i$ is working. It shows that the risk of maximum decrease of the system performance can be avoided by the improvement of the component, which is particularly useful for identifying improvements to the reliability of components which can most reduce risk. Comprehensive and extensive extensions and improvements are presented in Cheok *et al.* (1998), Vasseur and Llory (1999), Van der Borst and Schoonakker (2001), Borgonovo and Apostolakis (2001), and Borgonovo and Smith (2012). Furthermore, Borgonovo and Apostolakis (2001) introduce an additive IM, the differential importance measure (DIM). Later, two interaction order and multiple interaction order for the criticality of combinations of components are presented by Zio

and Podofillini (2006) and Do Van *et al.* (2010), respectively.

Barlow and Proschan (1975) propose a time-independent modification of the BIM corresponding to the conditional probability that component causes the system to fail in the time interval $(t_h,\ t_F)$, given that the system has failed in the same period, which leads to the well-known Barlow-Proschan IM and is expressed as given in Eq. (4.5)

$$I_{BP}^{i} = \frac{\int_{t_h}^{t_F} \frac{\partial G(q(t))}{\partial q_i} \frac{dq_i}{dt} dt}{\sum_{k=1}^{n} \int_{t_h}^{t_F} \frac{\partial G(q(t))}{\partial q_k} \frac{dq_k}{dt} dt} \tag{4.5}$$

where $n$ is the total number of components in the system. Based on Barlow-Proschan IM, Lambert (1975a) introduces the enabler IM as another time-independent IM. Xie (1987) and Xie and Bergman (1991) generalize Barlow-Proschan IM using the system yield function and develop a time-independent lifetime IM when all components are independent. Iyer (1992) extends Barlow–Proschan IM to the case of dependent components. Recently, Natvig and Gåsemyr (2006) consider both system failure and survival as two extensions of Barlow–Proschan IM.

Lambert (1975b) proposes the upgrading function IM for non-repairable systems as the fractional reduction in the probability of the system failure when component failure rate $\lambda_i$ is reduced fractionally. It is expressed as given in Eq. (4.6)

$$I_{UF}^{i}(t) = \frac{\lambda_i}{G(q(t))} \frac{\partial G(q(t))}{\partial \lambda_i} \tag{4.6}$$

Later Lambert and Yadigaroglu (1977) apply this IM to the problem of determining the optimal choice of system upgrade.

A further notable time-independent IM is proposed by Natvig (1979) and is defined mathematically as given in Eq. (4.7)

$$I_{N}^{\mathrm{i}}(t) = \frac{E(Z_i)}{\sum_{\forall j} E(Z_j)} \tag{4.7}$$

where $E(Z_i)$ is the expected reduction of system's residual life due to the $i^{th}$ unit's failure. It suggests that importance of the $i^{th}$ component to the system is reflected in terms of the impact of its failure on the reduction of system's residual life. Through continuous improvement, Natvig (1982a) obtains at the distribution of reduction in remaining system lifetime and develops another IM for the case where components have proportional hazards without repair.

Gandini (1990) provides criticality IM, which corresponds to the conditional probability that the system is in a state at time $t$ such that component $i$ is critical and has failed, given that the system has failed by the same time. It is expressed as given in Eq. (4.8)

$$I_{CR}^{i}(t)=\frac{\partial G(q(t))}{\partial q_i(t)}\times\frac{q_i(t)}{G(q(t))}=\frac{[G(1_i,q((t))-G(0_i,q(t))]\times q_i(t)}{G(q(t))} \tag{4.8}$$

## 4.2 Proposed IM for Non-repairable System

Although BIM and its extensions have been widely used for non-repairable systems, they do not adequately and effectively distinguish the importance of components in some scenarios. For example, in parallel configuration, some of the IMs rank all the components equally important in terms of their impact on the overall reliability of the system, such as Fussell-Vesely IM and criticality IM. This is a shortcoming of the measures since in parallel configuration, the most reliable component has the most impact on the system reliability. Furthermore, other IMs such as BIM can overcome the sensitivity of the parallel configuration, however, BIM fails to distinguish the importance when the components have the same failure rates but may have other information relevant to their importance. Therefore, in order to consider the importance of components in the system before applying current IMs, we assign additional weights to components regarding their importance, availability, and integrity of data, specific system structure and other special features.

Specifically, we apply the weighted IM by incorporating the weight of component $i$ in the $i^{th}$ IM for non-repairable systems. For illustration, we modify the BIM and incorporate the weights of the components as shown in Eq. (4.9)

$$I_{wB}^{i}(t) = w_i \cdot \frac{\partial G(q(t))}{\partial q_i(t)} = w_i \cdot \left(G\left(1_i, q(t)\right) - G\left(0_i, q(t)\right)\right) \tag{4.9}$$

where $w_i$ is the weight of component $i$. In order to show the effectiveness of weighted IM, we compare the results of non-weighted and weighted BIM for non-repairable cyber network in Chapter 5.

### 4.3 IMs for Repairable Systems

As presented above, the resilience of repairable systems depends on its ability to recover after the hazard occurrence. This requires methodologies that recover system performance to the desired level in a relatively short time. Identifying the repair priorities of the system's components becomes necessary. This can be achieved by estimating IMs of the system's components and their impact on the system's recovery level.

Unlike non-repairable systems, IM of components in repairable systems needs to consider components' repair and system availability. Natvig (1985) extends Eq. (4.7) to Eq. (4.10) and shows that the $i^{th}$ component's importance is determined by the expected increase in system lifetime if the $i^{th}$ component is repaired to have the same distribution of residual life as original ($E\left(U_i\right)$).

$$I_N^i(t) = \frac{E(U_i)}{\sum_{\forall j} E(U_j)} \tag{4.10}$$

Natvig and Gåsemyr (2009) extend Barlow–Proschan IM and the Natvig IM to stationary states in repairable systems by introducing dual term. Natvig *et al.* (2009) apply the extended version of Natvig IM to repairable systems, showing that a component is important if both by failing it strongly reduces the expected system uptime and by repairing it strongly reduces the expected system downtime. Natvig (2011) and Natvig *et al.* (2011) generalize previous results to multistate coherent systems.

In addition to Eq. (4.10), there exists other IMs for repairable components and systems. Hajian-Hoseinabadi and Golshan (2012) investigate component's IM in terms of the effects of component's repair on system availability improvement. Similarly, Barabady and Kumar (2007) determine the component's IM as the partial derivative of the system availability with respect to the component's availability, failure rate, and repair rate. Der Kiureghian *et al.* (2007) identify system's importance of components by providing closed-form expressions for the change rate of the probabilistic system performance with respect to the mean failure rate and mean repair of the component. Cassady *et al.* (2004) use a set of IMs to show that focusing on reducing the occurrence of system failures provides greater benefit than increasing the repair rate. Probabilistically, Miman and Pohl (2006) provide a variance importance measure, where the

component's criticality is dependent on the improvement in the system availability estimated variance due to the reduction of component's availability estimated variance. More studies on IMs regarding repairable systems are presented in Barabady (2005), Zheng *et al.* (2015), Gravette and Barker (2015), and Qarahasanlou *et al.* (2017).

In MSMC, the generalization of IMs for systems with multi-state components is investigated by El-Neweihi *et al.* (1978) to analyze the relationships between multi-state coherent system's reliability behavior and multi-state component's performance under deterministic and stochastic scenarios. Barlow and Wu (1978) obtain the IM for coherent multi-state systems, where the criticality of component $i$ to the system at state $j$ is probabilistically measured as the likelihood that when component $i$ in state $j$, the system is in state $j$ and when component $i$ is not in state $j$, the system is not in state $j$. Levitin *et al.* (2003) study the generalized IMs for multi-state components based on the restriction that component's performance is only reachable to certain states.

In particular, Griffith (1980) proposes Griffith Importance Measure (GIM), which formalizes the concept of system performance through expected utility and studies the effect of component improvement on system performance by introducing the reliability importance vector for each system component. Through this concept, a generalization of the binary BIM is extended to the multi-state case. It is expressed as given in Eq. (4.11)

$$I_G^m(i)=\sum_{\forall j}\alpha_j\left\{\left[P(\phi=j)\middle|m_i\right]-\left[P(\phi=j)\middle|(m-1)_i\right]\right\} \tag{4.11}$$

where $\alpha_j$ is the system performance at $j^{th}$ level; $P(\phi=j)|m_i$ and $P(\phi=j)|(m-1)_i$ are respectively the probability that the system is in state $j$ when the $i^{th}$ component is in state $m$ and state $m-1$. Therefore, GIM can be interpreted as the decrement of the system performance when a component $i$ deteriorates from $m$ state to $m-1$ state, which can be regarded as the importance of component $i$ in state $m$. Later Wu and Chan (2003) propose a new utility importance for a certain component state in multi-state systems to measure which component affects it the most, or which state of a certain component contributes the most to the system's reliability. Liu *et al.* (2016b) introduce the generalized GIM (GGIM) which considers the time accumulation impact on the changing of system performance by introducing an additional parameter, transition probability. It is expressed as given in Eq. (4.12)

$$I_{GGIM}^i=\sum_{\forall m}P_i(m)\sum_{l=m}^{M}P_i(l\mid m)\sum_{\forall j}\alpha_j\left\{\left[P(\phi=j)\middle|l_i\right]-\left[P(\phi=j)\middle|m_i\right]\right\} \tag{4.12}$$

where $P_i(m)$ is the probability of component $i$ is in state $m$; $P_i(l\mid m)$ is the transition probability of component $i$ from state $m$ to state $l$ (the state space of component is $\{0,...,m,...,l,...M\}$, here 0 means component functions is the ideal functioning state and $M$ means component failed; assume that system and the component can only transit from state $l$ to a better state $m$ in the maintenance process; $P(\phi=j)|m_i$ and $P(\phi=j)|l_i$ are respectively the probability that system is

in state $j$ when the $i^{th}$ component is in state $m$ and state $l$. Therefore, GGIM can be interpreted as the incremental improvement of the system performance caused by repairing component $i$.

### 4.4 Proposed IM for Repairable System

As stated earlier in section 3.3, the most common and important reliability metrics for repairable systems is availability since it includes both failure rates and repair rates of the systems, and is defined as the probability that the system is operating properly (or available for use) when it is requested. Therefore, similar to the proposed weighted IM for non-repairable systems, we propose a novel weighted IM for repairable systems by applying availability to the components and systems. It is expressed as given in Eq. (4.13)

$$I_i(t) = w_i \cdot \left( \overline{A}\left(1_i, \overline{a}(t)\right) - \overline{A}\left(0_i, \overline{a}(t)\right) \right) \tag{4.13}$$

where $\overline{a}_i(t)$ is the unavailability function of the component $i$; $\overline{A}(\overline{a}(t))$ is the unavailability function of the system; $\overline{A}\left(1_i, \overline{a}(t)\right)$ is the unavailability of the system when component $i$ is not working and $\overline{A}\left(0_i, \overline{a}(t)\right)$ is the unavailability of the system when component $i$ is working (assuming that components are independent and binary-state, here $1_i$ means $\overline{a}_i = 1$ and $0_i$ means $\overline{a}_i = 0$).

### 4.5 Summary and Conclusions

IM is of great benefit not only for the designer's insight into a system but also for system maintenance. In this chapter, we present an overview of the quantifications of IM for non-repairable systems and repairable systems. In non-repairable systems, BIM and its extended IMs are studied and widely applied. However, some of these IMs do not adequately and effectively distinguish the importance of components in some scenarios. For example, in parallel configuration, some of IMs rank all the components equally in terms of their impact on the overall reliability of the system, such as Fussell-Vesely IM and criticality IM. Furthermore, although other IMs such as BIM can overcome the sensitivity to the parallel configuration, once the components contain different importance of the content (data) but same failure rates, BIM also fails to distinguish them. Therefore, in order to consider the importance of components in the system before applying current IMs, we assign additional weights to components regarding their importance, availability, and integrity of data, specific system structure, and special features. Unlike non-repairable systems, IMs of components for repairable systems need to consider components' repair ability and system availability. We propose a weighted IM for repairable systems which provides more realistic ranking of the components' importance.

# CHAPTER 5

# RESILIENCE AND IM APPLICATION IN CYBER NETWORK

In chapters 3 and 4, we present a variety of quantifications of the resilience and IM, followed by our proposed quantification methods for non-repairable and repairable systems. With the rapid development of technology, cyber is becoming important to our daily life and the national security. Cyber resilience is attracting increasing interests and is becoming a primary cyber network objective. In this chapter, we apply our proposed methods of resilience quantification and IM in a cyber network in order to demonstrate their effectiveness and adequacy. We begin this chapter with cyber resilience, which consists of cyber robustness and cyber recovery in section 5.1.1 and 5.1.2, respectively. We then apply the proposed resilience and IM methods for non-repairable small cyber network including cascading failures in section 5.2. We also discuss the sources of compromise of cyber networks in order to estimate importance weights for each node in the cyber network. In section 5.3, we demonstrate our proposed resilience quantification and IM methods for repairable cyber networks including cascading failures.

## 5.1 Cyber Resilience

Cyber resilience is attracting increasing interests and is becoming a primary system objective because it is unrealistic to completely defend against cyber attacks; instead,

it is more realistic to ensure network operation even in a degraded or contested environment (Goldman *et al.* (2011)). Specifically, cyber resilience can be viewed and understood from two aspects: cyber robustness (the ability that a network can withstand and minimize the consequence of a cyber attack) and cyber recovery (the ability that a network can quickly recover from the disruptive state). In the following, we discuss cyber resilience in terms of its robustness and recovery ability, during and after the cyber attack.

### 5.1.1 Cyber Robustness

The ability that a network system detects, defends and absorbs the impact of the cyber attack is an indicator of system's robustness. Cyber attack detection has been defined as "the problem of identifying individuals who are using a computer system without authorization (crackers) and those who have legitimate access to the system but are abusing their privileges (insider threat)" (Singh and Silakari (2009)). Modern cyber attack detection systems monitor either host computers or network links to assess cyber attack data (Karthikeyan and Indra (2010)). Host intrusion detection refers to the class of intrusion detection systems that reside on and monitor an individual host machine. In addition, a cyber attack detection system monitors the packets that traverse a given network link. Currently, a cyber attack detection system has three basic approaches to identify cyber attacks: misuse detection, anomaly detection and specification based detection (Singh and Silakari (2009)). These detection methods are applied in cyber-

physical systems (CPS) such as large-scale industrial applications, critical infrastructures, industrial automation systems (Kim and Kumar (2012) and Ahmed *et al.* (2013)). Corradini and Cristofaro (2017) propose a design technique to address the problem of detection and reconstruction of a linear cyber-physical system after the cyber attacks. Chhetri *et al.* (2016) present a novel attack detection method to detect zero-day kinetic cyber attacks on additive manufacturing, by identifying anomalous analog emissions which arise as an outcome of the attack. Bezemskij *et al.* (2016) develop a detection mechanism, which monitors real-time data from a large number of sources onboard a vehicle, including its sensors, networks and processing. Pasqualetti *et al.* (2013) propose a mathematical framework for cyber-physical systems under attacks, monitor and characterize fundamental monitoring limitations from system-theoretic and graph-theoretic perspectives, and design centralized and distributed attack detection and identification monitors. Sun *et al.* (2016) detect coordinated cyber attacks on power systems by identifying the relations among detected events. Canepa and Claudel (2013) consider the problem of detecting spoofing cyber attacks in probe-based traffic flow information systems as mixed integer linear feasibility problem, the proposed framework can be used to detect spoofing attacks in real-time, or to evaluate the worst-case effects of an attack offline.

Cyber defense uses digital tools to defend computer systems and networks from cyber attacks. There are two common ways to defend against cyber attacks: active cyber defense (ACD) and passive cyber defense (PCD).

ACD can be considered as an approach to achieve cybersecurity upon the deployment of measures to detect, analyze, identify and mitigate threats as well as the malicious actors (Dewar (2017)). ACD not only identifies and stops cyber incidents as they are occurring but also takes offensive measures to minimize attackers' capabilities. Numerous techniques and technical measures can be categorized as ACD. Dewar (2017) compares four most common techniques of ACD: white worms; hack-back; address hopping and honeypots. White worms are computer viruses deliberately deployed by a defender in its own network to identify, analyze, locate, or destroy "black" software (malware) which is deployed by attackers (Lu *et al.* (2013)). Hack-back analyzes an intrusion to identify perpetrators and technology sources responsible for a cyber attack and hacking them in return to neutralize their efforts (Heckman *et al.* (2013)). Address hopping is a defensive technique adapted from the practice of regularly changing radio frequencies in military communications. Honeypots are decoys deliberately placed in a defender's network. These decoys simulate genuine software or data in order to provide artificial targets (Spitzner (2003) and Repik (2008)).

PCD, however, is used as a "catch-all" to describe any form of cyber defense without an offensive node, including the installation of firewalls, information-sharing and the development of resilient networks. PCD aims to promote good workplace practices such as secure passwords and encryption, partnerships between actors and agencies and greater situational awareness. Two specific approaches: Fortified Cyber Defense (FCD) and Resilient Cyber Defense (RCD), are defined by Farwell and Rohozinski (2012).

FCD includes firewalls and antivirus software to set up defensive digital perimeters around key assets or potential targets (Dewar (2014)). With the development of cyber attacks, FCD requires constant maintenance and updating to ensure it can withstand the up-to-date attacks. RCD includes restorative resilience and adaptive resilience to ensure the performance and serviceability of critical infrastructures, which rely on digital networks to continue to function in the event of a cyber attack. Restorative resilience means halting a malicious intrusion and repairing its effects so that the system returns to the state before the incident took place; adaptive resilience aims to ensure that the victim system can change its status to reflect the new situation following an intrusion (Dewar (2017)). RCD not only anticipates the occurrence of cyber attacks and ensures the functional continuity of systems, but also identifies system potential weaknesses to guide maintenance during the design stage. Specifically, one of the simplest and most cost-effective methods is to take regular backups or copies of data and software so that systems can be restored in the event of an incident with minimal loss of data. Similarly, installation of redundant systems to set up a secondary network improves cyber resilience since once the primary network is attacked, the secondary system can be brought into operation.

### 5.1.2 Cyber Recovery

When systems fail to defend the cyber attacks, recovery becomes a critical task. RCD prevents the system from being further damaged and repairs the attacked part. A threat

model is adopted for cyber resiliency assessment by Bodeau and Graubart (2011). Brand *et al.* (2011) conceptually present a threat to cyber resilience which can be used in a variety of scenarios. Vugrin and Turgeon (2014) describe a hybrid infrastructure resilience assessment approach that combines qualitative analysis techniques with performance-based metrics. Choudhury *et al.* (2015) recommend general actions for cyber resilience improvements. Moyer *et al.* (2016) analyze data provenance, which is a critical technology in building resilient systems that allow systems to recover from attackers that manage to overcome the "hard-shell" defenses. Recovery methods in different domains vary. Nationally, Linkov *et al.* (2013) develop and organize effective resilience metrics for cyber systems, which link national policy goals to specific system measures, e.g., resource allocation decisions can be translated into actionable interventions and investments. In the commercial field, Khan and Estay (2015) identify whether current models can incorporate the dimension of cyber-risk and cyber resilience in supply chain and create a research agenda for supply chain cyber resilience. Similarly, Urciuoli (2015) provides strategies to improve the cyber resilience of supply chains. Jensen (2015) examines the specific characteristics of the maritime industry in relation to cyber resilience. Tran *et al.* (2016) present the implementation of dynamic Cyber Resilience Recovery Model (CRRM) to combat a zero-day outbreak within a closed network and minimize disruptions of cyber attacks to business operations. In infrastructure systems, Choudhury *et al.* (2015) present a unifying graph-based model to represent the infrastructure, behavior and missions of an enterprise to simulate resilient cyber systems. Arghandeh *et al.* (2016) not only generalize cyber-

physical resilience concepts to power systems vocabulary but also propose a new way of thinking about grid operation with unexpected extreme disturbances, hazards and leveraging distributed energy resources. Khalid and Peng (2016) propose a Bayesian algorithm to enhance the resilience of wide area measurement system (WAMS) applications against cyber attacks.

Specifically, suggestions on improving the resilience of industrial control systems (Chaves *et al.* (2017)), critical infrastructures (Bologna *et al.* (2015)), power grid systems (Ashok *et al.* (2017)) and communication networks (Sterbenz *et al.* (2010)) are provided. More studies on design and improvement of system resilience under cyber attack are discussed in Moyer *et al.* (2016), Musman (2016), Choras *et al.* (2015), Smith *et al.* (2011), Krotofil and Cárdenas (2013), Collier and Linkov (2014), Carvalho *et al.* (2013) and Liu *et al.* (2016c).

## 5.2 Proposed Resilience and IM Application in Non-repairable Cyber Network

Cyber networks are a common place in many areas such as telecommunication networks, power grids, transportation systems, healthcare delivery systems, information technology, financial systems and supply chain systems. The failure process may cascade through the nodes of the system like a ripple on a pond and continues until substantially all of the nodes in the system are compromised and the system interrupted becomes functionally disconnected from the source of its load. The

increasing reliance on cyber infrastructure has promoted cyber resilience to the forefront of consideration by network designers and users.

For example, an increasing demand for reliable energy and numerous technological advancements have motivated the development of the smart electric grid and increasingly conveyed to power systems considerable economic benefits and reliability improvements (Mamo *et al.* (2009)). Smart grid initiatives are becoming achievable through the use of information infrastructures that feature peer-to-peer communication, monitoring, protection and automated control (McGranaghan *et al.* (2008)). Smart grid expands the current capabilities of the grid's generation, transmission, and distribution systems to provide an infrastructure capable of handling future requirements for distributed generation, renewable energy sources, electric vehicles, and the demand-side management of electricity (Sridhar *et al.* (2012)). Moreover, from the economic viewpoint, the smart grid technologies enable the grid to operate with lower marginal limits and utilize the resources more efficiently because more precise and trustful data on the state of the power system is achievable (Kirschen and Bouffard (2009)). Most significantly, from the reliability perspective is the capability of self-healing, which can recognize and isolate the faulted domain, reenergize the nonfaulty part automatically, and reduce the outage time (Tram (2008)). Figure 5.1 presents an overview of a typical smart grid, which includes power plants, power transmission grid, power distribution grid, control center, and power consumers (Li *et al.* (2012)).

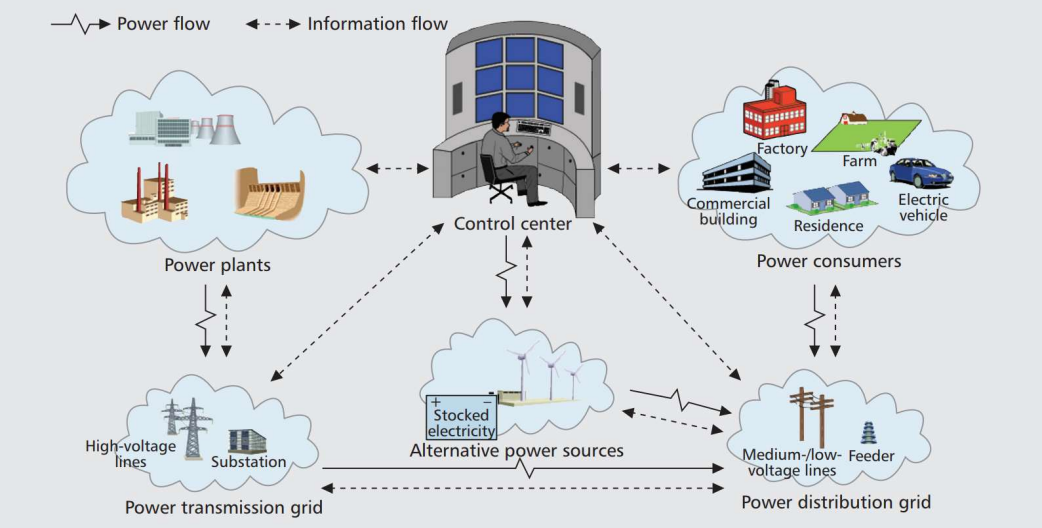



**Figure 5.1** An overall view of the typical smart grid (Li *et al.* (2012)).

However, an increasing and sophisticated implementation of cyber units in the smart grid is introducing a higher risk of failure. For example, a cyber attack caused a severe blackout in Ukraine through a computer malware called BlackEnergy, as the result, 80,000 customers were deprived of power for more than six hours (Case (2016)). Both manmade hazards such as the Ukraine outage and natural hazards mentioned in chapter 1 and Chapter 2 lead to major failures of the smart grid, which presents unique challenges in the modeling of more resilient cyber networks. Moreover, failures of cyber units are more difficult to trace than those in electrical power units. Certain types of failures in cyber units are hidden and appear only when a mal-operation occurs in the cyber power system (Falahati *et al.* (2012)). Therefore, new requirements are imposed on the design of such networks. For example, the U.S. Department of Energy has identified seven properties required for the smart grid to meet future demands, which include attack resistance, self-healing, consumer motivation, power quality,

generation and storage accommodation, enabling markets, and asset optimization (National Energy Technology Laboratory (2007)). Moreover, Gupta *et al.* (2014) propose a probabilistic framework of smart grid power network with statistical decision theory to evaluate system performance in steady state as well as under dynamical case and identify the probable critical links which can cause cascading failure. Next generation smart grid demands real-time multiple contingency analysis with self-healing and robust technology, which leads to various open research areas in the field of smart grid resilience of cascade failure.

The proposed quantifications can effectively assess the resilience of a smart grid including cascading failures and help improve its resilience. They are applicable to other networks. In this chapter, we present a simplified smart grid network shown in Figure 5.2 (simplified version of Figure 5.1) to demonstrate the proposed quantifications. We assume that there are three subnetworks (a), (b) and (c) within this smart grid network, which has a total of thirteen nodes experiencing dependent failures, such as power plants, control center, power distribution grid, transmission grid and consumers. They have binary states (working or failed), and the power flow (or information flow) of each subnetwork is shown by the arrows in Figure 5.2. In the following section, we use "$si$" to represent the subnetwork $i$ in smart grid cyber network.

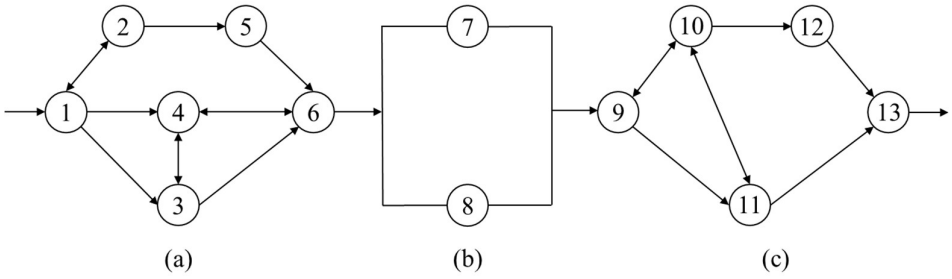



**Figure 5.2** Three subnetworks in simplified smart grid cyber network.

### 5.2.1 Nodes' Weights in Cyber Network

Cyber networks achieve certain specified functions by software and hardware working together through a specific logic or structure, which leads to the diversity of sources of compromise of the cyber network and the differences of compromise rates. In general, the sources of compromise of cyber network are (1) network structure; (2) hardware of the nodes and links in the network; (3) operating system (OS) of the network nodes; (4) the application being used in the node and; (5) data integrity stored at the nodes. Network structure usually shows the configuration and links between the network nodes; hardware is the physical unit such as computers and accessories as well as the physical links between nodes; OS is the operating system of the hardware associated with the node such as Microsoft Windows, macOS and Linux; the application (app) is a computer program designed to perform a group of coordinated functions, tasks, or activities associated with node; data refers to the information stored by the user or devices.

Therefore, for a more comprehensive consideration of the importance of nodes, we assign weights to the nodes in Eq. (5.1) from two sources: (a) network structure which is a function of the number of links associated with the node and (b) the integrity, availability and importance of the data in the nodes. The total weight is

$$\mathbf{w} = \mathbf{w}_A + \mathbf{w}_D \tag{5.1}$$

where $\mathbf{w}$ is the weight vector of the nodes , which consists of $(w_1,...,w_n)$, $w_i$ is the final weight of node $i$, $n$ is the total number of nodes; $\mathbf{w}_A$ (where $A$ means adjacency matrix of the cyber network) is the vector normalizing the number of links to each node, which consists of $(w_{A1},...,w_{An})$, $\sum_{i=1}^{n} w_{Ai} = 1$. It is based on the adjacency matrix ( $A$ ) of the network. For example, the adjacency matrix $A^{sa}$ of the subnetwork (a) is obtained in Eq. (5.2)

$$A^{sa} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \tag{5.2}$$

Therefore, $\mathbf{w}_A$ of subnetwork (a) can be calculated from $A^{sa}$ and normalized as given in Eq. (5.3)

$$\mathbf{w}_A^{sa} = \left( \frac{3}{10} \quad \frac{2}{10} \quad \frac{2}{10} \quad \frac{2}{10} \quad \frac{1}{10} \quad 0 \right) \tag{5.3}$$

$\mathbf{w}_D$ is the weight vector corresponding to the data integrity and availability (obtained from the engineers' experience), which consists of $(w_{D1},...,w_{Dn})$, $\sum_{i=1}^{n} w_{Di} = 1$;

Similar to component failure rate, we assume hardware compromise rate of node $i$ is $\lambda_{Hi}$; OS compromise rate of node $i$ is $\lambda_{OSi}$; application compromise rate of node $i$ is $\lambda_{Appi}$. The overall compromise rate of node $i$ can be obtained from other three sources and may be expressed as given in Eq. (5.4)

$$\lambda_i = \lambda_{Hi} + \lambda_{OSi} + \lambda_{Appi} \tag{5.4}$$

5.2.2 Application of the Proposed Resilience Quantification and Assessment

As stated earlier in section 3.2, we consider the reliability $R(t)$ of non-repairable cyber network as the performance function $P(t)$. The subnetworks of smart grid network and their nodes can be in either of two states, working or failed as denoted by 1 or 0, respectively. The state of the subnetwork depends only on the state of its nodes. We use the tie-set approach to determine the reliability of the subnetwork. For example, the minimum tie-sets of the subnetwork (a) are

$$T_1^{sa} = 1 \to 2 \to 5 \to 6$$

$$T_2^{sa} = 1 \to 4 \to 6$$

$$T_3^{sa} = 1 \to 3 \to 6$$

Subnetwork (a) can be considered that there are three subnetworks $T_1^{sa}$, $T_2^{sa}$ and $T_3^{sa}$ in parallel and subnetwork (a) functions properly when no more than two of them fail. Therefore, there are six cases (failure sequences) may cause the failure of subnetwork (a):

(i) $T_1^{sa} \to T_2^{sa} \to T_3^{sa}$

(ii) $T_1^{sa} \to T_3^{sa} \to T_2^{sa}$

(iii) $T_2^{sa} \to T_1^{sa} \to T_3^{sa}$

(iv) $T_2^{sa} \to T_3^{sa} \to T_1^{sa}$

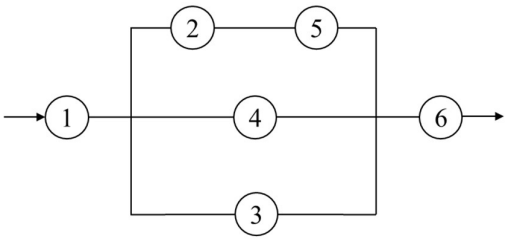
(v) $T_3^{sa} \to T_1^{sa} \to T_2^{sa}$

(vi) $T_3^{sa} \to T_2^{sa} \to T_1^{sa}$

The overall reliability of subnetwork (a) can be obtained in Eq. (5.5).

$$\begin{aligned} R_{sa} &= R_{sa}(\mathrm{i} \vee \mathrm{ii} \vee \mathrm{iii} \vee \mathrm{iv} \vee \mathrm{v} \vee \mathrm{vi}) \\ &= \sum_{i=\mathrm{i}}^{\mathrm{vi}} R_{sa}^{i} - \sum_{i=\mathrm{i}}^{\mathrm{v}} \sum_{j=i+\mathrm{i}}^{\mathrm{vi}} R_{sa}^{i} R_{sa}^{j} + \sum_{i=\mathrm{i}}^{\mathrm{iv}} \sum_{j=i+\mathrm{i}}^{\mathrm{v}} \sum_{k=j+\mathrm{i}}^{\mathrm{vi}} R_{sa}^{i} R_{sa}^{j} R_{sa}^{k} \\ &\quad - \sum_{i=\mathrm{1}}^{\mathrm{iii}} \sum_{j=i+\mathrm{i}}^{\mathrm{iv}} \sum_{k=j+\mathrm{i}}^{\mathrm{v}} \sum_{l=k+\mathrm{i}}^{\mathrm{vi}} R_{sa}^{i} R_{sa}^{j} R_{sa}^{k} R_{sa}^{l} \\ &\quad + \sum_{i=\mathrm{1}}^{\mathrm{ii}} \sum_{j=i+\mathrm{i}}^{\mathrm{iii}} \sum_{k=j+\mathrm{i}}^{\mathrm{iv}} \sum_{l=k+\mathrm{i}}^{\mathrm{v}} \sum_{m=l+\mathrm{i}}^{\mathrm{vi}} R_{sa}^{i} R_{sa}^{j} R_{sa}^{k} R_{sa}^{l} R_{sa}^{m} \\ &\quad - R_{sa}^{\mathrm{i}} R_{sa}^{\mathrm{ii}} R_{sa}^{\mathrm{iii}} R_{sa}^{\mathrm{iv}} R_{sa}^{\mathrm{v}} R_{sa}^{\mathrm{vi}} \end{aligned} \tag{5.5}$$

where $\vee$ is the OR Boolean. Since all failure sequences have same input node 1 and output node 6, we can simplify the three subnetworks based on minimum tie-sets of subnetwork (a) as shown in Figure 5.3.




(a)

**Figure 5.3** Simplified subnetwork (a).

We further assume that the overall compromise rate of node $i$ ($i = 2,\ 3,\ 4,\ 5$) of subnetwork (a) depends on following

1) $\lambda_{3i}$ when all subnetworks of subnetwork (a) are working properly;

2) $\lambda_{2i}$ when two subnetworks of subnetwork (a) are working properly and

3) $\lambda_{1i}$ when only one subnetwork of subnetwork (a) is working properly.

Then we use "*jdf*" mentioned in section 2.4 to obtain the conditional reliability of this subnetwork (a). For case (i) (in addition to node 1 and node 6), let $t_1$ be the time of first failure and $g_1(t_1)$ be the density function for the first failure. The time of the second failure is $t_2$ and its dependent density function, $g_2(t_2 \mid t_1)$, holds for $t_1 < t_2$. Then the third failure which causes the failure of subnetwork (a) occurs at time $t$ and

its dependent density function is $g_3(t \mid t_2)$ $(t_1 < t_2 < t)$.

In other words, we can expressed each density function in Eqs. (5.6)-(5.8)

$$g_1(t_1) = (\lambda_{32} + \lambda_{35}) \cdot e^{-(\lambda_{32}+\lambda_{35})t_1} \tag{5.6}$$

$$g_2(t_2 \mid t_1) = \lambda_{24} \cdot e^{-\lambda_{24}(t_2 - t_1)} \tag{5.7}$$

$$g_3(t \mid t_2) = \lambda_{13} \cdot e^{-\lambda_{13}(t - t_2)} \tag{5.8}$$

The *pdf* $\phi\ (t_1,\ t_2,\ t)$ can be expressed in Eq. (5.9).

$$\phi\ (t_1,\ t_2,\ t) = g_1(t_1) \cdot g_2(t_2 \mid t_1) \cdot g_3(t \mid t_2) \tag{5.9}$$

The marginal density function of the third failure, $f(t)$, can be obtained in Eq. (5.10)

$$f(t) = \int_0^\infty \int_{t_1}^\infty \phi(t_1,\ t_2,\ t)\ dt_2 dt_1 \tag{5.10}$$

The reliability of subnetwork (a) in case (i) is governed by the marginal density function $f(t)$, reliability of node 1 and reliability of node 6, which is obtained as given in Eq. (5.11)

$$R_{sa}^{i}(t) = R_{sa1}(t) \cdot R_{sa6}(t) \cdot (1 - \int_0^t f(\zeta)\, d\zeta) \tag{5.11}$$

where $R_{sa1}(t) = e^{-\lambda_1 t}$ is the reliability of node 1 and $\lambda_1$ is the overall compromise rate of node 1; $R_{sa6}(t) = e^{-\lambda_6 t}$ is the reliability of node 6 and $\lambda_6$ is the overall compromise rate of node 6.

Specifically, we assume that $\lambda_1 = 0.05$, $\lambda_6 = 0.07$, and the overall compromise rates of nodes (2, 3, 4, 5) in subnetwork (a) as shown in Table 5.1.

**Table 5.1** Overall compromise rates of the nodes (2, 3, 4, 5) in subnetwork (a).

| Node | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| $\lambda_{3i}$ | 0.0009 | 0.0007 | 0.0008 | 0.0005 |
| $\lambda_{2i}$ | 0.0019 | 0.0017 | 0.0018 | 0.0015 |
| $\lambda_{1i}$ | 0.0039 | 0.0037 | 0.0038 | 0.0035 |

Using Eq. (5.11), the reliability of subnetwork (a) in case (i) can be obtained in Eq. (5.12).

$$\begin{aligned} R_{sa}^{\mathrm{i}}(t) &= e^{-\lambda_1 t} \cdot e^{-\lambda_6 t} \cdot (1 - \int_0^t \int_0^\infty \int_{t_1}^\infty g_1(t_1) \cdot g_2(t_2 \mid t_1) \cdot g_3(t \mid t_2)\, dt_2 dt_1 d\zeta) \\ &= 0.5767 e^{-0.1237 t} + 0.4233 e^{-0.12 t} \end{aligned} \tag{5.12}$$

Similarly, we can apply above procedure to obtain the reliability of subsystems (a) in

other cases at a given time, then obtain the overall reliability of subsystems (a) by using Eq. (5.5). In order to illustrate the proposed resilience quantification, we compare the reliability and resilience of two subnetworks ((a) and (b)) with different nodes' compromise rates. Specifically, we assume that the overall compromise rates of nodes in subnetwork (b) as shown in Table 5.2.

**Table 5.2** Overall compromise rate of the nodes in subnetwork (b).

| Node | 7 | 8 |
|---|---|---|
| $\lambda_{bi}$ | 0.1 | 0.2 |
| $\lambda_{si}$ | 0.4 | 0.6 |

where $\lambda_{bi}$ is the compromise rate of node $i$ when both nodes operate simultaneously; and $\lambda_{si}$ is the compromise rate of node $i$ when they operate singularly. Assuming that the hazard occurs at $t_h = 10$, we obtain the reliability and resilience using Eq. (5.13) for the two subnetworks as shown in Figures 5.4 and 5.5 and Table 5.3.

$$\Re(t_d) = \frac{(t_d - t_h)}{2t_d}\left[P(t_h) + P(t_d)\right] = \frac{(t_d - 10)}{2t_d}\left[R(10) + R(t_d)\right] \tag{5.13}$$

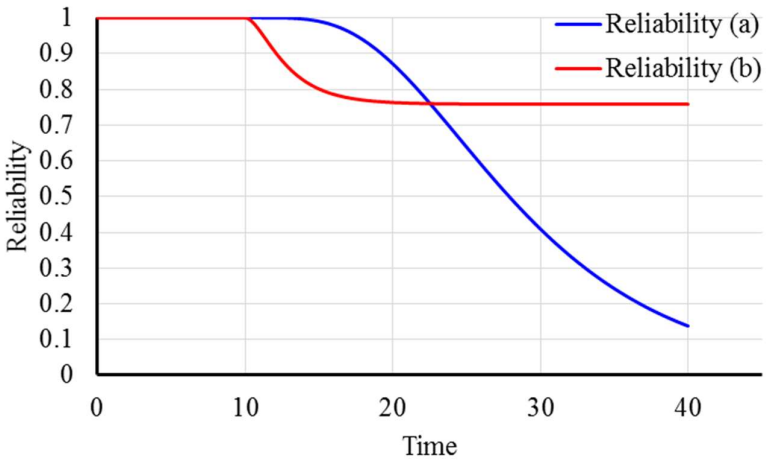



**Figure 5.4** Reliability of the two subnetworks over time.

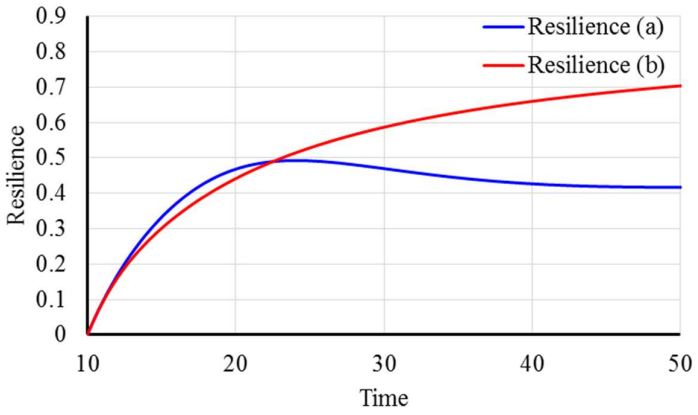



**Figure 5.5** Resilience of the two subnetworks over time.

**Table 5.3** Resilience and reliability of the two subnetworks over time.

| Time | Reliability (a) | Resilience (a) | Reliability (b) | Resilience (b) |
|---|---|---|---|---|
| 0 | 1.0000 | - | 1.0000 | - |
| 5 | 1.0000 | - | 1.0000 | - |
| 10 | 1.0000 | - | 1.0000 | - |
| 15 | 0.9903 | 0.3317 | 0.8028 | 0.3005 |
| 20 | 0.8717 | 0.4679 | 0.7650 | 0.4412 |
| 25 | 0.6385 | 0.4916 | 0.7606 | 0.5282 |
| 30 | 0.4091 | 0.4697 | 0.7601 | 0.5867 |
| 35 | 0.2423 | 0.4437 | 0.7600 | 0.6286 |
| 40 | 0.1373 | 0.4265 | 0.7600 | 0.6600 |
| 45 | 0.0760 | 0.4184 | 0.7600 | 0.6844 |
| 50 | 0.0415 | 0.4166 | 0.7600 | 0.7040 |

5.2.3 Applications of the Proposed IM in Subnetwork (a)

As stated in section 4.2, we compare the results of non-weighted and weighted BIM in subnetwork (a) to show that the weighted IM is more effective. In cyber networks, we obtain the weight of data from the engineers' experience and the weight of network structure from adjacency matrix. Therefore, referring to the weights derived from network structure in Eq. (5.3), we assume the final weights of the six nodes in subnetwork (a) in Eq. (5.14) as:

$$\mathbf{w}_{sa} = (0.4 \quad 0.25 \quad 0.3 \quad 0.4 \quad 0.2 \quad 0.45) \tag{5.14}$$

BIM defines the importance of node $i$ is the difference of the unavailability of the system when component $i$ is not working and the unavailability of the system when component $i$ is working. Therefore, for weighted BIM, we apply Eq. (4.9) and Eq.

(5.14) to obtain the importance of each node in subnetwork (a). Similarly, we obtain the importance of each node by using BIM in Eq. (4.1). Considering the time period $(10,100)$, the variation trends of the importance values of each node compared by the two different importance measures are shown in Figure 5.6. We extract the following time points to illustrate the details as shown in Table 5.4 and Table 5.5.

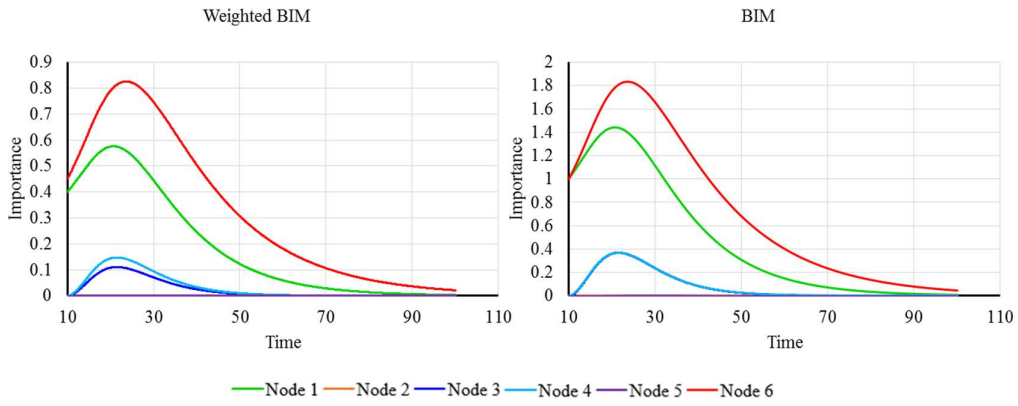



**Figure 5.6** Importance of nodes by weighted BIM and BIM in subnetwork (a) over time.

**Table 5.4** Importance of nodes by weighted BIM in subnetwork (a) over time.

| Time | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 10 | 0.400000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.450000 |
| 20 | 0.574881 | 0.000169 | 0.108011 | 0.144015 | 0.000135 | 0.789931 |
| 30 | 0.444868 | 0.000368 | 0.070782 | 0.094376 | 0.000294 | 0.746623 |
| 40 | 0.246196 | 0.000227 | 0.025030 | 0.033374 | 0.000182 | 0.504673 |
| 50 | 0.122750 | 0.000098 | 0.007542 | 0.010056 | 0.000079 | 0.307333 |
| 60 | 0.059360 | 0.000037 | 0.002169 | 0.002892 | 0.000030 | 0.181526 |
| 70 | 0.028451 | 0.000013 | 0.000615 | 0.000819 | 0.000011 | 0.106269 |
| 80 | 0.013602 | 0.000005 | 0.000173 | 0.000231 | 0.000004 | 0.062051 |
| 90 | 0.006497 | 0.000002 | 0.000049 | 0.000065 | 0.000001 | 0.036204 |
| 100 | 0.003103 | 0.000001 | 0.000014 | 0.000018 | 0.000000 | 0.021118 |

**Table 5.5** Importance of nodes by BIM in subnetwork (a) over time.

| Time | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 10 | 1.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 1.000000 |
| 20 | 1.437201 | 0.000675 | 0.360037 | 0.360037 | 0.000675 | 1.755402 |
| 30 | 1.112170 | 0.001471 | 0.235939 | 0.235939 | 0.001471 | 1.659163 |
| 40 | 0.615490 | 0.000908 | 0.083434 | 0.083434 | 0.000908 | 1.121495 |
| 50 | 0.306875 | 0.000393 | 0.025140 | 0.025140 | 0.000393 | 0.682963 |
| 60 | 0.148399 | 0.000149 | 0.007230 | 0.007230 | 0.000149 | 0.403390 |
| 70 | 0.071128 | 0.000053 | 0.002049 | 0.002049 | 0.000053 | 0.236154 |
| 80 | 0.034004 | 0.000018 | 0.000577 | 0.000577 | 0.000018 | 0.137892 |
| 90 | 0.016243 | 0.000006 | 0.000162 | 0.000162 | 0.000006 | 0.080453 |
| 100 | 0.007757 | 0.000002 | 0.000045 | 0.000045 | 0.000002 | 0.046929 |

### 5.3 Proposed Resilience and IM for Repairable Cyber Network

Without loss of generality, we may consider repairable cyber network instantaneous availability $A(t)$ as the performance function $P(t)$. As stated earlier in section 3.3, the system availability is a three-stages piece-wise function of time in repairable system. In stage (1), we assume that repairable smart grid cyber network maintains the steady-state availability $A(t_0)=1$ until the occurrence of hazard at time $t_h$; In stage (2), assuming that the all nodes experience same dependent failures as in section 5.2; Stage (3) starts when the availabilities of two subnetworks deteriorate to the unacceptable levels. Assuming the repair-time distribution of each node follows a geometric Brownian motion and two subnetworks have "mean repair rate" $\mu_i$ and "mean diffusion coefficients" $\sigma_i$ of subnetwork $i$ as shown in Table 5.6.

**Table 5.6** Mean repair rates and mean diffusion coefficients of two subnetworks.

| Subnetwork | (a) | (b) |
|---|---|---|
| $\mu_i$ | 0.005 | 0.007 |
| $\sigma_i$ | 0.01 | 0.02 |

The resilience of the subnetwork is obtained using Eq. (5.15). Figure 5.7, Figure 5.8 and Table 5.7 show the availability and resilience of two subnetworks when the hazard occurs at time $t_h = 10$ until deteriorating their availabilities to the unacceptable level 0.63 and 0.76 at time $t_d = 25$, then repair starts. The resilience is assessed at different values of $t_r$.

$$\Re(t_r) = \frac{P(t_r) - P(t_d)}{P(t_h) - P(t_d)} \cdot \frac{t_d - t_h}{t_r - t_h} = \frac{A(t_r) - A(25)}{A(10) - A(25)} \cdot \frac{(25-10)}{(t_r - 10)} \tag{5.15}$$

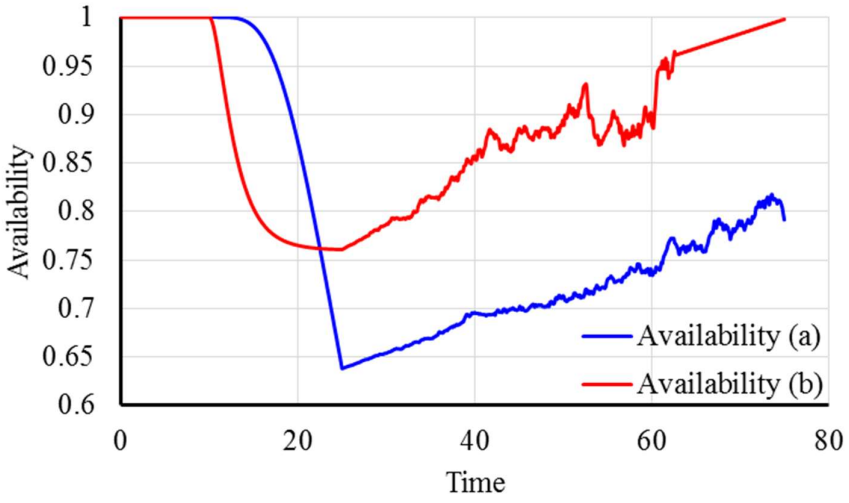



**Figure 5.7** Availability of the two subnetworks over time.

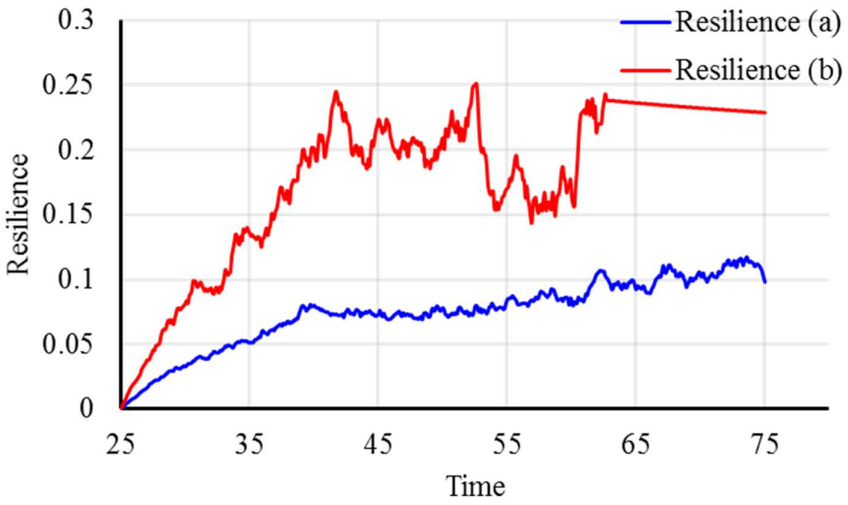



**Figure 5.8** Resilience of the two subnetworks over time.

**Table 5.7** Availability and resilience of the two subnetworks over time.

| Time | Availability (a) | Resilience (a) | Availability (b) | Resilience (b) |
|---|---|---|---|---|
| 0 | 1.00000 | - | 1.00000 | - |
| 25 | 0.63854 | - | 0.76062 | - |
| 30 | 0.65412 | 0.03232 | 0.78660 | 0.08139 |
| 35 | 0.66909 | 0.05071 | 0.81464 | 0.13539 |
| 40 | 0.69618 | 0.07973 | 0.85699 | 0.20128 |
| 45 | 0.69994 | 0.07280 | 0.88542 | 0.22342 |
| 50 | 0.71341 | 0.07767 | 0.89404 | 0.20900 |
| 55 | 0.72999 | 0.08434 | 0.88292 | 0.17030 |
| 60 | 0.73762 | 0.08223 | 0.89065 | 0.16295 |
| 65 | 0.76028 | 0.09185 | 0.96787 | 0.23612 |
| 70 | 0.78648 | 0.10232 | 0.98287 | 0.23211 |
| 75 | 0.79149 | 0.09765 | 0.99787 | 0.22872 |

### 5.3.1 Application of the Proposed IM in Subnetwork (a)

Similar to section 5.2.3, we apply Eq. (4.13) to obtain the importance of each node in repairable smart grid cyber network. The importance of the six nodes in subnetwork (a)

from $t = 10$ to $t = 75$ are plotted in Figure 5.9 and presented in Table 5.8.

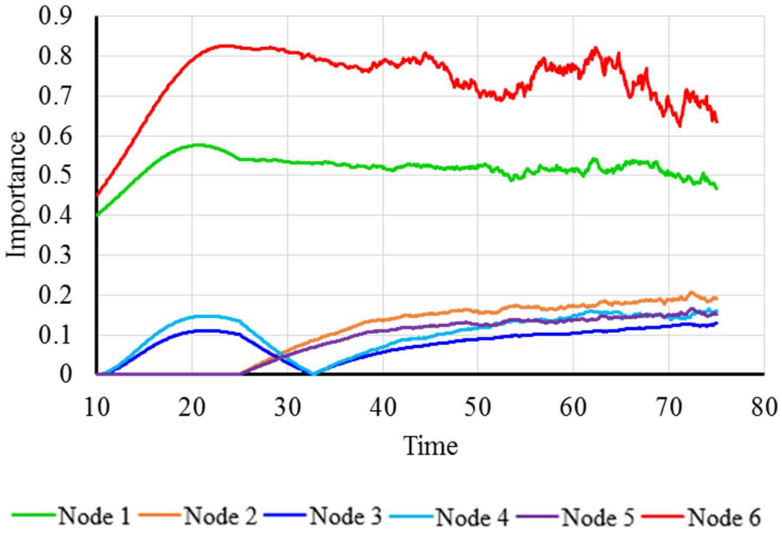



**Figure 5.9** Importance of the nodes in subnetwork (a) over time.

**Table 5.8** Importance of the nodes in subnetwork (a) over time.

| Time | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 0 | 0.00000 | 0.00000 | 0.00000 | 0.00000 | 0.00000 | 0.00000 |
| 10 | 0.400000 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.450000 |
| 15 | 0.508641 | 0.000018 | 0.058169 | 0.077559 | 0.000014 | 0.632402 |
| 20 | 0.574881 | 0.000169 | 0.108011 | 0.144015 | 0.000135 | 0.789931 |
| 25 | 0.540716 | 0.000332 | 0.100580 | 0.134107 | 0.000266 | 0.821126 |
| 30 | 0.533857 | 0.059838 | 0.030229 | 0.041109 | 0.047870 | 0.811614 |
| 35 | 0.529720 | 0.102895 | 0.023023 | 0.026349 | 0.082316 | 0.779497 |
| 40 | 0.522041 | 0.136367 | 0.056279 | 0.069306 | 0.109093 | 0.784610 |
| 45 | 0.523495 | 0.153810 | 0.075325 | 0.095616 | 0.123048 | 0.793224 |
| 50 | 0.525715 | 0.157110 | 0.089145 | 0.116801 | 0.125688 | 0.709168 |
| 55 | 0.509196 | 0.168232 | 0.098138 | 0.133932 | 0.134585 | 0.711907 |
| 60 | 0.510947 | 0.173509 | 0.103965 | 0.148847 | 0.138807 | 0.778491 |
| 65 | 0.513981 | 0.178155 | 0.112268 | 0.153979 | 0.142524 | 0.759140 |
| 70 | 0.504038 | 0.188416 | 0.121506 | 0.142995 | 0.150733 | 0.683279 |
| 75 | 0.466947 | 0.191066 | 0.128325 | 0.159930 | 0.152853 | 0.636277 |

## 5.4 Summary and Conclusions

Cyber networks are common place in many areas such as telecommunication networks, power grids, transportation systems, healthcare delivery systems, information technology, financial systems and supply chain systems. The failures of such systems may result in cascading effects and significant damages and interruptions of its services. The increasing reliance on cyber infrastructure has promoted cyber resilience to the forefront of consideration by network designers and users. In this chapter, we present a detailed overview of the cyber resilience, specifically, cyber robustness and cyber recovery. We then illustrate the assessment of the resilience and the use of proposed importance measures. Moreover, due to the different sources of compromising to cyber networks, we assign additional weights to the nodes for each possible compromised source in order to determine the importance of the nodes. In non-repairable smart grid cyber network, we consider reliability $R(t)$ as the performance function $P(t)$ and obtain the resilience of the network; by comparing the non-weighted BIM and weighted BIM, we show that the latter can effectively distinguish the importance of nodes with time. For repairable smart grid cyber network, we consider availability $A(t)$ as the performance function $P(t)$. By assuming system availability is a three-stages piece-wise function of time, the change of availability of the network can be obtained separately using different methods, where stage (1) provides steady-state availability; stage (2) shows decreasing availability by inducing dependent failures among all nodes; stage (3) increases the availability by considering the recovery as geometric Brownian motion repair process. Finally, the importance of each node in the network is obtained during each stage.

# CHAPTER 6

# SUMMARY AND FUTURE RESEARCH

## 6.1 Summary

The continuous improvements in systems engineering and the unprecedented rate of technological advances, systems have become larger and more complex. During the recent decades, there has been significant development of complex engineered systems such as telecommunication networks, power grids, transportation systems, healthcare delivery systems, information technology, financial systems and supply chain systems. Such systems are intrinsically difficult to be modeled not only due to its substantial number of subsystems and components but also the dependencies, relationships, or interactions among them under given working environment. Therefore, failures of such systems may result in significant cascading effects and more significant damages and interruptions of its services with longer times. Full or partial restorations of its functions under limited resources and time constraints is a challenging engineering task, which has given rise to the assessment of such systems' resilience.

In chapter 2, we present the overall system's failure rate in an additive form by integrating the occurrence frequency and severity of the different types of hazards; where all the failure rates are assumed to be constant. We then review current studies on natural and manmade hazard prediction and assessment, as well as the studies on

system performance modeling, improvement and other related topics. Moreover, the natural and manmade hazard induce severe damage under some circumstance, and the traditional reliability (availability) metrics are limited in measuring the severity of system damage upon failure and system ability to recover (the rate of repair) to a specific performance level. Therefore, we extend the system reliability metrics to system resilience. We introduce the basic concept of resilience as a mechanical property of materials and review current literature on resilience definitions. Since the resilience of repairable systems is a function of its recovery ability after the hazard occurrence, methodologies are required to recover the system to the desired performance level in a relatively short time. Specifically, only partial recovery can be achieved at a time when the repair resources and time are limited, and identifying the repair priorities of the system's components becomes critical. Furthermore, the optimal repair sequence of the components can be achieved by estimating importance measure (IM) of the components in terms of their impact on the system's recovery level. We then present a thorough review of literature of the importance measures. Specifically, importance measures are developed from binary systems to multi-state systems, from discrete-state systems to continuous-state systems and from non-repairable systems to repairable systems. However, the applications of importance measures are limited to specific scenarios. Most of large complex systems include cascading failures may lead to the failure of the entire system due to a minor failure. Finally, we discuss the cascading failures in different type of systems and corresponding methods of their mitigation or avoidance in order to improve the system's resilience.

In chapter 3, we provide a detailed literature review of resilience quantifications and conclude that most of the current quantifications of resilience either fails to accurately assess system recovery ability or system design robustness. Therefore, in non-repairable systems and repairable systems, we separately recommend a general quantification of system resilience, taking the system robustness and system recovery ability into consideration. Two proposed resilience quantifications are applicable when the system is subjected to multi hazard, but acceptance and unification of the resilience definition and quantification across disciplines require interdisciplinary interactions and research collaborations. There are many system performance indicators, reliability and availability are only two of them.

In chapter 4, we present a detailed overview of the quantifications of IM for non-repairable systems and repairable systems. In non-repairable systems, BIM and its extended IMs have been studied and widely applied. However, some of these IMs still do not adequately and effectively distinguish the importance of components in some scenarios. Therefore, in order to more comprehensively consider the importance of components in the system before applying the current IMs, we assign additional weights to components regarding their importance, availability, and integrity of data, specific system structure, and special scenario. Unlike non-repairable systems, IMs of components for repairable systems need to consider components' repair ability and system availability. To adapt to the more general situation, the weighted IM applying availability to the components and systems for repairable systems is proposed.

In chapter 5, we describe the importance of the cyber networks and review current studies on cyber resilience, specifically, cyber robustness and cyber recovery. In addition, we take a smart grid cyber network as an example of large and complex systems to validate the effectiveness of proposed resilience quantifications and IMs. Furthermore, we assign additional weights to the nodes regarding network structure and data integrity stored at the nodes, to help be more comprehensive and effective in determining the importance of nodes. The results show that the proposed methods are valid in non-repairable and repairable smart grid cyber network, which can help improve the resilience of the systems.

## 6.2 Future Research

The proposed methods have some limitations which require further investigation. In chapter 2, we propose an additive form of the multi hazard by taking the occurrence frequency and severity of all potential types of hazards into consideration to obtain the overall system's failure rate; where all the failure rates are assumed to be constant. However, under most circumstances, system normal failure rate is time-dependent (such as Weibull and Lognormal). Likewise, the factors that affect the natural and manmade hazards vary dynamically and randomly and the proposed system failure rate needs to be modified accordingly.

Furthermore, the proposed resilience quantifications are limited in assessing the single

system (subsystem). In general, we can obtain the reliability of the overall system by multiplying the reliability of its subsystems. We intend to seek similar conclusions for system resilience. Moreover, system and its subsystems or components usually have multiple degradation states, which are necessary to be investigated.

In chapter 4, the proposed IMs to determine the importance of nodes are limited in determining the importance of the nodes in the minimal tie-sets of the system. For example, we can obtain the minimum tie-sets of the following network as shown in Figure 6:

$$T_1 = 1 \to 3 \to 5 \to 9$$

$$T_2 = 1 \to 3 \to 7 \to 8 \to 9$$

$$T_3 = 1 \to 4 \to 7 \to 8 \to 9$$

By applying the proposed IM to this network, we cannot distinguish the importance of node 2 and node 6 among others. The importance values of node 2 and node 6 are zero at all the times since they are not in the minimal tie-sets. However, node 2 and node 6 also have a certain degree of importance to this network in real life, which causes some obstacles to comprehensively assess and rank the nodes. In the future work, we investigate these shortcomings and modify and optimize these measures.

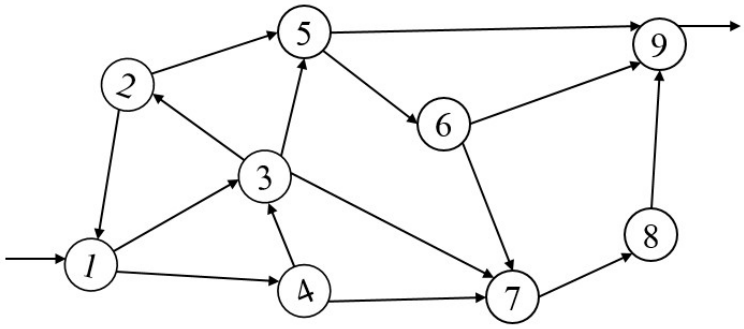



**Figure 6** Network example.

# REFERENCE


Adams, T. M., Bekkem, K. R. & Toledo-Durán, E. J. 2012. Freight resilience measures. *Journal of Transportation Engineering,* 138**,** 1403-1409.

Adibi, M., Clelland, P., Fink, L., Happ, H., Kafka, R., Raine, J., Scheurer, D. & Trefny, F. 1987. Power system restoration-a task force report. *IEEE Transactions on Power Systems,* 2**,** 271-277.

Adjetey-Bahun, K., Birregah, B., Châtelet, E., Planchet, J.-L. & Laurens-Fonseca, E. A simulation-based approach to quantifying resilience indicators in a mass transportation system. ISCRAM, 2014.

Ahmed, S. H., Kim, G. & Kim, D. Cyber Physical System: Architecture, applications and research challenges. Wireless Days (WD), 2013 IFIP, 2013. IEEE, 1-5.

Albert, R. 2002. R. Albert and A.-L. Barabási, Rev. Mod. Phys. 74, 47 (2002). *Rev. Mod. Phys.,* 74**,** 47.

Alexander, D. E. 1993. *Natural disasters*, Springer Science & Business Media.

Aliee, H., Borgonovo, E., Glaß, M. & Teich, J. 2017. On the Boolean extension of the Birnbaum importance to non-coherent systems. *Reliability Engineering & System Safety,* 160**,** 191-200.

Alos-Moya, J., Paya-Zaforteza, I., Garlock, M., Loma-Ossorio, E., Schiffner, D. & Hospitaler, A. 2014. Analysis of a bridge failure due to fire using computational fluid dynamics and finite element models. *Engineering Structures,* 68**,** 96-110.

Andrews, J. D. & Beeson, S. 2003. Birnbaum's measure of component importance for noncoherent systems. *IEEE Transactions on Reliability,* 52**,** 213-219.

Argauer, B. & Yang, S. 2008. VTAC: Virtual terrain assisted impact assessment for cyber attacks.

Arghandeh, R., von Meier, A., Mehrmanesh, L. & Mili, L. 2016. On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews,* 58**,** 1060-1069.

Armstrong, M. J. 1995. Joint reliability-importance of components. *IEEE Transactions on Reliability,* 44**,** 408-412.

Armstrong, M. J. 1997. Reliability-importance and dual failure-mode components. *IEEE Transactions on Reliability,* 46**,** 212-221.

Arora, A., Nandkumar, A. & Telang, R. 2006. Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers,* 8**,** 350-362.

Artioli, E., Battaglia, R. & Tralli, A. 2017. Emilia 2012 earthquake and the need of accounting for multi-hazard design paradigm for strategic infrastructures. *Engineering Structures,* 140**,** 353-372.

Ash, J. & Newth, D. 2007. Optimizing complex networks for resilience against cascading failure. *Physica A: Statistical Mechanics and its Applications,* 380**,** 673-683.

Ashok, A., Govindarasu, M. & Wang, J. 2017. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proceedings of the IEEE*.

Asprone, D., Jalayer, F., Prota, A. & Manfredi, G. 2010. Proposal of a probabilistic model for multi-hazard risk assessment of structures in seismic zones subjected to blast

for the limit state of collapse. *Structural Safety,* 32**,** 25-34.
Attoh-Okine, N. O., Cooper, A. T. & Mensah, S. A. 2009. Formulation of resilience index of urban infrastructure using belief functions. *IEEE Systems Journal,* 3**,** 147-153.
Aven, T. 1985. Reliability/availability evaluations of coherent systems based on minimal cut sets. *Reliability Engineering,* 13**,** 93-104.
Aven, T. 1993. On performance measures for multistate monotone systems. *Reliability Engineering & System Safety,* 41**,** 259-266.
Aven, T. & Nøkland, T. 2010. On the use of uncertainty importance measures in reliability and risk analysis. *Reliability Engineering & System Safety,* 95**,** 127-133.
Ayyub, B. M. 2014. Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. *Risk Analysis,* 34**,** 340-355.
Aziz, E. & Kodur, V. 2013. An approach for evaluating the residual strength of fire exposed bridge girders. *Journal of Constructional Steel Research,* 88**,** 34-42.
Babaei, M., Ghassemieh, H. & Jalili, M. 2011. Cascading failure tolerance of modular small-world networks. *IEEE Transactions on Circuits and Systems II: Express Briefs,* 58**,** 527-531.
Bai, Y., Burkett, W. R. & Nash, P. T. 2006. Rapid bridge replacement under emergency situation: Case study. *Journal of Bridge Engineering,* 11**,** 266-273.
Bak, P. 1987. P. Bak, C. Tang, and K. Wiesenfeld, Phys. Rev. Lett. 59, 381 (1987). *Phys. Rev. Lett.,* 59**,** 381.
Barabady, J. 2005. *Improvement of system availability using reliability and maintainability analysis.* Luleå tekniska universitet.
Barabady, J. & Kumar, U. 2007. Availability allocation through importance measures. *International journal of quality & reliability management,* 24**,** 643-657.
Barben, R. 2010. Vulnerability assessment of electric power supply under extreme weather conditions.
Barker, K., Ramirez-Marquez, J. E. & Rocco, C. M. 2013. Resilience-based network component importance measures. *Reliability Engineering & System Safety,* 117**,** 89-97.
Barlow, R. E. & Proschan, F. 1975. Importance of system components and fault tree events. *Stochastic Processes and their applications,* 3**,** 153-173.
Barlow, R. E. & Wu, A. S. 1978. Coherent systems with multi-state components. *Mathematics of operations research,* 3**,** 275-281.
Baroud, H., Barker, K. & Ramirez-Marquez, J. E. 2014. Importance measures for inland waterway network resilience. *Transportation research part E: logistics and transportation review,* 62**,** 55-67.
Bebbington, M., Cronin, S. J., Chapman, I. & Turner, M. B. 2008. Quantifying volcanic ash fall hazard to electricity infrastructure. *Journal of Volcanology and Geothermal Research,* 177**,** 1055-1062.
Bebbington, M. S. 2013. Assessing probabilistic forecasts of volcanic eruption onsets. *Bulletin of volcanology,* 75**,** 783.
Beeson, S. & Andrews, J. D. 2003. Importance measures for noncoherent-system analysis. *IEEE Transactions on Reliability,* 52**,** 301-310.
Bell, R. & Glade, T. 2011. Multi-hazard analysis in natural risk assessments. *WIT Transactions on State-of-the-art in Science and Engineering,* 53.

Bennetts, I. & Moinuddin, K. 2009. Evaluation of the impact of potential fire scenarios on structural elements of a cable-stayed bridge. *Journal of fire protection engineering,* 19**,** 85-106.
Berkeley III, A. R., Wallace, M. & COO, C. 2010. A framework for establishing critical infrastructure resilience goals.
Bhamra, R., Dani, S. & Burnard, K. 2011. Resilience: the concept, a literature review and future directions. *International Journal of Production Research,* 49**,** 5375-5393.
Bhuiyan, M. & Allan, R. 1994. Inclusion of weather effects in composite system reliability evaluation using sequential simulation. *IEE Proceedings-Generation, Transmission and Distribution,* 141**,** 575-584.
Billinton, R. & Acharya, J. Consideration of multi-state weather models in reliability evaluation of transmission and distribution systems. Electrical and Computer Engineering, 2005. Canadian Conference on, 2005. IEEE, 916-922.
Billinton, R. & Bollinger, K. E. 1968. Transmission system reliability evaluation using Markov processes. *IEEE Transactions on power apparatus and systems***,** 538-547.
Billinton, R. & Cheng, L. Incorporation of weather effects in transmission system models for composite system adequacy evaluation. IEE Proceedings C (Generation, Transmission and Distribution), 1986. IET, 319-327.
Billinton, R. & Kumar, Y. 1981. Transmission line reliability models including common mode and adverse weather effects. *IEEE Transactions on Power Apparatus and Systems***,** 3899-3910.
Billinton, R. & Singh, G. 2006. Application of adverse and extreme adverse weather: modelling in transmission and distribution system reliability evaluation. *IEE Proceedings-Generation, Transmission and Distribution,* 153**,** 115-120.
Billinton, R., Wu, C. & Singh, G. Extreme adverse weather modeling in transmission and distribution system reliability evaluation. Power Systems Computation Conf.(PSCC)-2002, Spain, 2002. 66.
Birnbaum, Z. W. 1968. On the importance of different components in a multicomponent system. Washington Univ Seattle Lab of Statistical Research.
Block, H. W. & Savits, T. H. 1982. A decomposition for multistate monotone systems. *Journal of Applied Probability,* 19**,** 391-402.
Boccaletti, S. 2006. S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Phys. Rep. 424, 175 (2006). *Phys. Rep.,* 424**,** 175.
Bocchini, P. & Frangopol, D. M. 2012. Restoration of bridge networks after an earthquake: Multicriteria intervention optimization. *Earthquake Spectra,* 28**,** 426-455.
Bodeau, D. & Graubart, R. 2011. Cyber resiliency engineering framework. *MTR110237, MITRE Corporation, September*.
Boin, A. & McConnell, A. 2007. Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management,* 15**,** 50-59.
Boland, P. J. & El-Neweihi, E. 1995. Measures of component importance in reliability theory. *Computers & operations research,* 22**,** 455-463.
Boland, P. J., Proschan, F. & Tong, Y. 1987. Optimal Arrangement of Components Via Pairwise Rearrangements. FLORIDA STATE UNIV TALLAHASSEE DEPT OF

STATISTICS.
Bologna, S., Lazari, A. & Mele, S. 2015. Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats.
Bonaiuto, M., Alves, S., De Dominicis, S. & Petruccelli, I. 2016. Place attachment and natural hazard risk: Research review and agenda. *Journal of Environmental Psychology,* 48**,** 33-53.
Borgonovo, E. 2010. The reliability importance of components and prime implicants in coherent and non-coherent systems including total-order interactions. *European Journal of Operational Research,* 204**,** 485-495.
Borgonovo, E., Aliee, H., Glaß, M. & Teich, J. 2016. A new time-independent reliability importance measure. *European Journal of Operational Research,* 254**,** 427-442.
Borgonovo, E. & Apostolakis, G. E. 2001. A new importance measure for risk-informed decision making. *Reliability Engineering & System Safety,* 72**,** 193-212.
Borgonovo, E. & Smith, C. L. 2012. Composite multilinearity, epistemic uncertainty and risk achievement worth. *European Journal of Operational Research,* 222**,** 301-311.
Brand, M., Valli, C. & Woodward, A. 2011. A threat to cyber resilience: A malware rebirthing botnet.
Brummitt, C. 2012. CD Brummitt, RM D'Souza, and EA Leicht, Proc. Natl. Acad. Sci. USA 109, E680 (2012). *Proc. Natl. Acad. Sci. USA,* 109**,** E680.
Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A. & Von Winterfeldt, D. 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake spectra,* 19**,** 733-752.
Bruneau, M. & Reinhorn, A. 2007. Exploring the concept of seismic resilience for acute care facilities. *Earthquake Spectra,* 23**,** 41-62.
Buchanan, A. H. & Abu, A. K. 2017. *Structural design for fire safety*, John Wiley & Sons.
Bueno, V. C. 1988. On the importance of components for multistate monotone systems. *Statistics & probability letters,* 7**,** 51-59.
Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. 2010. Catastrophic cascade of failures in interdependent networks. *Nature,* 464**,** 1025.
Bullock, J., Haddow, G. & Coppola, D. P. 2017. *Homeland security: the essentials*, Butterworth-Heinemann.
Burgherr, P. & Hirschberg, S. 2008. Severe accident risks in fossil energy chains: a comparative analysis. *Energy,* 33**,** 538-553.
Burton, I. 1993. *The environment as hazard*, Guilford Press.
Butler, D. A. 1977. An importance ranking for system components based upon cuts. *Operations Research,* 25**,** 874-879.
Cabinet Office 2011. Keeping the country running: Natural hazards and infrastructure.
Campanella, T. J. 2006. Urban resilience and the recovery of New Orleans. *Journal of the American Planning Association,* 72**,** 141-146.
Campbell, R. J. 2012. Weather-Related Power Outages and Electric System Resiliency. *In:* Service, C. R. (ed.). Washington, DC, USA.
Canepa, E. S. & Claudel, C. G. Spoofing cyber attack detection in probe-based traffic

monitoring systems using mixed integer linear programming. Computing, Networking and Communications (ICNC), 2013 International Conference on, 2013. IEEE, 327-333.

Carpignano, A., Golia, E., Di Mauro, C., Bouchon, S. & Nordvik, J. P. 2009. A methodological approach for the definition of multi‐risk maps at regional level: first application. *Journal of risk research,* 12**,** 513-534.

Carreras, B. A., Lynch, V. E., Newman, D. E. & Dobson, I. Blackout mitigation assessment in power transmission systems. System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on, 2003. IEEE, 10 pp.

Cartwright, G. J. 2011. Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5. *Depatment of Defense, Washington DC*.

Carvalho, M., Eskridge, T. C., Bunch, L., Dalton, A., Hoffman, R., Bradshaw, J. M., Feltovich, P. J., Kidwell, D. & Shanklin, T. MTC2: A command and control framework for moving target defense and cyber resilience. Resilient Control Systems (ISRCS), 2013 6th International Symposium on, 2013. IEEE, 175-180.

Case, D. U. 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid.

Cassady, R., A. Pohl, E. & Jin, S. 2004. Managing availability improvement efforts with importance measures and optimization. *IMA Journal of Management Mathematics,* 15**,** 161-174.

Cavelty, M. D. 2013. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review,* 15**,** 105-122.

Chadjiconstantinidis, S. & Koutras, M. V. 1999. Measures of component importance for Markov chain imbeddable reliability structures. *Naval Research Logistics (NRL),* 46**,** 613-639.

Chai, W. K., Kyritsis, V., Katsaros, K. V. & Pavlou, G. Resilience of interdependent communication and power distribution networks against cascading failures. IFIP Networking Conference (IFIP Networking) and Workshops, 2016, 2016. IEEE, 37-45.

Chang, G. J., Cui, L. & Hwang, F. K. 1999. New comparisons in Birnbaum importance for the consecutive-k-out-of-n system. *Probability in the Engineering and Informational Sciences,* 13**,** 187-192.

Chang, S. E. 2003. Evaluating disaster mitigations: Methodology for urban infrastructure systems. *Natural Hazards Review,* 4**,** 186-196.

Chang, S. E. & Shinozuka, M. 2004. Measuring improvements in the disaster resilience of communities. *Earthquake Spectra,* 20**,** 739-755.

Chaudry, M., Ekins, P., Ramachandran, K., Shakoor, A., Skea, J., Strbac, G., Wang, X. & Whitaker, J. 2011. Building a resilient UK energy system.

Chaves, A., Rice, M., Dunlap, S. & Pecarina, J. 2017. Improving the cyber resilience of industrial control systems. *International Journal of Critical Infrastructure Protection,* 17**,** 30-48.

Chen, H.-M., Kazman, R., Monarch, I. & Wang, P. Predicting and fixing vulnerabilities before they occur: a big data approach. Proceedings of the 2nd International Workshop on BIG Data Software Engineering, 2016. ACM, 72-75.

Chen, H., Cullinane, K. & Liu, N. 2017. Developing a model for measuring the

resilience of a port-hinterland container transportation network. *Transportation Research Part E: Logistics and Transportation Review,* 97**,** 282-301.
Chen, L. & Miller-Hooks, E. 2012. Resilience: an indicator of recovery capability in intermodal freight transport. *Transportation Science,* 46**,** 109-123.
Chen, S.-C., Ferng, J.-W., Wang, Y.-T., Wu, T.-Y. & Wang, J.-J. 2008. Assessment of disaster resilience capacity of hillslope communities with high risk for geological hazards. *Engineering Geology,* 98**,** 86-101.
Chen, X. & Elsayed, E. A. Reliability and Resilience Assessment of Stochastic Networks. *2017 Engineering Mechanics Institute Conference*, San Diego, June 4-7, 2017
Chen, Z., Du, W.-B., Cao, X.-B. & Zhou, X.-L. 2015. Cascading failure of interdependent networks with different coupling preference under targeted attack. *Chaos, Solitons & Fractals,* 80**,** 7-12.
Cheng, Y., Elsayed, E. A. & Chen, X. 2018. Review of Multi Hazard Resilience. *International Journal of Production Research*.
Cheok, M. C., Parry, G. W. & Sherry, R. R. 1998. Use of importance measures in risk-informed regulatory applications. *Reliability Engineering & System Safety,* 60**,** 213-226.
Chhetri, S. R., Canedo, A. & Al Faruque, M. A. Kcad: kinetic cyber-attack detection method for cyber-physical additive manufacturing systems. Computer-Aided Design (ICCAD), 2016 IEEE/ACM International Conference on, 2016. IEEE, 1-8.
Choras, M., Kozik, R., Bruna, M. P. T., Yautsiukhin, A., Churchill, A., Maciejewska, I., Eguinoa, I. & Jomni, A. Comprehensive approach to increase cyber security and resilience. Availability, Reliability and Security (ARES), 2015 10th International Conference on, 2015. IEEE, 686-692.
Choudhury, S., Rodriguez, L., Curtis, D., Oler, K., Nordquist, P., Chen, P.-Y. & Ray, I. Action recommendation for cyber resilience. Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, 2015. ACM, 3-8.
Cimellaro, G. P., Reinhorn, A. M. & Bruneau, M. 2010a. Framework for analytical quantification of disaster resilience. *Engineering Structures,* 32**,** 3639-3649.
Cimellaro, G. P., Reinhorn, A. M. & Bruneau, M. 2010b. Seismic resilience of a hospital system. *Structure and Infrastructure Engineering,* 6**,** 127-144.
Clarke, J. & Obrien, E. 2016. A multi-hazard risk assessment methodology, stress test framework and decision support tool for transport infrastructure networks. *Transportation Research Procedia,* 14**,** 1355-1363.
Collier, Z. A. & Linkov, I. 2014. Decision making for resilience within the context of network centric operations. ARMY CORPS OF ENGINEERS VICKSBURG MS ENGINEER RESEARCH AND DEVELOPMENT CENTER.
Comfort, L. K. 2007. *Shared risk: Complex systems in seismic response*, Emerald Group Publishing.
Coppola, D. P. 2006. *Introduction to international disaster management*, Butterworth-Heinemann.
Corradini, M. L. & Cristofaro, A. 2017. Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes. *IET Control Theory & Applications*.

Crucitti, P., Latora, V. & Marchiori, M. 2004a. Model for cascading failures in complex networks. *Physical Review E,* 69**,** 045104.
Crucitti, P., Latora, V. & Marchiori, M. 2004b. A topological analysis of the Italian electric power grid. *Physica A: Statistical mechanics and its applications,* 338**,** 92-97.
Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., Goodchild, M. F., Kunreuther, H. C., Li-Vollmer, M. & Schoch-Spana, M. 2013. Disaster resilience: A national imperative. *Environment: Science and Policy for Sustainable Development,* 55**,** 25-29.
Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E. & Webb, J. 2008. A place-based model for understanding community resilience to natural disasters. *Global environmental change,* 18**,** 598-606.
Cutter, S. L., Burton, C. G. & Emrich, C. T. 2010. Disaster resilience indicators for benchmarking baseline conditions. *Journal of Homeland Security and Emergency Management,* 7.
Das, S., Mukhopadhyay, A. & Shukla, G. K. i-HOPE framework for predicting cyber breaches: a logit approach. System Sciences (HICSS), 2013 46th Hawaii International Conference on, 2013. IEEE, 3008-3017.
Debar, H., Becker, M. & Siboni, D. A neural network component for an intrusion detection system. Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on, 1992. IEEE, 240-250.
Department of Regional Development and Environment, Project, O. o. A. S. N. H. & Assistance, U. S. A. f. I. D. O. o. F. D. 1990. *Disaster, planning and development: managing natural hazards to reduce loss*, The Department.
Der Kiureghian, A., Ditlevsen, O. D. & Song, J. 2007. Availability, reliability and downtime of systems with repairable components. *Reliability Engineering & System Safety,* 92**,** 231-242.
Dessavre, D. G., Ramirez-Marquez, J. E. & Barker, K. 2016. Multidimensional approach to complex system resilience analysis. *Reliability Engineering & System Safety,* 149**,** 34-43.
Dewar, R. S. The "triptych of cyber security": A classifi cation of active cyber defence. Cyber Conflict (CyCon 2014), 2014 6th International Conference On, 2014. IEEE, 7-21.
Dewar, R. S. 2017. Active Cyber Defense. *CSS Cyber Defence Trend Analysis,* 1.
Di Mauro, C., Bouchon, S., Carpignana, A., Golia, E. & Peressin, S. Definition of multi-risk maps at regional level as management tool: experience gained by civil protection authorities of Piemonte region. Proceedings of the 5th Conference on Risk Assessment and Management in the Civil and Industrial Settlements, 2006. 17-19.
Dindar, S., Kaewunruen, S., An, M. & Osman, M. H. 2016. Natural hazard risks on railway turnout systems. *Procedia Engineering,* 161**,** 1254-1259.
Do Van, P., Barros, A. & Bérenguer, C. 2010. From differential to difference importance measures for Markov reliability models. *European Journal of Operational Research,* 204**,** 513-521.
Dorogovtsev, S. 2002. SN Dorogovtsev and JFF Mendes, Adv. Phys. 51, 1079 (2002). *Adv. Phys.,* 51**,** 1079.

Dorogovtsev, S. N. & Mendes, J. F. 2002. Evolution of networks. *Advances in physics,* 51**,** 1079-1187.
Dreyer, J. T. 2015. *China's Political System*, Routledge.
Duenas-Osorio, L. & Vemuru, S. M. 2009. Cascading failures in complex infrastructure systems. *Structural safety,* 31**,** 157-167.
Dui, H., Si, S., Cui, L., Cai, Z. & Sun, S. 2014. Component importance for multi-state system lifetimes with renewal functions. *IEEE Transactions on Reliability,* 63**,** 105-117.
Dui, H., Si, S., Zuo, M. J. & Sun, S. 2015. Semi-Markov process-based integrated importance measure for multi-state systems. *IEEE Transactions on Reliability,* 64**,** 754-765.
Easterby-Smith, M., Thorpe, R. & Jackson, P. R. 2012. *Management research*, Sage.
Eidsvig, U. M. K., Kristensen, K. & Vangelsten, B. V. 2017. Assessing the risk posed by natural hazards to infrastructures. *Natural Hazards and Earth System Sciences,* 17**,** 481.
El-Neweihi, E., Proschan, F. & Sethuraman, J. 1978. Multistate coherent systems. *Journal of Applied Probability,* 15**,** 675-688.
Elsayed, E. A. 2012. *Reliability engineering*, John Wiley & Sons.
Energy Networks Association 2011. Electricity networks climate change adaptation report. London, U.K.
Enjalbert, S., Vanderhaegen, F., Pichon, M., Ouedraogo, K. A. & Millot, P. 2011. Assessment of transportation system resilience. *Human Modelling in Assisted Transportation.* Springer.
Eryilmaz, S. 2013. Joint reliability importance in linear $ m $-consecutive-$ k $-out-of-$ n $: F systems. *IEEE Transactions on Reliability,* 62**,** 862-869.
Esfahani, P. M., Vrakopoulou, M., Margellos, K., Lygeros, J. & Andersson, G. Cyber attack in a two-area power system: Impact identification using reachability. American Control Conference (ACC), 2010, 2010. IEEE, 962-967.
Eshrati, L., Mahmoudzadeh, A. & Taghvaei, M. 2015. Multi hazards risk assessment, a new methodology. *International Journal of Health System and Disaster Management,* 3**,** 79.
Espinoza, S., Panteli, M., Mancarella, P. & Rudnick, H. 2016. Multi-phase assessment and adaptation of power systems resilience to natural hazards. *Electric Power Systems Research,* 136**,** 352-361.
Ettouney, M. M. & Alampalli, S. 2016. *Multihazard Considerations in Civil Infrastructure*, CRC Press.
Falahati, B., Fu, Y. & Wu, L. 2012. Reliability assessment of smart grid considering direct cyber-power interdependencies. *IEEE Transactions on Smart Grid,* 3**,** 1515-1524.
Fang, Y.-P., Pedroni, N. & Zio, E. 2016. Resilience-based component importance measures for critical infrastructure network systems. *IEEE Transactions on Reliability,* 65**,** 502-512.
Farwell, J. P. & Rohozinski, R. 2012. The new reality of cyber war. *Survival,* 54**,** 107-120.
Faturechi, R., Levenberg, E. & Miller-Hooks, E. 2014. Evaluating and optimizing resilience of airport pavement networks. *Computers & Operations Research,* 43**,** 335-

348.
Faturechi, R. & Miller-Hooks, E. 2014a. Measuring the performance of transportation infrastructure systems in disasters: A comprehensive review. *Journal of infrastructure systems,* 21**,** 04014025.
Faturechi, R. & Miller-Hooks, E. 2014b. Travel time resilience of roadway networks under disaster. *Transportation research part B: methodological,* 70**,** 47-64.
Feng, G., Patelli, E., Beer, M. & Coolen, F. P. 2016. Imprecise system reliability and component importance based on survival signature. *Reliability Engineering & System Safety,* 150**,** 116-125.
Filippini, R. & Silva, A. 2014. A modeling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. *Reliability*
Flanagan, J. P. 2001. Early warning system for natural and manmade disasters. Google Patents.
Force, U.-C. P. S. O. T., Abraham, S., Dhaliwal, H., Efford, R. J., Keen, L. J., McLellan, A., Manley, J., Vollman, K., Diaz, N. J. & Ridge, T. 2004. *Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations*, US-Canada Power System Outage Task Force.
Foster Jr, J. S., Gjelde, E., Graham, W. R., Hermann, R. J., Kluepfel, H. M., Lawson, R. L., Soper, G. K., Wood Jr, L. L. & Woodard, J. B. 2004. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report. NATIONAL RESEARCH COUNCIL WASHINGTON DC COMMITTEE ON ELECTROMAGNETIC PULSE ENVIRONMENT.
Fotouhi, H., Moryadee, S. & Miller-Hooks, E. 2017. Quantifying the resilience of an urban traffic-electric power coupled system. *Reliability Engineering & System Safety,* 163**,** 79-94.
Franchin, P. & Cavalieri, F. 2015. Probabilistic assessment of civil infrastructure resilience to earthquakes. *Computer‐Aided Civil and Infrastructure Engineering,* 30**,** 583-600.
Francis, R. & Bekera, B. 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety,* 121**,** 90-103.
Frolova, N., Larionov, V., Sushchev, S. & Bonnin, J. 2012. Seismic and Integrated Risk Assessment and Management Line 1 Management with Information Technology Application.
Fussell, J. 1975. How to hand-calculate system reliability and safety characteristics. *IEEE Transactions on Reliability,* 24**,** 169-174.
Gall, M., Borden, K. A., Emrich, C. T. & Cutter, S. L. 2011. The unsustainable trend of natural hazard losses in the United States. *Sustainability,* 3**,** 2157-2181.
Gallina, V., Torresan, S., Critto, A., Sperotto, A., Glade, T. & Marcomini, A. 2016. A review of multi-risk methodologies for natural hazards: Consequences and challenges for a climate change impact assessment. *Journal of environmental management,* 168**,** 123-132.
Gallos, L. 2005. LK Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, Phys. Rev. Lett. 94, 188701 (2005). *Phys. Rev. Lett.,* 94**,** 188701.

Galloway, D. L., Jones, D. R. & Ingebritsen, S. E. 1999. *Land subsidence in the United States*, US Geological Survey.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. 2011. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine,* 30**,** 28-38.

Gandini, A. 1990. Importance and sensitivity analysis in assessing system reliability. *IEEE Transactions on Reliability,* 39**,** 61-70.

Gao, J., Li, D. & Havlin, S. 2014. From a single network to a network of networks. *National Science Review,* 1**,** 346-356.

Gao, X., Cui, L. & Li, J. 2007. Analysis for joint importance of components in a coherent system. *European Journal of Operational Research,* 182**,** 282-299.

Garcia-Aristizabal, A., Selva, J. & Fujita, E. 2013. Integration of stochastic models for long-term eruption forecasting into a Bayesian event tree scheme: a basis method to estimate the probability of volcanic unrest. *Bulletin of volcanology,* 75**,** 689.

Garribba, S., Guagnini, E. & Mussio, P. 1985. Multistate block diagrams and fault trees. *IEEE Trans Reliab***,** 463-72.

Geis, D. E. 2000. By design: the disaster resistant and quality-of-life community. *Natural Hazards Review,* 1**,** 151-160.

Ghosh, A. K., Schwartzbard, A. & Schatz, M. Learning Program Behavior Profiles for Intrusion Detection. Workshop on Intrusion Detection and Network Monitoring, 1999. 1-13.

Ghosn, M., Moses, F. & Wang, J. 2003. *Design of highway bridges for extreme events*, Transportation Research Board.

Gill, J. C. & Malamud, B. D. 2014. Reviewing and visualizing the interactions of natural hazards. *Reviews of Geophysics,* 52**,** 680-722.

Gill, J. C. & Malamud, B. D. 2017. Anthropogenic processes, natural hazards, and interactions in a multi-hazard framework. *Earth-Science Reviews*.

Gillani, F., Al-Shaer, E., Lo, S., Duan, Q., Ammar, M. & Zegura, E. Agile virtualized infrastructure to proactively defend against cyber attacks. Computer Communications (INFOCOM), 2015 IEEE Conference on, 2015. IEEE, 729-737.

Glanz, J., Perez-Pena, R. & Revkin, A. C. 2003. 90 seconds that left tens of millions of people in the dark. *The New York Times***,** 1-1.

Godschalk, D., Beatley, T., Berke, P., Brower, D. & Kaiser, E. J. 1998. *Natural hazard mitigation: Recasting disaster policy and planning*, Island Press.

Goh, K. & Lee, D. 2003. K.-I. Goh, D.-S. Lee, B. Kahng, and D. Kim, Phys. Rev. Lett. 91, 148701 (2003). *Phys. Rev. Lett.,* 91**,** 148701.

Goldman, H., McQuaid, R. & Picciotto, J. Cyber resilience for mission assurance. Technologies for Homeland Security (HST), 2011 IEEE International Conference on, 2011. IEEE, 236-241.

Government of Canada 2010. Canada's Cyber Security Strategy.

Granger, K., Jones, T. G., Leiba, M. & Scott, G. 1999. Community risk in Cairns: a multi-hazard risk assessment. *Australian Journal of Emergency Management, The,* 14**,** 25.

Gravette, M. A. & Barker, K. 2015. Achieved availability importance measure for

enhancing reliability-centered maintenance decisions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 229**,** 62-72.
Griffith, W. S. 1980. Multistate reliability models. *Journal of Applied Probability,* 17**,** 735-744.
Guimerà, R. 2003. R. Guimerà, L. Danon, A. Díaz-Guilera, F. Giralt, and A. Arenas, Phys. Rev. E 68, 065103 (R)(2003). *Phys. Rev. E,* 68**,** 065103.
Guimera, R., Arenas, A., Díaz-Guilera, A. & Giralt, F. 2002. Dynamical properties of model communication networks. *Physical Review E,* 66**,** 026704.
Gunderson, L. H. 2000. Ecological resilience—in theory and application. *Annual review of ecology and systematics,* 31**,** 425-439.
Gupta, S., Kazi, F., Wagh, S. & Singh, N. Probabilistic framework for evaluation of smart grid resilience of cascade failure. Innovative Smart Grid Technologies-Asia (ISGT Asia), 2014 IEEE, 2014. IEEE, 255-260.
Haddow, G., Bullock, J. & Coppola, D. P. 2017. *Introduction to emergency management*, Butterworth-Heinemann.
Haimes, Y. Y. 2009. On the definition of resilience in systems. *Risk Analysis,* 29**,** 498-501.
Hajian-Hoseinabadi, H. & Golshan, M. E. H. 2012. Availability, reliability, and component importance evaluation of various repairable substation automation systems. *IEEE Transactions on Power Delivery,* 27**,** 1358-1367.
Hanfling, D., Altevogt, B. M., Viswanathan, K. & Gostin, L. O. 2012. *Crisis standards of care: a systems framework for catastrophic disaster response*, National Academies Press.
Hashimoto, T., Stedinger, J. R. & Loucks, D. P. 1982. Reliability, resiliency, and vulnerability criteria for water resource system performance evaluation. *Water resources research,* 18**,** 14-20.
Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. 2012. The law of cyber-attack. *California Law Review***,** 817-885.
He, F., Zhuang, J., Rao, N. S., Ma, C. Y. & Yau, D. K. Game-theoretic resilience analysis of cyber-physical systems. Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013 IEEE 1st International Conference on, 2013. IEEE, 90-95.
Heckman, K. E., Walsh, M. J., Stech, F. J., O'boyle, T. A., DiCato, S. R. & Herber, A. F. 2013. Active cyber defense with denial and deception: A cyber-wargame experiment. *computers & security,* 37**,** 72-77.
Henry, D. & Ramirez-Marquez, J. E. 2012. Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety,* 99**,** 114-122.
Hirsch, W. M., Meisner, M. & Boll, C. 1968. Cannibalization in multicomponent systems and the theory of reliability. *Naval Research Logistics (NRL),* 15**,** 331-360.
Holling, C. S. 1973. Resilience and stability of ecological systems. *Annual review of ecology and systematics,* 4**,** 1-23.
Hollnagel, E., Woods, D. D. & Leveson, N. 2007. *Resilience engineering: Concepts and precepts*, Ashgate Publishing, Ltd.
Holme, P. & Kim, B. J. 2002. Vertex overload breakdown in evolving networks.

*Physical Review E,* 65**,** 066109.
Hong, J.-S., Koo, H.-Y. & Lie, C.-H. 2000. Computation of joint reliability importance of two gate events in a fault tree. *Reliability Engineering & System Safety,* 68**,** 1-5.
Hong, J.-S., Koo, H.-Y. & Lie, C.-H. 2002. Joint reliability importance of k-out-of-n systems. *European Journal of Operational Research,* 142**,** 539-547.
Hong, J. S. & Lie, C. H. 1993. Joint reliability-importance of two edges in an undirected network. *IEEE transactions on reliability,* 42**,** 17-23.
Hosseini, S. & Barker, K. 2016. Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. *Computers & Industrial Engineering,* 93**,** 252-266.
Huang, L., Yang, L. & Yang, K. 2006. Geographical effects on cascading breakdowns of scale-free networks. *Physical Review E,* 73**,** 036102.
Hurst, W., Shone, N. & Monnet, Q. Predicting the Effects of DDoS Attacks on a Network of Critical Infrastructures. Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 2015. IEEE, 1697-1702.
Institute of Medicine 2015. *Healthy, Resilient, and Sustainable Communities After Disasters: Strategies, Opportunities, and Planning for Recovery,* Washington, DC, The National Academies Press.
Islam, T. & Ryan, J. 2015. *Hazard Mitigation in Emergency Management*, Butterworth-Heinemann.
Iyer, S. 1992. The Barlow–Proschan importance and its generalizations with dependent components. *Stochastic processes and their applications,* 42**,** 353-359.
Jackson, P. S. 1983. On the s-importance of elements and prime implicants of non-coherent systems. *IEEE Transactions on Reliability,* 32**,** 21-25.
Jacobson, V. Congestion avoidance and control. ACM SIGCOMM computer communication review, 1988a. ACM, 314-329.
Jacobson, V. 1988b. V. Jacobson, Comput. Commun. Rev. 18, 314 (1988). *Comput. Commun. Rev.,* 18**,** 314.
Janić, M. 2015a. Modelling the resilience, friability and costs of an air transport network affected by a large-scale disruptive event. *Transportation Research Part A: Policy and Practice,* 71**,** 1-16.
Janić, M. 2015b. Reprint of "Modelling the resilience, friability and costs of an air transport network affected by a large-scale disruptive event". *Transportation Research Part A: Policy and Practice,* 81**,** 77-92.
Jenelius, E., Petersen, T. & Mattsson, L.-G. 2006. Importance and exposure in road network vulnerability analysis. *Transportation Research Part A: Policy and Practice,* 40**,** 537-560.
Jensen, L. 2015. Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review,* 5**,** 35.
Jin, J. G., Tang, L. C., Sun, L. & Lee, D.-H. 2014. Enhancing metro network resilience via localized integration with bus services. *Transportation Research Part E: Logistics and Transportation Review,* 63**,** 17-30.

Kahan, J. H., Allen, A. C. & George, J. K. 2009. An operational framework for resilience. *Journal of Homeland Security and Emergency Management,* 6.
Kappes, M. S., Keiler, M., von Elverfeldt, K. & Glade, T. 2012. Challenges of analyzing multi-hazard risk: a review. *Natural hazards,* 64**,** 1925-1958.
Karthikeyan, K. & Indra, A. 2010. Intrusion detection tools and techniques-a survey. *International Journal of Computer Theory and Engineering,* 2**,** 901.
Keogh, M. & Cody, C. 2013. Resilience in Regulated Utilities. *In:* Commissioners, T. N. A. o. R. U. (ed.). Washington, DC, USA.
Khalid, H. M. & Peng, J. C.-H. 2016. A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks. *IEEE Transactions on Smart Grid,* 7**,** 2026-2037.
Khalili, A., Michalk, B., Alford, L., Henney, C. & Gilbert, L. Impact modeling and prediction of attacks on cyber targets. Proc. of SPIE Vol, 2010. 77090M-1.
Khan, O. & Estay, D. A. S. 2015. Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review,* 5.
Kim, B. J. 2004. Phase transition in the modified fiber bundle model. *EPL (Europhysics Letters),* 66**,** 819.
Kim, C. & Baxter, L. A. 1987. Reliability importance for continuum structure functions. *Journal of applied probability,* 24**,** 779-785.
Kim, D.-H., Kim, B. J. & Jeong, H. 2005. Universality class of the fiber bundle model on complex networks. *Physical review letters,* 94**,** 025501.
Kim, D., Paek, S.-H. & Oh, H.-S. 2008. A Hilbert–Huang transform approach for predicting cyber-attacks. *Journal of the Korean Statistical Society,* 37**,** 277-283.
Kim, K.-D. & Kumar, P. R. 2012. Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE,* 100**,** 1287-1308.
Kim, S. J. & Hong, S. Study on the development of early warning model for cyber attack. Information Science and Applications (ICISA), 2011 International Conference on, 2011. IEEE, 1-8.
Kinney, R., Crucitti, P., Albert, R. & Latora, V. 2005. Modeling cascading failures in the North American power grid. *The European Physical Journal B-Condensed Matter and Complex Systems,* 46**,** 101-107.
Kirschen, D. & Bouffard, F. 2009. Keeping the lights on and the information flowing. *IEEE Power and Energy magazine,* 7.
Kivelä, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y. & Porter, M. A. 2014. Multilayer networks. *Journal of complex networks,* 2**,** 203-271.
Klein, R. J., Nicholls, R. J. & Thomalla, F. 2003. Resilience to natural hazards: How useful is this concept? *Global Environmental Change Part B: Environmental Hazards,* 5**,** 35-45.
Kleinberg, J. 2007. Computing: The wireless epidemic. *Nature,* 449**,** 287.
Klimburg, A. 2012. National cyber security framework manual.
Kodur, V., Gu, L. & Garlock, M. 2010. Review and assessment of fire hazard in bridges. *Transportation Research Record: Journal of the Transportation Research Board***,** 23-29.
Kodur, V. & Naser, M. 2013. Importance factor for design of bridges against fire hazard.

*Engineering Structures,* 54**,** 207-220.
Kong, Z. & Yeh, E. M. 2010. Resilience to degree-dependent and cascading node failures in random geometric networks. *IEEE Transactions on Information Theory,* 56**,** 5533-5546.
Kosterev, D. N., Taylor, C. W. & Mittelstadt, W. A. 1999. Model validation for the August 10, 1996 WSCC system outage. *IEEE transactions on power systems,* 14**,** 967-979.
Kotenko, I. & Chechulin, A. A cyber attack modeling and impact assessment framework. Cyber Conflict (CyCon), 2013 5th International Conference on, 2013. IEEE, 1-24.
Kovacevic, A. & Nikolic, D. 2014. Cyber Attacks on Critical Infrastructure: Review and Challenges. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance***,** 1.
Krausmann, E., Cruz, A. M. & Salzano, E. 2016. *Natech Risk Assessment and Management: Reducing the Risk of Natural-Hazard Impact on Hazardous Installations*, Elsevier.
Krotofil, M. & Cárdenas, A. A. Resilience of process control systems to cyber-physical attacks. Nordic Conference on Secure IT Systems, 2013. Springer, 166-182.
Kumar, S. 1995. *Classification and detection of computer intrusions.* PhD thesis, Purdue University.
Kundur, P., Balu, N. J. & Lauby, M. G. 1994. *Power system stability and control*, McGraw-hill New York.
Kuo, W. & Zhu, X. 2012. Some recent advances on importance measures in reliability. *IEEE Transactions on Reliability,* 61**,** 344-360.
Kusky, T. M. 2003. *Geological hazards: a sourcebook*, Greenwood Publishing Group.
Labaka, L., Hernantes, J. & Sarriegi, J. M. 2015. Resilience framework for critical infrastructures: An empirical study in a nuclear plant. *Reliability Engineering & System Safety,* 141**,** 92-105.
Lambert, H. 1975a. Measures of importance of events and cut sets in fault trees. *In reliability and fault tree analysis: theoretical and applied aspects of system reliability and safety assessment***,** 77-100.
Lambert, H. E. 1975b. Fault trees for decision making in systems analysis. California Univ., Livermore (USA). Lawrence Livermore Lab.
Lambert, H. E. & Yadigaroglu, G. 1977. Fault trees for diagnosis of system fault conditions. *Nuclear Science and Engineering,* 62**,** 20-34.
Latora, V. & Marchiori, M. 2001. Efficient behavior of small-world networks. *Physical review letters,* 87**,** 198701.
Lee, J. Y. & Ellingwood, B. R. 2017. A decision model for intergenerational life-cycle risk assessment of civil infrastructure exposed to hurricanes under climate change. *Reliability Engineering & System Safety,* 159**,** 100-107.
Leemis, L. M. 1995. *Reliability: probabilistic models and statistical methods*, Prentice-Hall, Inc.
Levitin, G. 2005. *The universal generating function in reliability analysis and optimization*, Springer.
Levitin, G. & Lisnianski, A. 1999. Importance and sensitivity analysis of multi-state

systems using the universal generating function method. *Reliability Engineering & System Safety,* 65**,** 271-282.
Levitin, G., Podofillini, L. & Zio, E. 2003. Generalised importance measures for multi-state elements based on performance level restrictions. *Reliability Engineering & System Safety,* 82**,** 287-298.
Lewis, T. G. 2014. *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons.
Li, S., Si, S., Dui, H., Cai, Z. & Sun, S. 2014. A novel decision diagrams extension method. *Reliability Engineering & System Safety,* 126**,** 107-115.
Li, X., Liang, X., Lu, R., Shen, X., Lin, X. & Zhu, H. 2012. Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine,* 50.
Li, Y. & Lence, B. J. 2007. Estimating resilience for water resources systems. *Water Resources Research,* 43.
Lie, C., Hwang, C. & Tillman, F. 1977. Availability of maintained systems: a state-of-the-art survey. *AIIE Transactions,* 9**,** 247-259.
Lin, T. C. 2015. Financial Weapons of War. *Minn. L. Rev.,* 100**,** 1377.
Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J. & Kott, A. 2013. Resilience metrics for cyber systems. *Environment Systems and Decisions,* 33**,** 471-476.
Lisnianski, A. & Levitin, G. 2003. *Multi-state system reliability: assessment, optimization and applications*, World Scientific Publishing Co Inc.
Liu, B., Siu, Y. L. & Mitchell, G. 2016a. Hazard interaction analysis for multi-hazard risk assessment: a systematic classification based on hazard-forming environment. *Natural Hazards and Earth System Sciences,* 16**,** 629-642.
Liu, P. 2005. A game theoretic approach to cyber attack prediction. Pennsylvania State University.
Liu, X., Al-Khalifa, K. N., Elsayed, E. A., Coit, D. W. & Hamouda, A. S. 2014. Criticality measures for components with multi-dimensional degradation. *IIE Transactions,* 46**,** 987-998.
Liu, Y., Si, S., Cui, L., Wang, Z. & Sun, S. 2016b. A generalized Griffith importance measure for components with multiple state transitions. *IEEE Transactions on Reliability,* 65**,** 662-673.
Liu, Y. & Singh, C. 2010a. Evaluation of hurricane impact on composite power system reliability considering common-cause failures. *International Journal of Systems Assurance Engineering and Management,* 1**,** 135-145.
Liu, Y. & Singh, C. 2010b. Reliability evaluation of composite power systems using Markov cut-set method. *IEEE Transactions on Power Systems,* 25**,** 777-785.
Liu, Y., Xin, H., Qu, Z. & Gan, D. 2016c. An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks. *IEEE Transactions on Smart Grid,* 7**,** 2923-2932.
Lu, W., Bésanger, Y., Zamaï, E. & Radu, D. 1996. Blackouts: Description analysis and classification. *network,* 2**,** 14.
Lu, W., Xu, S. & Yi, X. Optimizing active cyber defense. International Conference on Decision and Game Theory for Security, 2013. Springer, 206-225.
Luh, J., Royster, S., Sebastian, D., Ojomo, E. & Bartram, J. 2017. Expert assessment of

the resilience of drinking water and sanitation systems to climate-related hazards. *Science of the Total Environment,* 592**,** 334-344.
Luo, M.-Y. & Yang, C.-S. 2002. Enabling fault resilience for web services. *Computer communications,* 25**,** 198-209.
Madni, A. M. & Jackson, S. 2009. Towards a conceptual framework for resilience engineering. *IEEE Systems Journal,* 3**,** 181-191.
Mamo, X., Mallet, S., Coste, T. & Grenard, S. Distribution automation: The cornerstone for smart grid development strategy. Power & Energy Society General Meeting, 2009. PES'09. IEEE, 2009. IEEE, 1-6.
Marzocchi, W. & Bebbington, M. S. 2012. Probabilistic eruption forecasting at short and long time scales. *Bulletin of volcanology,* 74**,** 1777-1805.
Marzocchi, W., Garcia-Aristizabal, A., Gasparini, P., Mastellone, M. L. & Di Ruocco, A. 2012. Basic principles of multi-risk assessment: a case study in Italy. *Natural hazards,* 62**,** 551-573.
Marzocchi, W., Mastellone, M., Di Ruocco, A., Novelli, P. R. E. & Gasparini, P. 2009. Principles of multi-risk assessment: Interaction amongst natural and man-induced risks.
Marzocchi, W., Sandri, L., Gasparini, P., Newhall, C. & Boschi, E. 2004. Quantifying probabilities of volcanic events: the example of volcanic hazard at Mount Vesuvius. *Journal of Geophysical Research: Solid Earth,* 109.
Marzocchi, W., Sandri, L. & Selva, J. 2010. BET_VH: a probabilistic tool for long-term volcanic hazard assessment. *Bulletin of volcanology,* 72**,** 705-716.
Marzocchi, W. & Woo, G. 2007. Probabilistic eruption forecasting and the call for an evacuation. *Geophysical Research Letters,* 34.
Marzocchi, W. & Zaccarelli, L. 2006. A quantitative model for the time‐size distribution of eruptions. *Journal of Geophysical Research: Solid Earth,* 111.
Masi, D. M., Smith, E. E. & Fischer, M. J. 2010. Understanding and mitigating catastrophic disruption and attack. *Sigma Journal***,** 16-22.
Mayer, A. J., Laing, B. & Lloyd, M. 2012. Methods and apparatus for prioritization of remediation techniques for network security risks. Google Patents.
McColl, L., Palin, E. J., Thornton, H. E., Sexton, D. M., Betts, R. & Mylne, K. 2012. Assessing the potential impact of climate change on the UK's electricity network. *Climatic Change,* 115**,** 821-835.
McGranaghan, M., Von Dollen, D., Myrda, P. & Gunther, E. Utility experience with developing a smart grid roadmap. Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE, 2008. IEEE, 1-5.
Mei, S., Ni, Y., Wang, G. & Wu, S. 2008. A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin. *IEEE Transactions on Power Systems,* 23**,** 1719-1726.
Mendes, P. A., Valente, J. C. & Branco, F. A. 2000. Simulation of ship fire under Vasco da Gama Bridge. *ACI structural journal,* 97**,** 285-290.
Meng, F. C. 1994. Comparing criticality of nodes via minimal cut (path) sets for coherent systems. *Probability in the Engineering and Informational Sciences,* 8**,** 79-87.
Meng, F. C. 1995. Some further results on ranking the importance of system

components. *Reliability Engineering & System Safety,* 47**,** 97-101.
Meng, F. C. 1996. Comparing the importance of system components by some structural characteristics. *IEEE Transactions on Reliability,* 45**,** 59-65.
Meng, F. C. 2000. Relationships of Fussell–Vesely and Birnbaum importance to structural importance in coherent systems. *Reliability Engineering & System Safety,* 67**,** 55-60.
Mezher, T., El Khatib, S. & Sooriyaarachchi, T. M. 2016. Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts. *Civil and Environmental Engineering: Concepts, Methodologies, Tools, and Applications*. IGI Global.
Miller-Hooks, E., Zhang, X. & Faturechi, R. 2012. Measuring and maximizing resilience of freight transportation networks. *Computers & Operations Research,* 39**,** 1633-1643.
Miman, M. & Pohl, E. Uncertainty assessment for availability: importance measures. Reliability and Maintainability Symposium, 2006. RAMS'06. Annual, 2006. IEEE, 222-227.
Mirzasoleiman, B., Babaei, M., Jalili, M. & Safari, M. 2011. Cascaded failures in weighted networks. *Physical Review E,* 84**,** 046114.
Mitchell, J. K., Devine, N. & Jagger, K. 1989. A contextual model of natural hazard. *Geographical review***,** 391-409.
MOD, U. 2011. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. London: UK MOD.
Montz, B. E., Tobin, G. A. & Hagelman III, R. R. 2017. *Natural hazards: explanation and integration*, Guilford Publications.
Moon, Y.-H. & Jeon, Y.-S. Network resilience estimation to cascading failures. Information and Communication Technology Convergence (ICTC), 2015 International Conference on, 2015. IEEE, 962-963.
Moreira, A. A., Andrade Jr, J. S., Herrmann, H. J. & Indekeu, J. O. 2009. How to make a fragile network robust and vice versa. *Physical review letters,* 102**,** 018701.
Moreno, Y. 2003. Y. Moreno, R. Pastor-Satorras, A. Vázquez, and A. Vespignani, Europhys. Lett. 62, 292 (2003). *Europhys. Lett.,* 62**,** 292.
Moreno, Y., Gómez, J. & Pacheco, A. 2002. Instability of scale-free networks under node-breaking avalanches. *EPL (Europhysics Letters),* 58**,** 630.
Moreno, Y., Pastor-Satorras, R., Vázquez, A. & Vespignani, A. 2003. Critical load and congestion instabilities in scale-free networks. *EPL (Europhysics Letters),* 62**,** 292.
Motter, A. E. 2004. Cascade control and defense in complex networks. *Physical Review Letters,* 93**,** 098701.
Motter, A. E. & Lai, Y.-C. 2002. Cascade-based attacks on complex networks. *Physical Review E,* 66**,** 065102.
Mowbray, T. J. 2013. *Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions*, John Wiley & Sons.
Moyer, T., Chadha, K., Cunningham, R., Schear, N., Smith, W., Bates, A., Butler, K., Capobianco, F., Jaeger, T. & Cable, P. Leveraging Data Provenance to Enhance Cyber Resilience. Cybersecurity Development (SecDev), IEEE, 2016. IEEE, 107-114.

Mugume, S. N., Gomez, D. E., Fu, G., Farmani, R. & Butler, D. 2015. A global analysis approach for investigating structural resilience in urban drainage systems. *Water research,* 81**,** 15-26.

Murray-Tuite, P. & Mahmassani, H. 2004. Methodology for determining vulnerable links in a transportation network. *Transportation Research Record: Journal of the Transportation Research Board***,** 88-96.

Musman, S. Assessing prescriptive improvements to a system's cyber security and resilience. Systems Conference (SysCon), 2016 Annual IEEE, 2016. IEEE, 1-6.

Musman, S., Temin, A., Tanner, M., Fox, D. & Pridemore, B. Evaluating the impact of cyber attacks on missions. International Conference on Cyber Warfare and Security, 2010. Academic Conferences International Limited, 446.

Musman, S. & Turner, A. 2017. A game theoretic approach to cyber security risk management. *The Journal of Defense Modeling and Simulation***,** 1548512917699724.

Nan, C. & Sansavini, G. 2017. A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety,* 157**,** 35-53.

National Academies of Sciences Engineering and Medicine 2017. Volcanic Eruptions and Their Repose, Unrest, Precursors, and Timing.

National Energy Technology Laboratory 2007. A Systems View of the Modern Grid. *U.S. Department of Energy*

National Research Council 2011. *National earthquake resilience: Research, implementation, and outreach,* Washington, DC, National Academies Press.

National Research Council 2012. *Dam and levee safety and community resilience: A vision for future practice*, National Academies Press.

National Research Council, Committee on U.S. Army Corps of Engineers Water Resources Science, E., and Planning: Coastal Risk Reduction,, Water Science and Technology Board, Ocean Studies Board & Division on Earth and Life Studies 2014. Reducing coastal risk on the east and gulf coasts. Citeseer.

National Research Council, Division on Earth and Life Studies, Ocean Studies Board & Preparedness, C. o. t. R. o. t. T. W. a. F. S. a. O. o. t. N. s. T. 2011. *Tsunami warning and preparedness: an assessment of the us tsunami program and the nation's preparedness efforts*, National Academies Press.

Natvig, B. 1979. A suggestion of a new measure of importance of system components. *Stochastic Processes and their Applications,* 9**,** 319-330.

Natvig, B. 1982a. On the reduction in remaining system lifetime due to the failure of a specific component. *Journal of Applied Probability,* 19**,** 642-652.

Natvig, B. 1982b. Two suggestions of how to define a multistate coherent system. *Advances in Applied Probability,* 14**,** 434-455.

Natvig, B. 1985. New light on measures of importance of system components. *Scandinavian Journal of Statistics***,** 43-54.

Natvig, B. 2011. Measures of component importance in nonrepairable and repairable multistate strongly coherent systems. *Methodology and Computing in Applied Probability,* 13**,** 523-547.

Natvig, B., Eide, K. A., Gåsemyr, J., Huseby, A. B. & Isaksen, S. L. 2009. Simulation based analysis and an application to an offshore oil and gas production system of the

Natvig measures of component importance in repairable systems. *Reliability Engineering & System Safety,* 94**,** 1629-1638.
Natvig, B. & Gåsemyr, J. 2006. New results on Barlow-Proschan type measures of component importance in nonrepairable and repairable systems. *Preprint series. Statistical Research Report* http://urn*. nb. no/URN: NBN: no-23420*.
Natvig, B. & Gåsemyr, J. 2009. New results on the Barlow–Proschan and Natvig measures of component importance in nonrepairable and repairable systems. *Methodology and Computing in Applied Probability,* 11**,** 603-620.
Natvig, B., Huseby, A. B. & Reistadbakk, M. O. 2011. Measures of component importance in repairable multistate systems—a numerical study. *Reliability Engineering & System Safety,* 96**,** 1680-1690.
Newman, M. 2003. MEJ Newman, SIAM Rev. 45, 167 (2003). *SIAM Rev.,* 45**,** 167.
Newth, D. & Ash, J. Evolving cascading failure resilience in complex networks. Proc. of 8th Asia Pacific Symp. on Intelligent and Evolutionary Systems, 2004.
Nigg, J. M. & Mileti, D. 1997. Natural hazards and disasters.
North American Electric Reliability Corporation 2010. High-Impact, Low-Frequency Event Risk Report. Washington, DC, USA.
Northern PowerGrid 2013. Climate Change Adaptation Report.
O'Rourke, T. D. 2007. Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING-,* 37**,** 22.
Omer, M., Mostashari, A. & Lindemann, U. 2014. Resilience analysis of soft infrastructure systems. *Procedia Computer Science,* 28**,** 565-574.
Omer, M., Nilchiani, R. & Mostashari, A. 2009. Measuring the resilience of the trans-oceanic telecommunication cable system. *IEEE Systems Journal,* 3**,** 295-303.
Orwin, K. H. & Wardle, D. A. 2004. New indices for quantifying the resistance and resilience of soil biota to exogenous disturbances. *Soil Biology and Biochemistry,* 36**,** 1907-1912.
Ouedraogo, K. A., Enjalbert, S. & Vanderhaegen, F. 2013. How to learn from the resilience of Human–Machine Systems? *Engineering Applications of Artificial Intelligence,* 26**,** 24-34.
Ouyang, M. 2017. A mathematical framework to optimize resilience of interdependent critical infrastructure systems under spatially localized attacks. *European Journal of Operational Research,* 262**,** 1072-1084.
Ouyang, M. & Dueñas-Osorio, L. 2012. Time-dependent resilience assessment and improvement of urban infrastructure systems. *Chaos: An Interdisciplinary Journal of Nonlinear Science,* 22**,** 033122.
Ouyang, M. & Dueñas-Osorio, L. 2014. Multi-dimensional hurricane resilience assessment of electric power systems. *Structural Safety,* 48**,** 15-24.
Ouyang, M., Dueñas-Osorio, L. & Min, X. 2012. A three-stage resilience analysis framework for urban infrastructure systems. *Structural safety,* 36**,** 23-31.
Ouyang, M. & Wang, Z. 2015. Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety,* 141**,** 74-82.
Overbye, T. J., Vittal, V. & Dobson, I. 2012. Engineering resilient cyber-physical

systems. *PSERC Publication*, 1-22.
Page, L. B. & Perry, J. E. 1994. Reliability polynomials and link importance in networks. *IEEE Transactions on Reliability,* 43, 51-58.
Pan, S., Morris, T. & Adhikari, U. 2015. Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Transactions on Industrial Informatics,* 11, 650-662.
Pan, Z. & Nonaka, Y. 1995. Importance analysis for the systems with common cause failures. *Reliability Engineering & System Safety,* 50, 297-300.
Pant, R., Barker, K., Ramirez-Marquez, J. E. & Rocco, C. M. 2014a. Stochastic measures of resilience and their application to container terminals. *Computers & Industrial Engineering,* 70, 183-194.
Pant, R., Barker, K. & Zobel, C. W. 2014b. Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliability Engineering & System Safety,* 125, 92-102.
Panteli, M. & Mancarella, P. 2015. Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events. *IEEE Systems Journal*.
Papastavridis, S. 1987. The most important component in a consecutive-k-out-of-n: F system. *IEEE transactions on reliability,* 36, 266-268.
Parshani, R., Buldyrev, S. V. & Havlin, S. 2010. Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. *Physical review letters,* 105, 048701.
Passeri, P. 2018. 2017 Cyber Attacks Statistics.
Payá-Zaforteza, I. & Garlock, M. 2012. A numerical investigation on the fire response of a steel girder bridge. *Journal of Constructional Steel Research,* 75, 93-103.
Peng, H., Coit, D. W. & Feng, Q. 2012. Component reliability criticality or importance measures for systems with degrading components. *IEEE Transactions on Reliability,* 61, 4-12.
Perry, R. W. & Lindell, M. K. 2008. Volcanic risk perception and adjustment in a multi-hazard environment. *Journal of Volcanology and Geothermal Research,* 172, 170-178.
Pettit, T. J., Fiksel, J. & Croxton, K. L. 2010. Ensuring supply chain resilience: development of a conceptual framework. *Journal of business logistics,* 31, 1-21.
Pitilakis, K., Franchin, P., Khazai, B. & Wenzel, H. 2014. *SYNER-G: Systemic seismic vulnerability and risk assessment of complex urban, utility, lifeline systems and critical facilities: Methodology and applications*, Springer.
Poelhekke, L., Jäger, W. S., van Dongeren, A., Plomaritis, T. A., McCall, R. & Ferreira, Ó. 2016. Predicting coastal hazards for sandy coasts with a Bayesian network. *Coastal Engineering,* 118, 21-34.
Postelnicu, V. 1970. Nondichotomic multi-component structures. *Bulletin mathématique de la Société des Sciences Mathématiques de la République Socialiste de Roumanie,* 14, 209-217.
Poursanidis, D. & Chrysoulakis, N. 2017. Remote Sensing, natural hazards and the contribution of ESA Sentinels missions. *Remote Sensing Applications: Society and Environment,* 6, 25-38.
Pregenzer, A. L. 2011. Systems resilience: a new analytical framework for nuclear

nonproliferation. *Sandia National Laboratories, Albuquerque. New México,* 8**,** 1-21.
Preston, B. L., Backhaus, S. N., Ewers, M., Phillips, J., Dagle, J. E., Silva-Monroy, C., Tarditi, A., Looney, J. & King Jr, T. 2016. Resilience of the US Electricity System: A Multi-Hazard Perspective. Department of Energy, forthcoming.
Qarahasanlou, A. N., Khalokakaie, R., Ataei, M. & Ghodrati, B. 2017. Operating Environment-Based Availability Importance Measures for Mining Equipment (Case Study: Sungun Copper Mine). *Journal of Failure Analysis and Prevention,* 17**,** 56-67.
Qin, X. & Lee, W. Attack plan recognition and prediction using causal networks. Computer Security Applications Conference, 2004. 20th Annual, 2004. IEEE, 370-379.
Ramirez-Marquez, J. E. & Coit, D. W. 2005. Composite importance measures for multi-state systems with multi-state components. *IEEE Transactions on Reliability,* 54**,** 517-529.
Ramirez-Marquez, J. E. & Coit, D. W. 2007. Multi-state component criticality analysis for reliability improvement in multi-state systems. *Reliability Engineering & System Safety,* 92**,** 1608-1619.
Ramirez-Marquez, J. E., Rocco, C. M., Gebre, B. A., Coit, D. W. & Tortorella, M. 2006. New insights on multi-state component criticality and importance. *Reliability Engineering & System Safety,* 91**,** 894-904.
Ran, J. & Nedovic-Budic, Z. 2016. Integrating spatial planning and flood risk management: A new conceptual framework for the spatially integrated policy infrastructure. *Computers, Environment and Urban Systems,* 57**,** 68-79.
Reed, D. A., Kapur, K. C. & Christie, R. D. 2009. Methodology for assessing the resilience of networked infrastructure. *IEEE Systems Journal,* 3**,** 174-180.
Ren, H. & Dobson, I. 2008. Using transmission line outage data to estimate cascading failure propagation in an electric power system. *IEEE Transactions on Circuits and Systems II: Express Briefs,* 55**,** 927-931.
Repik, K. A. 2008. Defeating adversary network intelligence efforts with active cyber defense techniques. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING AND MANAGEMENT.
Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems,* 21**,** 11-25.
Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S. & Setola, R. 2008. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures,* 4**,** 63-79.
Rose, A. 2007. Economic resilience to natural and man-made disasters: Multidisciplinary origins and contextual dimensions. *Environmental Hazards,* 7**,** 383-398.
Ross, S. M. 1979. Multivalued state component systems. *The Annals of Probability,* 7**,** 379-383.
Ross, S. M. 2014. *Introduction to probability models*, Academic press.
Sachtjen, M., Carreras, B. & Lynch, V. 2000. Disturbances in a power transmission system. *Physical Review E,* 61**,** 4877.
Sahebjamnia, N., Torabi, S. A. & Mansouri, S. A. 2015. Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal*

*of Operational Research,* 242**,** 261-273.
Saini, H., Rao, Y. S. & Panda, T. 2012. Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications,* 2**,** 202-9.
Sarre, S., Redlich, C., Tinker, A., Sadler, E., Bhalla, A. & McKevitt, C. 2014. A systematic review of qualitative studies on adjusting after stroke: lessons for the study of resilience. *Disability and rehabilitation,* 36**,** 716-726.
Schäfer, M., Scholz, J. & Greiner, M. 2006. Proactive robustness control of heterogeneously loaded networks. *Physical review letters,* 96**,** 108701.
Schmidt, J., Matcham, I., Reese, S., King, A., Bell, R., Henderson, R., Smart, G., Cousins, J., Smith, W. & Heron, D. 2011. Quantitative multi-risk analysis for natural hazards: a framework for multi-risk modelling. *Natural Hazards,* 58**,** 1169-1192.
Shackelford, S. 2009. From nuclear war to net war: analogizing cyber attacks in international law.
Shaw, J. J. Predicting the impact of cyber-attacks on BMC/sup 3/enterprises. DARPA Information Survivability Conference and Exposition, 2003. Proceedings, 2003. IEEE, 208-213.
Shen, D., Chen, G., Haynes, L. & Blasch, E. Strategies comparison for game theoretic cyber situational awareness and impact assessment. Information Fusion, 2007 10th International Conference on, 2007. IEEE, 1-8.
Shirali, G. A., Mohammadfam, I. & Ebrahimipour, V. 2013. A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering & System Safety,* 119**,** 88-94.
Si, S., Cai, Z., Sun, S. & Zhang, S. 2010. Integrated importance measures of multi-state systems under uncertainty. *Computers & Industrial Engineering,* 59**,** 921-928.
Si, S., Dui, H., Cai, Z. & Sun, S. 2012a. The integrated importance measure of multi-state coherent systems for maintenance processes. *IEEE Transactions on Reliability,* 61**,** 266-273.
Si, S., Dui, H., Cai, Z., Sun, S. & Zhang, Y. 2012b. Joint integrated importance measure for multi-state transition systems. *Communications in Statistics-Theory and Methods,* 41**,** 3846-3862.
Si, S., Dui, H., Zhao, X., Zhang, S. & Sun, S. 2012c. Integrated importance measure of component states based on loss of system performance. *IEEE Transactions on Reliability,* 61**,** 192-202.
Si, S., Levitin, G., Dui, H. & Sun, S. 2013. Component state-based integrated importance measure for multi-state systems. *Reliability Engineering & System Safety,* 116**,** 75-83.
Silva, A., Pontes, E., Zhou, F., Guelf, A. & Kofuji, S. PRBS/EWMA based model for predicting burst attacks (Brute Froce, DoS) in computer networks. Digital Information Management (ICDIM), 2014 Ninth International Conference on, 2014. IEEE, 194-200.
Simonsen, I., Buzna, L., Peters, K., Bornholdt, S. & Helbing, D. 2008. Transient dynamics increasing network vulnerability to cascading failures. *Physical review letters,* 100**,** 218701.
Singh, S. & Silakari, S. 2009. A survey of cyber-attack detection systems. *International*

*Journal of Computer Science and Network Security,* 9**,** 1-10.
Smith, P., Hutchison, D., Sterbenz, J. P., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, C. & Plattner, B. 2011. Network resilience: a systematic approach. *IEEE Communications Magazine,* 49**,** 88-97.
Spitzner, L. 2003. *Honeypots: tracking hackers*, Addison-Wesley Reading.
Sridhar, S., Hahn, A. & Govindarasu, M. 2012. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE,* 100**,** 210-224.
Stamp, J., McIntyre, A. & Ricardson, B. Reliability impacts from cyber attack on electric power systems. Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES, 2009. IEEE, 1-8.
Steinberg, L. J., Sengul, H. & Cruz, A. M. 2008. Natech risk and management: an assessment of the state of the art. *Natural Hazards,* 46**,** 143-152.
Sterbenz, J. P., Cetinkaya, E. K., Hameed, M. A., Jabbar, A. & Rohrer, J. P. Modelling and analysis of network resilience. Communication Systems and Networks (COMSNETS), 2011 Third International Conference on, 2011. IEEE, 1-10.
Sterbenz, J. P., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M. & Smith, P. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks,* 54**,** 1245-1265.
Stewart, M. G., Netherton, M. D. & Rosowsky, D. V. 2006. Terrorism risks and blast damage to built infrastructure. *Natural Hazards Review,* 7**,** 114-122.
Sun, C.-C., Hong, J. & Liu, C.-C. A coordinated cyber attack detection system (CCADS) for multiple substations. Power Systems Computation Conference (PSCC), 2016, 2016. IEEE, 1-7.
Sun, K. & Han, Z.-X. Analysis and comparison on several kinds of models of cascading failure in power system. Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES, 2005. IEEE, 1-7.
Talukdar, S. N., Apt, J., Ilic, M., Lave, L. B. & Morgan, M. G. 2003. Cascading failures: survival versus prevention. *The Electricity Journal,* 16**,** 25-31.
Tan, F., Xia, Y., Zhang, W. & Jin, X. 2013. Cascading failures of loads in interconnected networks under intentional attack. *EPL (Europhysics Letters),* 102**,** 28009.
Tansel, B. 1995. Natural and manmade disasters: accepting and managing risks. *Safety science,* 20**,** 91-99.
Tarvainen, T., Jarva, J. & Greiving, S. 2006. Spatial pattern of hazards and hazard interactions in Europe. *SPECIAL PAPER-GEOLOGICAL SURVEY OF FINLAND,* 42**,** 83.
Temesgen, B., Mohammed, M. & Korme, T. 2001. Natural hazard assessment using GIS and remote sensing methods, with particular reference to the landslides in the Wondogenet area, Ethiopia. *Physics and Chemistry of the Earth, Part C: Solar, Terrestrial & Planetary Science,* 26**,** 665-675.
Thierry, P., Stieltjes, L., Kouokam, E., Nguéya, P. & Salley, P. M. 2008. Multi-hazard risk mapping and assessment on an active volcano: the GRINP project at Mount Cameroon. *Natural Hazards,* 45**,** 429-456.
Tilman, D. & Downing, J. A. 1994. Biodiversity and stability in grasslands. *Nature,* 367**,** 363-365.

Times, T. N. Y. 2011. Israeli Test on Worm Called Crucial in Iran Nuclear Delay.
Tram, H. Technical and operation considerations in using smart metering for outage management. Transmission and Distribution Conference and Exposition, 2008. T&D. IEEE/PES, 2008. IEEE, 1-3.
Tran, H., Campos-Nanez, E., Fomin, P. & Wasek, J. 2016. Cyber resilience recovery model to combat zero-day malware attacks. *computers & security,* 61**,** 19-31.
Tran, H. T., Balchanos, M., Domercant, J. C. & Mavris, D. N. 2017. A framework for the quantitative assessment of performance-based system resilience. *Reliability Engineering & System Safety,* 158**,** 73-84.
U.S. Department of Energy, U. S. 2014. Energy Sector Vulnerabilities to Climate Change and Extreme Weather. Washington, DC and Denver, CO.
Unesco 1972. Report of consultative meeting of experts on the statistical study of natural hazards and their consequences. *Document SC/WS/500,* 11.
Ungar, M. 2003. Qualitative contributions to resilience research. *Qualitative social work,* 2**,** 85-102.
Urciuoli, L. 2015. Cyber-resilience: a strategic approach for supply chain management. *Technology Innovation Management Review,* 5**,** 13.
Van der Borst, M. & Schoonakker, H. 2001. An overview of PSA importance measures. *Reliability Engineering & System Safety,* 72**,** 241-245.
Van Noortwijk, J. 2009. A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety,* 94**,** 2-21.
Van Westen, C., Van Asch, T. W. & Soeters, R. 2006. Landslide hazard and risk zonation—why is it still so difficult? *Bulletin of Engineering geology and the Environment,* 65**,** 167-184.
Vassell, G. S. 1990. The northeast blackout of 1965. *Public Utilities Fortnightly;(United States),* 126.
Vasseur, D. & Llory, M. 1999. International survey on PSA figures of merit. *Reliability Engineering & System Safety,* 66**,** 261-274.
Vaurio, J. K. 2011. Importance measures for multi-phase missions. *Reliability Engineering & System Safety,* 96**,** 230-235.
Vaurio, J. K. 2016. Importances of components and events in non-coherent systems and risk models. *Reliability Engineering & System Safety,* 147**,** 117-122.
Venkatasubramanian, M. 2003. Analyzing Blackout Events: Experience from Major Western Blackouts in 1996. *Washington, Power Systems Engineering Research Center, Washington State University*.
Vesely, W. 1970. A time-dependent methodology for fault tree evaluation. *Nuclear engineering and design,* 13**,** 337-360.
Vesely, W. E. & Davis, T. C. 1985. Two measures of risk importance and their application. *Nuclear technology,* 68**,** 226-234.
Vespignani, A. 2010. Complex networks: The fragility of interdependency. *Nature,* 464**,** 984.
Vlacheas, P., Stavroulaki, V., Demestichas, P., Cadzow, S., Ikonomou, D. & Gorniak, S. 2013. Towards end-to-end network resilience. *International Journal of Critical Infrastructure Protection,* 6**,** 159-178.

Vugrin, E. D. & Turgeon, J. 2014. Advancing Cyber Resilience Analysis with Performance-Based Metrics from Infrastructure Assessments. *Cyber Behavior: Concepts, Methodologies, Tools, and Applications.* IGI Global.

Vugrin, E. D., Turnquist, M. A. & Brown, N. J. 2014. Optimal recovery sequencing for enhanced resilience and service restoration in transportation networks. *International Journal of Critical Infrastructures,* 10**,** 218-246.

Walker, B., Holling, C. S., Carpenter, S. & Kinzig, A. 2004. Resilience, adaptability and transformability in social–ecological systems. *Ecology and society,* 9.

Wang, B. & Kim, B. J. 2007. A high-robustness and low-cost model for cascading failures. *EPL (Europhysics Letters),* 78**,** 48001.

Wang, D. & Ip, W. 2009. Evaluation and analysis of logistic network resilience with application to aircraft servicing. *IEEE Systems Journal,* 3**,** 166-173.

Wang, J., Gao, F. & Ip, W. 2010. Measurement of resilience and its application to enterprise information systems. *Enterprise Information Systems,* 4**,** 215-223.

Wang, W.-X. & Chen, G. 2008. Universal robustness characteristic of weighted networks against cascading failure. *Physical Review E,* 77**,** 026101.

Waxman, M. C. 2011. Cyber-attacks and the use of force: Back to the future of article 2 (4).

White, G. F. 1974. *Natural hazards, local, national, global*, Oxford University Press.

White House Office United States 2011. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked Worldr*, White House.

Whitson, J. C. & Ramirez-Marquez, J. E. 2009. Resiliency as a component importance measure in network reliability. *Reliability Engineering & System Safety,* 94**,** 1685-1693.

Wildavsky, A. B. 1988. *Searching for safety*, Transaction publishers.

Willis, H. H., Narayanan, A., Fischbach, J. R., Molina-Perez, E., Stelzner, C., Loa, K. & Kendrick, L. 2016. *Current and Future Exposure of Infrastructure in the United States to Natural Hazards*, RAND.

Wood, A. P. 1985. Multistate block diagrams and fault trees. *IEEE Transactions on Reliability,* 34**,** 236-240.

Wu, J., Yin, L. & Guo, Y. Cyber attacks prediction model based on Bayesian network. Parallel and Distributed Systems (ICPADS), 2012 IEEE 18th International Conference on, 2012. IEEE, 730-731.

Wu, S. 2005. Joint importance of multistate systems. *Computers & Industrial Engineering,* 49**,** 63-75.

Wu, S. & Chan, L.-Y. 2003. Performance utility-analysis of multi-state systems. *IEEE Transactions on Reliability,* 52**,** 14-21.

Wu, S. & Coolen, F. P. 2013. A cost-based importance measure for system components: An extension of the Birnbaum importance. *European Journal of Operational Research,* 225**,** 189-195.

Xia, Y., Fan, J. & Hill, D. 2010. Cascading failure in Watts–Strogatz small-world networks. *Physica A: Statistical Mechanics and its Applications,* 389**,** 1281-1285.

Xie, M. 1987. On some importance measures of system components. *Stochastic processes and their applications,* 25**,** 273-280.

Xie, M. & Bergman, B. 1991. On a general measure of component importance. *Journal*

*of statistical planning and inference,* 29**,** 211-220.
Xie, M. & Shen, K. 1989. On ranking of system components with respect to different improvement actions. *Microelectronics Reliability,* 29**,** 159-164.
Yang, S. J., Stotz, A., Holsopple, J., Sudit, M. & Kuhl, M. 2009. High level information fusion for tracking and projection of multistage cyber attacks. *Information Fusion,* 10**,** 107-121.
Yao, Q., Zhu, X. & Kuo, W. 2011. Heuristics for component assignment problems based on the Birnbaum importance. *IIE Transactions,* 43**,** 633-646.
Yodo, N. & Wang, P. 2016. Engineering resilience quantification and system design implications: a literature survey. *Journal of Mechanical Design,* 138**,** 111408.
Yodo, N., Wang, P. & Zhou, Z. 2017. Predictive resilience analysis of complex systems using dynamic Bayesian networks. *IEEE Transactions on Reliability,* 66**,** 761-770.
Youn, B. D., Hu, C. & Wang, P. 2011. Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design,* 133**,** 101011.
Zeng, Y., Xiao, R. & Li, X. 2013. A resilience approach to symbiosis networks of ecoindustrial parks based on cascading failure model. *Mathematical Problems in Engineering,* 2013.
Zhan, Z., Xu, M. & Xu, S. 2013. Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *IEEE Transactions on Information Forensics and Security,* 8**,** 1775-1789.
Zhan, Z., Xu, M. & Xu, S. 2015. Predicting cyber attack rates with extreme values. *IEEE Transactions on Information Forensics and Security,* 10**,** 1666-1677.
Zhao, L., Lai, Y.-C., Park, K. & Ye, N. 2005a. Onset of traffic congestion in complex networks. *Physical Review E,* 71**,** 026125.
Zhao, L., Park, K. & Lai, Y.-C. 2004. Attack vulnerability of scale-free networks due to cascading breakdown. *Physical review E,* 70**,** 035101.
Zhao, L., Park, K., Lai, Y.-C. & Cupertino, T. H. 2007. Attack induced cascading breakdown in complex networks. *Journal of the Brazilian Computer Society,* 13**,** 67-76.
Zhao, L., Park, K., Lai, Y.-C. & Ye, N. 2005b. Tolerance of scale-free networks against attack-induced cascades. *Physical Review E,* 72**,** 025104.
Zhao, S., Liu, X. & Zhuo, Y. 2017. Hybrid Hidden Markov Models for resilience metrics in a dynamic infrastructure system. *Reliability Engineering & System Safety,* 164**,** 84-97.
Zheng, J., Okamura, H. & Dohi, T. 2015. Availability importance measures for virtualized system with live migration. *Applied Mathematics,* 6**,** 359.
Zhu, B., Joseph, A. & Sastry, S. A taxonomy of cyber attacks on SCADA systems. Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing, 2011. IEEE, 380-388.
Zhu, Q. & Başar, T. A dynamic game-theoretic approach to resilient control system design for cascading failures. Proceedings of the 1st international conference on High Confidence Networked Systems, 2012. ACM, 41-46.
Zhu, X., Fu, Y., Yuan, T. & Wu, X. 2017. Birnbaum importance based heuristics for multi-type component assignment problems. *Reliability Engineering & System Safety,* 165**,** 209-221.

Zhu, X., Yao, Q. & Kuo, W. 2012. Patterns of the Birnbaum importance in linear consecutive-k-out-of-n systems. *IIE Transactions,* 44**,** 277-290.

Zio, E. & Podofillini, L. 2003a. Importance measures of multi-state components in multi-state systems. *International Journal of Reliability, Quality and Safety Engineering,* 10**,** 289-310.

Zio, E. & Podofillini, L. 2003b. Monte Carlo simulation analysis of the effects of different system performance levels on the importance of multi-state components. *Reliability Engineering & System Safety,* 82**,** 63-73.

Zio, E. & Podofillini, L. 2006. Accounting for components interactions in the differential importance measure. *Reliability Engineering & System Safety,* 91**,** 1163-1174.

Zobel, C. W. Comparative visualization of predicted disaster resilience. Proceedings of the 7th International ISCRAM Conference, 2010. 1-5.

Zobel, C. W. 2011. Representing perceived tradeoffs in defining disaster resilience. *Decision Support Systems,* 50**,** 394-403.

Zobel, C. W. 2014. Quantitatively representing nonlinear disaster recovery. *Decision Sciences,* 45**,** 1053-1082.

Zobel, C. W. & Khansa, L. 2014. Characterizing multi-event disaster resilience. *Computers & Operations Research,* 42**,** 83-94.