# The Conceptual Framework of Resilience and its Measurement Approaches in Electrical Power Systems

**A. Shakeri Kahnamouei[1], T. Ghanizadeh Bolandi[2], M-R. Haghifam[3]**

[1,2,3] Faculty of Electrical and Computer Engineering, Tarbiat Modares University (TMU), Tehran, Iran

[1]ali.shakeri@modares.ac.ir

**Keywords:** Power Systems, Vulnerability, Resiliency, Risk.

## Abstract

The resilience assessment of complex and large-scale systems such as electrical power systems has becoming an inseparable part in analysing the reliable performance of the systems in the presence of high-impact, low-probability (HILP) incidents, such as extreme natural disasters. Considering the application of the resilience in various domains, the different definitions can be found for assessment of resilience in one system and several approaches can be applied to measure it. The necessity of increasing the resilience of power system infrastructures in response to HILP disasters for supplying at least emergency loads when facing unexpected and catastrophic events has becoming more and more clear. Reliability evaluation of power systems provides the likely behaviour of a system in normal condition but fails to model the high order contingencies which have low probabilities of occurrence. However, withstanding, absorbing and rapidly recovering from HILP events still remains a significant challenge which can be analysed in resilience assessment. This paper presents a conceptual framework of resilience domains and its measurement approaches, especially a thorough conceptual framework of resilience as a subcategory of vulnerability in electrical power systems. The conceptual difference between resilience and other indices of power system assessment such as reliability, risk and security are also presented in this research.

## 1 Introduction

One of the essential critical infrastructures (CIs) of modern societies is electrical power system. CIs compose the assets, systems, and networks, whether physical or virtual, that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Recent electrical wide-scale perturbations, such that mentioned in [1-4], have ascertained the impressive effect of power disruption on other CIs, such as telecommunications and transportation.

Given that performance of electrical power systems must be reliable during their normal operation and also when encountering known and foreseeable contingencies should guarantee a high-quality power supply to customers with few interruptions over a specific time period, they have been traditionally designed and driven by considering the key reliability principles, i.e., security and adequacy [5-7], which are well-known concepts. Additionally, risk management strategies focuses traditionally on reducing likelihood of disruptive incidents and the potential consequences of the event. Recent HILP events represented that not all the events can be prevented by conventional risk assessment methods. Therefore, the necessity of increasing the resilience of power infrastructures in response to HILP disasters for supplying at least emergency loads when facing unexpected and catastrophic events has becoming more and more apparent.

In this regard, resilience is an emerging concept that has not yet been adequately focused comparing other concepts of power systems such as reliability, security, or risk, especially in designing the power system infrastructures. Since the constitution of power system resilience is not still thoroughly clear, there is not a universal resilience definition which represents the new aforementioned concept of power systems that fills defects of previous well-known power system concepts. On these premises, a conceptual framework of resilience as a subcategory of vulnerability in electrical power systems is provided in this paper for assessing and bringing insights into power system resilience.

Resilience (or resiliency) has been originated from the Latin word “resiliere,” which means to “bounce back” and refers to the ability of an object or system to return to its original position or normal condition after being stressed or the occurrence of an event [8]. Such a broad definition applies to the wide range of fields such as ecology, materials science, psychology, economics and engineering. In the context of electrical power systems, resilience means the ability of a power system to rapidly recover from disruptive incidents such as HILP events, and to absorb lessons for adapting its performance for preventing the hazardous effects of similar events in the future. General application domains of resilience are presented as organizational, social, economic, and engineering. It’s worth to notice that this classification may vary depending on researcher’s perspective. Varity of definitions of resilience according to four aforementioned groups will be presented as the following sections. The rest of paper includes the following structure. Section 2 presents the different domains of resilience application, Section 3 conceptualizes power system resilience, and Section 4 provides a conceptual comparison of resilience with reliability, risk, and security. Section 5 classifies resilience assessment approaches. Finally, we provide concluding remarks in Section 6.

## 2 Different domains of resilience application

### 2.1 Organizational domain

Rapidly changing the business environment caused to emerge the concept of organizational resilience. In other words, enterprises saw the need to response for this changing and thus requirement of this concept was undeniable. Sheffi [9] defined the organizational resilience as "the intrinsic ability to maintain or restore a steady state, thereby leading it to continue normal performance after a disruption or in the presence of continuous stress". Vogus and Sutcliffe [10] definition of organizational resilience was "the ability of an organization to withstand the disturbance and enhance performance despite the presence of difficulty". In [11] resilience of companies was defined as "the company's ability to restore to their normal performance level following by disruptive event". The definition of resilience in the context of organizations proposed by McDonald [12] was "the ability to adapt to the provisions of the environment and manage the environment variation". The essential idea which was proposed by Patterson et al. [13] highlighted that boosting the organizational resilience could be made by collaborative cross-checking. They defined it as an improved resilience strategy in which at least two groups or individuals with different viewpoints inquire the others' activations to assess accuracy or validity. The privilege of implementing collaborative cross-checking is detection of erroneous actions quickly enough so adverse consequences can be mitigated.

### 2.2 Social domain

Resilience capacities of social concepts such as environment, individuals, and community are discussed in social domain of resilience. Adger [14] proposed definition of social domain of resilience as "ability of communities to deal with external stresses and disturbances as a result of social, political, and environmental change". Resilience definition presented by The Community and Regional Resilience Institute (CARRI) [15] is "the capability to predict risk, limit adverse consequences, and return rapidly through survival, adaptability, and growth in confronting with turbulent changes". In [16] definition of social resilience was proposed which is consists of three aspects, i.e., coping, adaptive, and transformative capacities. Also Cohen et al. [17] defined community resilience as "the ability of community to perform appropriately during disruptions". Generally, the most studies of resilience were done in the social domain and subdomains of social resilience as ecology, psychology, and sociology.

### 2.3 Economic domain

Several references have presented a definition for economic resilience. One of these definitions was proposed by Rose and Liao [19] which is "the inherent ability of firms that enables them to avoid maximum potential losses". Rose [20] defined static and dynamic economic resilience as "the capability of a system to continue its performance such as production when confronts with a severe shock", and "the pace at which a system recovers from a severe shock to achieve a steady state", respectively. Martin [21] proposed a more particular definition of economic resilience as "the capability to reconfigure its structure so as to sustain an appropriate growth path in output, employment and wealth over time".

### 2.4 Engineering domain

In comparison to other domains of resilience, engineering resilience is relatively a novel concept. Electrical power system is in the engineering domain of resilience. Youn et al. [22] defined engineering resilience as the collection of reliability and restoration. Hollnagel et al. [23] presented another definition of resilience as the ability to adjust functionality of the system in the presence of disruptions and unanticipated events. Both comprehending the normal functioning of a technical system and finding out how it fails are necessary for resilience engineering [24]. The definition of engineering resilience presented by the American Society of Mechanical Engineers (ASME) [25] is the ability of a system to withstand disruptions without losing its performance or, if the performance of the system is disrupted, rapidly recover to the normal condition. In [26] six factors that boost the resilience engineering of industrial processes are identified as minimization of failure, limitation of effects, administrative procedures, flexibility, controllability, and early detection.

### 2.5 Analysis of resilience definitions

The review of resilience definitions indicates that there is no universal accepted definition of resilience, however several similarities can be observed across these definitions. The main highlights of resilience definitions are summarized as follow aiming to give insight about the concept.
(i) According to some definitions, such as [9] and ASME [25], coming back to steady state level of performance for a system(e.g., infrastructure, community) which has been damaged due to a disaster, is needed for resilience, while from the view point of other definitions recovery is not included as a part of resilience, (ii) For engineering systems, such as electrical power systems, measurement of the ability for warding off the disruption has been done considering reliability as an essential feature, (iii) Haimes [27] defines resilience considering a multidimensionality to the quantification of resilience. From the view of this definition, all the states of a system are not inherently at the same level of resilience. Further, Haimes emphasizes threat-dependency as a factor of system resilience, (iv) Mechanisms to achieve resilience are not specified in some definitions; however, many of them define "absorption", "adaptation", and "recovery" as critical parts of resilience, (v) Some definitions such as Allenby and Fink [28], Pregenzer [29], and Adger [14] defined resilience in terms of preparedness (pre-disaster) activities, while the role of recovery (post-disaster) activities are ignored. Definitions presented by organizations such as National Infrastructure Advisory Council (NIAC) [30] considered both pre-disaster and post-disaster activities to achieve resilience, (vi) Some definitions such as Allenby and Fink [28], Pregenzer [29], and Adger [14], consider resilience

just in preparedness (pre-disaster) activities and omit one of the critical parts of resilience (recovery) from the definition. Discarding recovery as an essential post-disaster activity from the definition of resilience is an undeniable defect of these definitions.

## 3 Concept of power system resilience

The first definition of resilience was presented by Holling in 1973 as "the measure of permanence of systems and of the ability to absorb disruptions without changing the relationships between state variables". As noted, after the first definition of resilience, numerous interpretations of resilience have been developed, causing in many different definitions which results a lack of universal accepted definition of resilience.

In the context of power systems, resilience is a lately emerged concept. There have been several attempts for distinguishing the concept of resilience from reliability. Some organizations such as the Cabinet Office, U.K., the U.S. Power Systems Engineering Research Centre (PSERC), the U.K. Energy Research Centre (UKERC), and the National Infrastructure Advisory Council (NIAC) have defined resilience to achieve this goal. For instance, the Cabinet Office, U.K. [31] defines resilience of a CI as the ability to "anticipate, absorb, adapt to and/or rapidly recover from a disruptive event". According to the Cabinet Office, the main attributes of a resilient CI are resistance, reliability, redundancy, and response/recovery. According to UKERC, "Resilience is the capacity of an energy system to tolerate disturbance and to continue to deliver affordable energy services to consumers. A resilient energy system can speedily recover from shocks and can provide alternative means of satisfying energy service needs in the event of changed external circumstances." Or The NIAC definition of resilience is "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event." Multidisciplinary and National Centre for Earthquake Engineering Research (MCEER) has developed a generic resilience framework which can be applied to any CI, including electrical power systems. This framework comprises of the "4Rs": robustness, redundancy, resourcefulness, and rapidity. In this regard, the NIAC has proposed a construction for resilience which is based on for features that are mentioned here briefly.

(i) Robustness – the ability to absorb shocks and continue operating. Designing structures or systems to be strong enough when occurring foreseeable contingencies is in domain of robustness. Moreover, robustness sometimes requires devising substitutes or redundant systems to play its role in resilient systems. Additionally, investing in and maintaining elements of CIs should be entailed to withstand HILP events, (ii) Resourcefulness – the ability to skilfully manage a crisis as it unfolds. There are three parts that play critical roles in this domain of resilience: (1) identifying options, (2) prioritizing actions to control damage and mitigate its consequences, and (3) communicating decisions to the people who will implement them. Resourcefulness depends on people rather than technology, (iii) Rapid recovery – the ability to get services back ASAP. As the previous part, rapid recovery also has three crucial parts: (1) carefully prepared contingency plans, (2) proper emergency actions, (3) the needed means to get the right people and resources to the right places, (iv) Adaptability – the ability to incorporate lessons learned from past events to improve resilience. It contains actions such as revising plans, modifying procedures, and using new tools and technologies to improve capabilities of the other part before the next crisis.

Figure 1 represents the sequence of the NIAC resilience construct. Robustness includes measurements prior to an event; measures taken as a crisis unfolds are in domain of resourcefulness; rapid recovery includes the post-disaster measures taken immediately after an event to lead the system to normal operation; and adaptability includes the lessons learned to modify the plans for the next contingency.

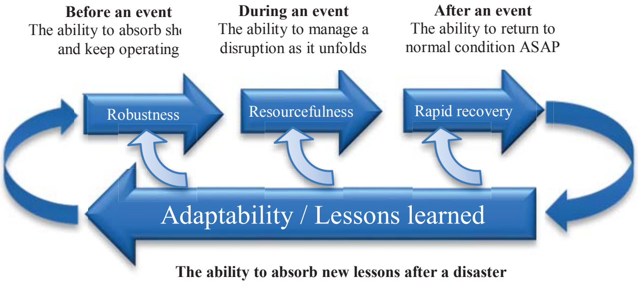

Figure 1: The sequence of the NIAC resilience construct

The baseline of resilience practices organized within the NIAC resilience framework for the electrical power systems, generated some essential goals which are: (i) withstanding a disaster with no loss of critical functions, (ii) preventing cascading power disruption in interconnected electrical power systems, (iii) minimizing the duration and magnitude of power disruptions through rapid recovery strategies, and (iv) reducing future risks by incorporating lessons from past experiences.

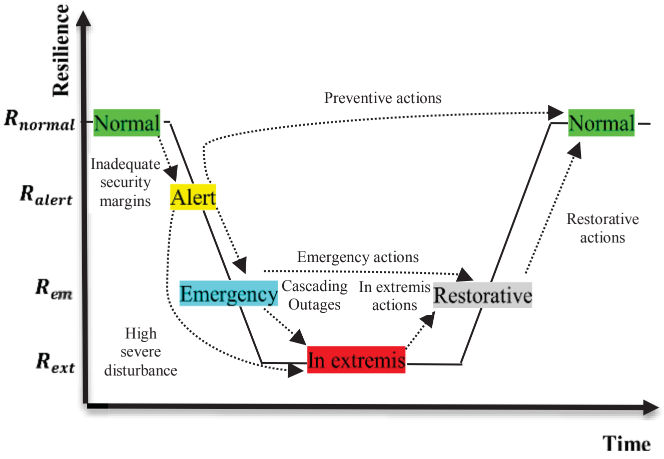

Figure 2: Conceptual resilience curve [60]

The main objective of electrical power systems is delivering uninterrupted electricity to the customers. When occurring HILP events, the priorities are to (i) maintain real-time integrity of the bulk power system (to avoid the cascading outages and blackout), and (ii) protect the generation and transmission equipment from catastrophic damage.

A conceptual resilience curve associated with an event is illustrated in figure 2 [60]. This illustration shows resilience as a function of time respecting catastrophe for instance, a heavy storm moving across the system. The key resilience features that an electrical power system must possess to cope effectively with the changing conditions associated to an event are illustrated in this figure.

### 3.1 Resilience as a subcategory of vulnerability

Several connotations are with the term "vulnerability". McCarthy (2001) reflected this view within the context of climate change. Exposure to a range of effects is most often considered as the definition of the concept of vulnerability. Kroger and Zio [61] defined vulnerability as "a flaw or weakness (inherent characteristic, including resilience capacity) in the design, implementation, operation, and/or management of a CI, or its components, that presents it susceptible to demolition or incapacitation when exposed to a hazard or threat, or reduces its capacity to resume new stable conditions". In the context of electrical power system, vulnerability is specified in terms of changes in network characteristics following attacks on nodes and the scale or the duration of the associated loss. In other words, it can be expressed in terms of the frequency of the major blackouts and the associated severity, measured either in power loss or energy unsaved. Figure 3 represents vulnerability elements and associated response scenarios.

Also the position of resilience studies in electrical power systems is shown in figure 4.

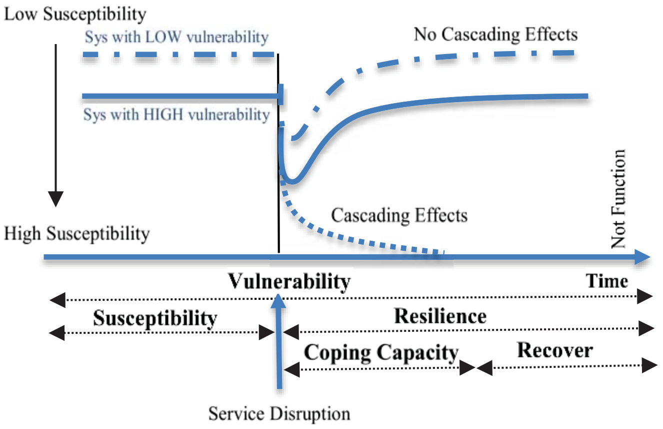

Figure 3: Vulnerability elements and associated response scenarios [61]

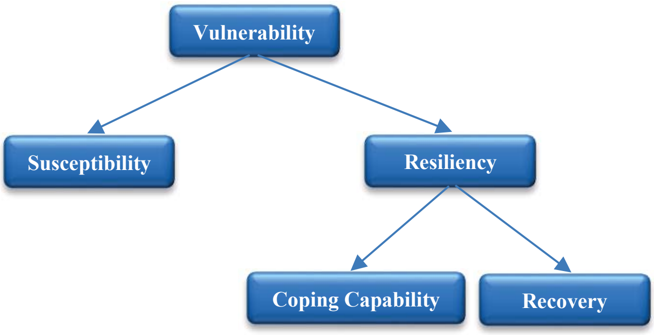

Figure 4: Position of resiliency studies

### 3.2 A conceptual framework of long-term and short-term resilience

It can be understood from the aforementioned resilience definitions that resilience is a time dependent concept. Given the dependency of resilience on time, it can be subcategorized as long-term and short-term resilience. The key features that a resilient power system must have before, during, and after a HILP event, i.e., robustness/resistance, resourcefulness/redundancy, and recovery, respectively, are in the domain of short-term resilience. The ability of the system operators in comprehending the received information and data, detecting the problem, setting priorities, identifying the available resources, and then applying the best measures to restore the system to a resilient state determines the effectiveness of the preventive and corrective actions. Adaptability of a CI to new threats and conditions is in the domain of long-term resilience. Adaptability can be achieved via immense risk and reliability studies in electrical power systems.

The short-term resilience of an electrical power system depends on its either ability to cope with changing conditions effectively and rapidly or ability to reduce the effect of the disruption. Recognizing the position of resilience in the power system studies, Fink and Carlsen [32] utilized the possible states of a power system based on the security margins, which are normal, alert, emergency, in extremis, and restorative. In the context of resilience, every power system state correspond to a different degree. Figure 2 represents the conceptual resilience curve and also correspondence of system states with resilience concept.

During the normal state, due to satisfaction of all the operational constraints and adequacy of the security margins, the resilience of the system, i.e., $R_{normal}$ is high. Therefore the robustness/resistance of the system would be enough to cope with a HILP event. However, entering the system to the alert state may cause inadequacy of security margins ($R_{alert}$). In this condition, the system operators should restore the system to normal state by applying preventive control actions immediately. Otherwise, if a disturbance occurs in this state, depending on the severity of the disturbance, the system enters the emergency or in extreme state. When the system enters the emergency or in extreme states, due to lack of resistance to new disruptions, the system resilience, i.e., $R_{em}$ and $R_{ext}$, respectively, decreases. The key resilience features at this stage are resourcefulness and redundancy which can mitigate the disturbance's consequences with applying emergency actions and enabling quick recovery of the system. Afterwards, the disturbance's causes and impact have to be assessed to provide adaptability to new threats. Then, the short-term resilience attributes of the system would be enhanced for dealing with this situations in the future. Figure 5 represents a conceptual long-term resilience framework.

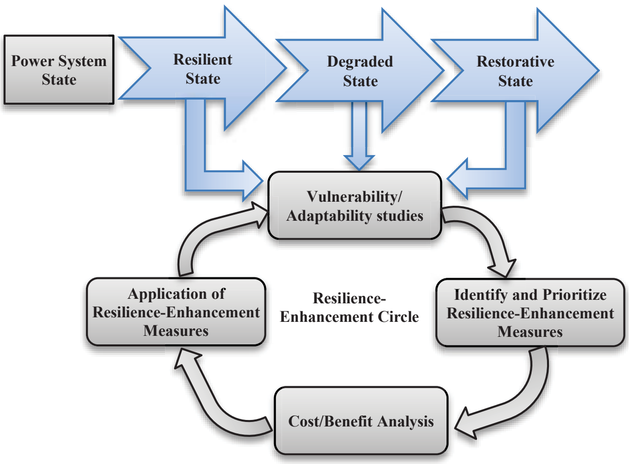
Power System State
Resilient State
Degraded State
Restorative State
Vulnerability/ Adaptability studies
Application of Resilience-Enhancement Measures
Resilience-Enhancement Circle
Identify and Prioritize Resilience-Enhancement Measures
Cost/Benefit Analysis

Figure 5: A conceptual long-term resilience framework [62]

### 3.3 Enhancing the resilience of power systems

The necessity of taking actions to boost power system resilience to HILP events is getting more and more obvious due to the critical effect of such events on power systems. For example, extreme weather events such as high temperatures, high winds, heavy snow and ice accumulation, lightning strikes, and floods can cause the failure of key components of the system, as discussed in [33] and [34]. Electrical utilities attempt to achieve system adaptation and survivability to achieve this aim. With high system adaptation, the impact of future events will be mitigated, and also high system survivability will maintain adequate functionality of the system during and after the disaster. These two resilience purposes can be fulfilled through hardening and operational measures. Hardening measures are actions in which make the power system less susceptible to HILP events. In contrast, operational measures are actions in which provide the asset with control capability and resources to effectively deal with the emergency. According to [62], "the goal of the operational measures is to make the system "bend," rather than "break," in the face of a disaster". Hardening measures lead the power system to be stronger, while operational measures lead it to be smarter. There are six helpful hardening measures which can make the system stronger and so it will be more resilient. These measures are: (i) moving distribution and transmission lines underground, (ii) elevating substations, (iii) rerouting transmission lines to areas less affected by weather, (iv) upgrading poles and structures with stronger, more robust materials, (v) relocating facilities to areas less prone extreme weather, (vi) redundant transmission routes by building additional transmission facilities. Operational measures or in other words, for making the system smarter, could be achieved through several manners such as distributed energy systems and decentralized control, microgrids and disaster response and risk management.

## 4 Conceptual comparison of resilience, reliability, risk, and security

In this section, we attempted to comprise the main well-known concepts of power systems, i.e., reliability, risk, and security, with resilience.

### 4.1 Reliability

In discussions related to reliability, several terms such as security, risk, vulnerability, and robustness are used. Reliability is often used to encompass all of these, representing an expected level of system services over a period of time (often measured annually) [63]. Reliability is one of the well-known concepts of power system and numerous reliability studies of power system have been developed in the last decade. According to NERC, reliability is the elements performance of the power system in which electricity is delivered to customers with existing standards and desired amount. Reliability measurement may be done through duration, frequency, and damaging effects magnitude on the electric supply. Two practical aspects of reliability of power system is adequacy (the ability of the power system to supply the total energy and demands of the customers continuously, considering scheduled and expected unscheduled disruptions of elements of the system) and security (the ability of the power system to tolerate sudden disruptions such as unexpected loss of system elements). As aforementioned, for supplying the customers' needed load at any conditions, the power system not only should be reliability-oriented, to deal with foreseeable threats, but also resiliency-oriented, to deal with unexpected HILP events, such as the extreme weather phenomena.

In the context of electricity, the measurement approach of reliability is often different at the distribution and transmission/generation level. At the distribution level, the System Average Interruption Frequency Index (SAIFI) and the System Average Interruption Duration Index (SAIDI) are the most useful reliability indices [35]. SAIFI and SAIDI represent the average frequency of outages per customer and the average duration of outages, over a specified period (often one year), per customer, respectively. At the bulk level (e.g. transmission), a common reliability metric is loss of load expectation (LOLE) which is the expected amount of electric energy demand that goes unserved over a specified period.

After identifying reliability metrics, there is a conceptual question about measurement of resilience. The question is "What's wrong with just applying duration and frequency metrics to resilience?". If we want to measure resilience with reliability metrics, there will be conceptual errors. Because those metrics miss two components: (i) they often concentrate on normal operating conditions and thus the impact of large-scale events would be undervalued, and (ii) they price lost load at a flat rate while in the concept of resilience it can't be true. Table 1 represents distinguishing characteristics of resilience and reliability.

Table 1: Reliability versus resilience ([62])

| Reliability | Resilience |
|---|---|
| High probability, low impact | Low probability, high impact |
| Static | Adaptive, ongoing, short and long term |
| Evaluates the power system states | Evaluates the power system states and transition times between states |
| Concerned with customer interruption time | Concerned with customer interruption time and the infrastructure recovery time |

### 4.2 Risk

There is considerable overlap in the words "risk" and "reliability." In other words, they are the two representations of the same fact. Higher risk means lower reliability, and vice versa. A dictionary definition of risk is "the probability of loss or damage to human beings or assets". This definition can be utilized in general cases. The risk evaluation of power systems should identify not only the likelihood of failure events but also the severity and degree of their consequences. According to [36], risk is the exposure to the possibility of adverse circumstances such as loss and injury. In the context of risk analysis, risk is often more formally defined as [63]:

$$Risk = Exposure \times Vulnerability \times Cost \qquad (1)$$

Exposure represents that how the system is exposed to potential hazards. In other words, exposure is the probability that a particular object or system will be contacted by a hazard. In this context, vulnerability is the probability of an object failure, given that it is contacted by a hazard. Exposure and vulnerability can compound into an overall probability which shows the failure probability of the system. Cost represents the total system cost resulting from the failure of a component or system.

Risk assessment metrics have the same defects of reliability metrics that described above. The main problem of these metrics that is worth noting is that, they don't consider high impact and low probability hazards. So resilience metrics should overcome this problem and thus using reliability or risk assessment approaches will not satisfy the resilience concept.

### 4.3 Security

As noted, conventional reliability metrics such as LOLE are scalar values. The trouble with these scalar values is that they can obscure risk from HILP events, such as an extreme weather event. When a system withstands low probability events, it is labelled as "secure," or more secure. However, security has a very specific meaning in electrical power systems. If operating limits (typically voltage limits at nodes, and flow limits on transmission links) of a power system is not violated following a single component failure, it's said to be secure. This is congruent with the general concept of security only if there is no chance of multiple components failing in close temporal proximity. However, when occurring HILP events, typically result in several outages nearly simultaneously. As a result, expressing a power system secure does not mean that it is particularly resistant to HILP events.

## 5 Classification of resilience assessment approaches

Generally, the resilience assessment approaches can be categorized into two major groups: qualitative and quantitative. Each of these two major categories contains several sub-categories. Assessing the resilience of system with qualitative indices and not utilizing quantitative indices is in qualitative domain of the resilience assessment approach. The qualitative approach of resilience assessment includes two sub-categories, i.e., conceptual frameworks, and semi-quantitative indices. Also, quantitative domain of the resilience evaluation includes two sub-categories: (i) general resilience approaches, and (ii) structural-based modelling approaches. Figure 6 represents the classification of resilience evaluation approaches. It's worth mentioning that, this classification is generally developed and not only can be utilized for power systems but also contains measurements of other domains of resilience.

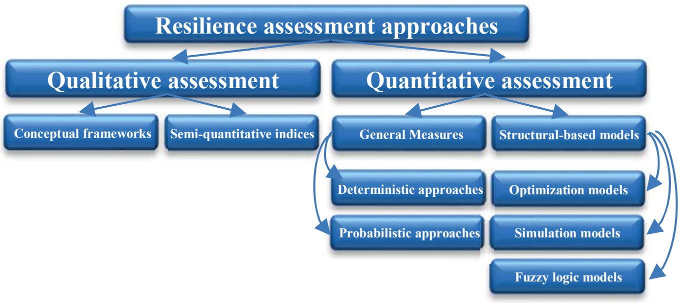

Figure 6: Classification scheme of resilience assessment approaches

### 5.1 Qualitative assessment approaches

In this section, the qualitative resilience assessment approaches categorized as conceptual frameworks and semi-quantitative indices are highlighted.

### 5.1.1 Conceptual frameworks

Constitution of majority of the qualitative approaches for assessing the system resilience are classified as conceptual frameworks. Collection of proposed frameworks for this part are presented briefly. We tried to highlight the best frameworks. A generic framework proposed by Alliance [37] which has been designed to evaluate the resilience of social-ecological systems, has composed of seven steps: (i) understanding the system, (ii) recognizing appropriate scale for resilience assessment, (iii) identifying all the types of disruptions of the system, (iv) recognizing the important players of the system, (v) defining critical recovery activities, (vi) implementing the results of step 5, and (vii) combining the findings of the step 6. Reference [38] developed a framework for analysing resilience of the "resources that people have and the strategies they adopt to make a living." The framework provides a few characteristics of three dimensions of resilience: buffer capacity (the amount of change that a system can tolerate), self-organization (the emergence of society through inherent social structure), and capacity for learning (an ability to adapt). Eight guiding principles of conceptual framework of system resilience proposed by [39] are: (i) threat evaluation, (ii) robustness, (iii) outcome reduction, (iv) adaptability, (v) risk-informed planning, (vi) risk-informed investment, (vii) goals harmonization, and (viii) universal scope. Labaka et al. [40] suggested a thorough resilience framework with close collaboration with general management. There are several qualitative resilience studies which have addressed CI applications. Sterbenz et al. [41] proposed a framework for resilience of a specific CI that provides only a conceptual understanding and does not assess system resilience and also they suggested a study that consists of resilience disciplines. The outcomes of their study represent that six factors of defend, detect, diagnose, remediate, refine, and recover chip in designing resilient networks that can be utilized in other domains. In a similar work, properties of resilience in a specific context were identified by [42]. According to their work, reliability, integrity, performance, availability, safety, maintainability, and confidentiality are the key properties of resilience. Reference [43] proposed three influential factors to achieve resilience in medication delivery which are advanced techniques for visualization of information, assessment of remedy, and teamwork during the extraction of necessities.

Resilience was introduced as function of absorptive capacity, adaptive capacity, and restorative capacity in [44]. Absorptive capacity is in the domain of preparedness activities and is the ability of a system to attract shocks arising from disruption, adaptive capacity is in the domain of recovery activities and is the ability of a system to adapt itself to new conditions, and restorative capacity is also in the domain of recovery activities and represents the system restoration ability when adaptive capacity is not able to effectively play its role. A unique feature of this definition that distinguish it from others is about introducing resilience cost index (RCI), which is composed of two elements: loss costs arising from disruptive events, and recovery costs. Shirali et al. [45] introduced the main obstacles of achieving resilience in a chemical process as a lack of experience about resilience engineering, intangibility of resilience engineering level, preference of production over safety, shortage of reporting system, religious beliefs, and out-of-date procedures and manual, poor feedback loop, and economic problems. A community resilience framework for an area which is exposed to earthquake was proposed by [46] which comprises: (i) identifying hazard/disaster attributes, (ii) determining vulnerability, (iii) risk admission and awareness preparedness, and (iv) finally improving social, economic, and physical resources.

### 5.1.2 Semi-quantitative indices

The semi-quantitative index approach is usually developed with a questionnaire designed to evaluate resilience of a system on a Likert (0 to 10) or percentage scale (0 to 100) [8]. For creating an index of resilience, evaluation of the characteristics from expert opinion are aggregated in some way. For instance, Cutter et al. [47] first identified several resilience variables, including redundancy, resourcefulness, and robustness. Then, each variable was scored between 0 and 100 according to the data observation from a government source. These variables were categorized into some sub-indices such as economic and social. Unweighted average method was used to calculate the score of each sub-index and subsequently, the total score. Pettit et al. [48] proposed the two vital drivers of resilience in an operation, i.e., vulnerability and capability of the operation to absorb the disaster and restore from it. The authors measured these drivers by a set of questions. The importance of each factor was weighted by policymakers, and finally the responses to the questions were calculated using the weighted sum approach. Reference [49] introduced six resilience indicators such as awareness and flexibility to evaluate resilience engineering using this approach.

## 5.2 Quantitative assessment approaches

In this section, quantitative resilience assessment approaches are classified and each approach will be described.

### 5.2.1 General measures

Regardless of the structure of system, resilience assessment of a system by measuring its performance is provided by general resilience measures. Generic resilience metrics compare the pre-disaster and post-disaster performance of system without focusing on its specific attributes. These general measures could be categorized as deterministic and stochastic, each of which have been used to describe static and dynamic system behaviour.

- Deterministic vs. probabilistic: Deterministic approach does not consider uncertainty when assessing resilience. In contrast, probabilistic approach determines stochasticity associated with system behaviour.
- Dynamic vs. static: A dynamic resilience approach accounts for time-dependent behaviour, while a static resilience approach is free of time dependent measures of resilience.

#### 5.2.1.1 Deterministic approaches

Reference [50] proposed four dimensions for resilience in the resilience triangle: (i) robustness, (ii) rapidity, (iii) resourcefulness, and (iv) redundancy. Then, for assessing the loss of resilience, they suggested a deterministic static approach. Equation (2) represents their approach. $t_0$ is the time at which the disaster happens, and $t_1$ is the time at which the community returns to its pre-disaster condition. Also, $Q(t)$ indicates the quality of the CI at time $t$.

$$RL = \int_{t_0}^{t_1} [100 - Q(t)]dt \qquad (2)$$

In figure 7, the area which represents RL was specified. The significant advantage of this method is its general applicability. Although this approach is used for a specific context, given that quality is a general concept, it can be extended to other domains of resilience such as electrical power systems. As such, an essential privilege of resilience triangle metric is its general applicability. This metric assumes that pre-disaster quality of community infrastructure is 100% which is considered optimistically and somehow unrealistic.

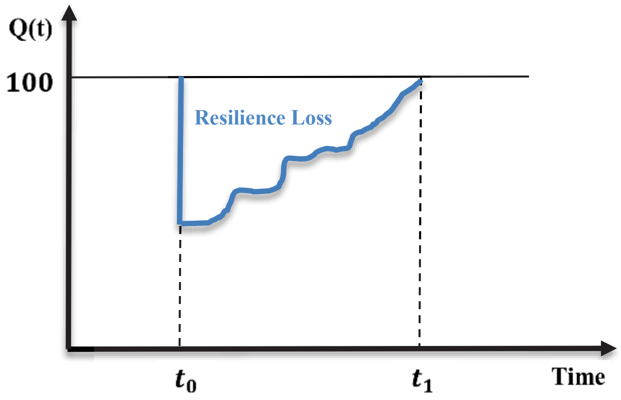

Figure 7: Resilience loss measurement from the resilience triangle ([50])

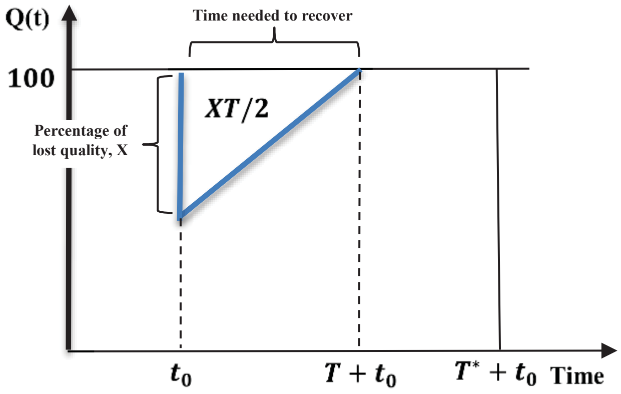

Figure 8: Reinterpretation of the resilience triangle ([51])

Application of the resilience triangle paradigm is widely general and could be utilized in several contexts. For instance, Zobel [51] proposed a metric by "calculating the percentage of the total possible loss over some suitably long time interval $T^*$" as shown in Equation (3). $X \in [0,1]$ is the percentage of loss of operation after a disaster, $T \in [0, T^*]$ is the time needed for full recovery, and $T^*$ is the time interval to determine lost operation. Zobel proposed that different compounds of $X$ and $T$ can give the same level of resilience which is obtained from resilience triangle. Then, a visualization of the trade-offs between lost functionality and recovery time for the same level of "resilience" was provided.

$$R(X, T) = \frac{T^* - XT/2}{T^*} \qquad (3)$$

In figure 8 it is represented that for a single disaster, the total possible loss can be obtained as triangle area ($XT/2$). Afterwards, the metric in Equation (3) was extended by in [52]. Although linear recovery of the proposed model is somehow optimistic and maybe away from reality, its privilege is its simplicity. Further, the conceptual illustration of resilience shown in Figure 8 proposed that performance mitigation after a disruptive event is immediate which could not be true for all the systems.

#### 5.2.1.2 Probabilistic approaches

Reference [53] is an instance of probabilistic approaches for evaluating resilience. According to [8], when assessing resilience with probabilistic approaches, resilience is defined as "probability of performance loss of the initial system being less than the maximum acceptable performance loss after a disruption and the time to full recovery being less than the maximum acceptable disruption time".

Equation (4) represents this measure where $A$ is the set of performance standards, $r^*$ shows maximum acceptable performance loss of system, $t^*$ represents maximum acceptable recovery time, and i is the disruption magnitude.

$$R = P(A|i) = P(r_0 < r^* \text{ and } t_1 < t^*) \qquad (4)$$

Although this approach was applied to measure the resilience of CIs following an earthquake, application of the metric is not limited to this case and can be generally applied to any other systems and disruptions. Acknowledgment of uncertainty in resilience measurement is the distinguishing feature of this approach. However, the defect of the proposed metric is lack of extra penalty for exceeding the maximum acceptable values of both performance loss and length recovery.

### 5.2.2 Structural based models

In this section, the impact of structure of a system on its resilience is examined through structural-based procedures. Accomplishing this aim requires observation of system behaviour and also modelling and simulating of characteristics of the system is needed. Structural based models are specified with three approaches: optimization models, simulation models, and fuzzy logic models.

#### 5.2.2.1 Optimization models

There are several works about optimization models of resilience assessment that we are going to describe two of them and mention the others' references. One of the best works of this section was done by Faturechi et al. [54] that aimed to maximize the resilience of an airport's runway and taxiway network. They proposed a mathematical model for assessing and optimizing airport resilience. Quick restoration of post-event take-off and landing capacities to the level of pre-event capacities is the main strategy of their mathematical model which takes into account time, physical, operational, space, resource, and budget restrictions. They considered two types of decision variables including pre-disruption and post-disruption decisions. Taking into account the preparedness and recovery activities in the stochastic integer model is the privilege of their work.

Another optimization model has been proposed by [55] which is a multi-objective, three stage stochastic mathematical model to quantify and optimize resilience of travel time in road networks. The three stage of decision process comprise: (i) pre-disruption reduction, (ii) preparedness, and (iii) post-disruption response. The resilience of the road network is defined as "network's ability to withstand and adapt to a disruption, with travel time utilized to evaluate resilience". Minimizing the total travel time and maximize the expectation of road network resilience over all possible disruption scenarios simultaneously is their objective function.

#### 5.2.2.2 Simulation models

Assessment of preparedness of a fire and rescue service department when occurring a hazardous threat was proposed by Albores and Shaw [56] which is a discrete event simulation model. In this model, preparedness is considered as key driving factor of pre-event disruption resilience. There were two simulation models: (i) the first model emulates the mass decontamination of population following a terrorist attack, while (ii) the second model deals with the harmonization of resource allocation across regions.

As another simulation model, Virgina et al. [57] suggested a dynamic simulation approach for simulating supply chain resilience. In this instance also, preparedness, responsiveness, and recovery are considered as essential elements of resilience. They utilized the Integral of Time Absolute Error (ITAE) as measure of resilience. The objective of simulation model is capturing the minimum value of ITAE which is corresponding to the best response and recovery with lowest deviation from the target level following by disruption.

#### 5.2.2.3 Fuzzy logic models

One of the examples of utilizing fuzzy model in resilience was proposed by Aleksic et al. [58]. Their model was utilized in organizational domain of resilience. In their model, fuzzy variables were used for expressing the importance of the factors of organizational resilience.

A fuzzy cognitive map (FCM) is used by [59] to evaluate the factors of engineering resilience. Describing the casual reasoning between nine factors of engineering resilience was done by utilizing a FCM. These nine factors are teamwork, preparedness, redundancy, awareness, reporting, learning culture, flexibility, management commitment, and fault tolerance. A fuzzy graph structure can represent a FCM and also it can be obtained as a consequence of neural network and fuzzy logic approaches.

## 6 Conclusion

Designing the power infrastructure which is reliable to known and foreseeable threats, and resilient to the high-impact low probability events is very challenging. To achieve this aim, we need first to have a deep understanding of what resilience is. Over the past decade, the significance of the concept of resilience has been well recognized among researchers and practitioners. Effort has been devoted to measure the resilience of engineering systems, but challenges still exist.

We presented a thorough conceptual framework of resilience, not only in power system but also in other domains of resilience. Then, several definitions of resilience in power system were presented which proved lack of universal accepted unique definition of resilience.

Reliable systems cannot defend HILP events and in presence of large-scale disasters may lead the system to cascading outages and subsequently the blackouts. Conceptual differences of the well-known indices such as reliability, risk, and security were discussed and then resilience assessment approaches were thoroughly presented.

## References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations", U.S. Dept. Energy, Washington, DC, USA, Apr. (2004).

[2] UCTE, "Interim report of the investigation committee on the 28 September 2003 blackout in Italy", Brussels, Belgium, Oct. (2003).

[3] UCTE, "Final report system disturbance on 4 November 2006", Brussels, Belgium, (2007).

[4] FERC and NERC, "Arizona–Southern California outages on September 8, 2011: Causes and recommendations", Washington, DC, USA, Apr. (2012).

[5] NERC, "Reliability Standards for the Bulk Electric Systems of North America", Swindon, U.K., May (2014).

[6] NERC, "State of Reliability", Swindon, U.K., May (2013).

[7] UCTE, "UCTE Operational Handbook", Paris, USA, (2004).

[8] S. Hosseini, K. Barker, J. E. Ramirez-Marquez. "A review of definitions and measures of system resilience", *Reliability Engineering & System Safety*, 145, pp. 47-61, (2016).

[9] Y. Sheffi, "The resilience enterprise: overcoming vulnerability for competitive enterprise", *MIT Press*, Cambridge, MA, (2005).

[10] T. J. Vogus, K. M. Sutcliffe, "Organizational resilience: toward a theory and research agenda", *IEEE International Conference on Systems, Man and Cybernetics*, 34, pp. 18-22, (2007).

[11] Y. Sheffi, "Resilience reduces risk. Logistics quarterly", 12(1), (2006).

[12] N. McDonald, “Organisational resilience and industrial risk”, In: E. Hollnagel, D.D. Woods, N. Leverson, eds. “Resilience engineering: Concepts and precepts”, *Ashgate Publishing Company*, USA, pp. 155-179, (2010).

[13] E. S. Patterson, D. D. Woods, R. I. Cook, M. L. Render, “Collaborative cross-checking to enhance resilience”, *Cognitive, Technology & Works*, 9(3), pp. 155-162, (2007).

[14] W. N. Adger, “Social ecological resilience: are they related?”, *Progress in Human Geography*, 24(3), pp. 347-64, (2000).

[15] “Community and Regional Resilience Institute (CARRI) Research Report 8, Economic resilience to disasters”, (2009).

[16] M. Keck, P. Sakdapolrak, “What is social resilience? Lessons learned and ways forward”, *Erdkunde*, 67(1), pp. 5-19, (2013).

[17] O. Cohen, D. Leykin, M. Lahad, A. Goldberg, L. Aharonson-Daniel, “The conjoint community resiliency assessment measure as a baseline for profiling and predicting”.

[18] B. Pfefferbaum, D. Reissman, R. Pfefferbaum, R. Klomp, R. Gurwitch, “Building resilience to mass trauma events”, In L. Doll, S. Bonzo, J. Mercy, & D. Sleet (Eds.), “Handbook on injury and violence prevention interventions”, New York: *Kluwer Academic Publishers*.

[19] A. Rose, S. Y. Liao, “Modelling regional economic resilience to disasters: a computable general equilibrium analysis of water service disruptions”, *Journal of Regional Science,* 45(1), pp. 75-112, (2005).

[20] A. Rose, “Economic resilience to natural and man-made disasters: multidisciplinary origins and contextual dimensions”, *Environmental Hazard*, 7(4), pp. 383-98, (2007).

[21] R. L. Martin, “Regional economic resilience, hysteresis and recessionary shocks”, *Journal of Economic Geography*, 12, pp. 1-32, (2012).

[22] B. D. Youn, C. Hu, P. Wang, “Resilience-driven system design of complex engineered systems”, *Journal of Mechanical Design*, 133(10), (2011).

[23] E. Hollnagel, D. D. Woods, N. Leveson, “Resilience Engineering: concepts and precepts”, *Ashgate, Aldershot*, UK, (2006).

[24] E. Hollnagel, “Prologue: The scope of resilience engineering. Resilience Engineering in Practice: A Guidebook”, *Ashgate Publishing Company*, USA, (2010).

[25] “American Society of Mechanical Engineers (ASME) Innovative Technological Institute (ITI)”, Washington, D.C., *ASME ITI*, LLC, (2009).

[26] L. T. Dinh, H. Pasman, X. Gao, M. Sam Mannan, “Resilience engineering of industrial processes: principles and contributing factors”, *Journal of Loss Prevention in the Process Industries*, 25, pp. 233-241, (2012).

[27] Y. Y. Haimes, “On the definition of resilience in systems”, *Risk Analysis*, 29(4), pp. 498-501, (2009).

[28] B. Allenby, J. Fink, “Social and ecological resilience: Toward inherently secure and resilient societies”, *Science*, 24(3), pp. 347-64, (2000).

[29] A. Pregenzer, “Systems resilience: A new analytical framework for nuclear non-proliferation”, Albuquerque, NM, Sandia National Laboratories, (2011).

[30] National Infrastructure Advisory Council (NIAC), “Critical Infrastructure Resilience: Final Report and Recommendations”, (2009).

[31] Cabinet Office, “Keeping the country running: Natural hazards and infrastructure”, London, U.K., Oct. (2011).

[32] L. H. Fink, K. Carlsen, “Operating under stress and strain,” *IEEE Spectr.*, 15(3), pp. 48–53, Mar. (1978).

[33] D. Ward, “The effect of weather on grid systems and the reliability of electricity supply”, *Climate Change*, 121(1), pp. 103-113, Nov. (2013).

[34] U. G. Knight, “Power Systems in Emergencies: From Contingency Planning to Crisis Management”, *Hoboken*, NJ, USA, Wiley, (2001).

[35] P1366/d8, mar 2012 – “IEEE draft guide for electric power distribution reliability indices”, Online: http://ieeexplore.ieee.org/servlet/opac?punumber=6194243, March (2012).

[36] “New Oxford American Dictionary”, *Oxford University Press*, USA, (2010).

[37] Resilience Alliance, “Assessing resilience in social ecological systems: A practitioner’s workbook”, (2007).

[38] C. I. Speranza, U. Wiesmann, S. Rist, “An indicator framework for assessing resilience in the context of social-ecological dynamics”, *Global Environmental Change*, 28, pp. 109-19, (2014).

[39] J. H. Kahan, A. C. Allen, J. K. George, “An operational framework for resilience”, *Journal of Homeland Security and Emergency Management*, 6(1), pp. 1-48, (2009).

[40] L. Labaka, J. Hernantes, J. M. Sarriegi, “Resilience framework for critical infrastructures: An empirical study in a nuclear plant”, *Reliability Engineering and System Safety*, 141, pp. 92-105, (2015).

[41] J. P. G. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbar, J. P. Rohrer, “Modelling and analysis of network resilience”, *Proceeding of IEEE COMSNETS*, Bangalore, India, (2011).

[42] P. Vlacheas, V. Stavroulaki, P. Demestichas, S. Cadzow, D. Ikonomou, S. Gorniak, “Towards end-to-end network resilience”, *International Journal of Critical Infrastructure Protection*, 6(3-4), pp. 159-78, (2013).

[43] E. S. Patterson, D. D. Woods, E. M. Roth, R. I. Cook, L. Robert, R. L. Wears, M. L. Render, “Three key levers for achieving resilience in medication delivery with information technology”, *Journal of Patient Safety*, 2(1), pp. 33-38, (2006).

[44] E. D. Vugrin, D. E. Warren, M. A. Ehlen, “Framework for infrastructure and Economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane”, *Process Safety Progress*, 30(3), pp. 280-290, (2011).

[45] G. H. A. Shirali, M. Motamedzade, I. Mohammadfam, V. Ebrahimipour, A. Moghimbeigi, “Challenges in

building resilience engineering (RE) and adaptive capacity: a field study in a chemical plant", *Process Safety and Environmental Protection*, 90, pp. 83-90, (2012).

[46] S. Ainuddin, J. K. Routray, "Community resilience framework for an earthquake prone area in Baluchistan", *International Journal of Disaster Risk Reduction*, 2, pp. 25-36, (2012).

[47] S. L. Cutter, M. Berry, C. Burton, E. Evans, E. Tate, J. Webb, "A place based model for understanding community resilience to natural disasters", *Global Environmental Change*, 18(4), pp. 598-606, (2008).

[48] T. J. Pettit, J. Fiksel, K. L. Croxton, "Ensuring supply chain resilience: Development of a conceptual framework", *Journal of Business Logistics*, 31(1), pp. 1-21, (2010).

[49] G. A. Shirali, I. Mohammadfam, V. Ebrahimpour, "A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry", *Reliability Engineering and Systems Safety*, 119, pp. 88-94, (2013).

[50] M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, D. V. Winterfeldt, "A framework to quantitatively assess and enhance the science the seismic resilience of communities", *Earthquake Spectra*, 19(4), pp. 733-52, (2003).

[51] C. W. Zobel, "Representing perceived trade-offs in defining disaster resilience", *Decision Support Systems*, 50(2), pp. 394-403, (2011).

[52] C. Zobel, L. Khansa, "Characterizing multi-event disaster resilience", *Computers & Operations Research*, 42, pp. 83-94, (2014).

[53] S. E. Chang, M. Shinozuka, "Measuring improvements in the disaster resilience of communities", *Earthquake Spectra*, 20(3), pp. 739-55, (2004).

[54] R. Faturechi, E. Levenberg, E. Miller-Hooks, "Evaluating and optimizing resilience of airport pavement networks", *Computers & Operations Research*, 43, pp. 335-48, (2014).

[55] R. Faturechi, E. Miller-Hooks, "Travel time resilience of roadway networks under disaster", *Transportation Research,* Part B, 70, pp. 47-64, (2014).

[56] P. Albores, D. Shaw, "Government preparedness: Using simulation to prepare for a terrorist attack", *Computers & Operations Research*, 35, pp. 1924-43, (2008).

[57] L. M. Virginia, M. Spiegler, M. M. Naim, J. Wikner, "A control engineering approach to the assessment of supply chain resilience", *International Journal of Production Research*, 50(21), pp. 6162-87, (2012).

[58] A. Aleksic, M. Stefanovic, S. Arsovski, D. Tadic, "An assessment of organizational resilience potential in SMEs of the process industry, a fuzzy approach", *Journal of Loss Prevention in the Process Industries*, 26(6), pp. 1238-45, (2013).

[59] A. Azadeh, V. Salehi, M. Arvan, M. Dolatkhah, "Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant", *Safety Science*, 68, pp. 99-107, (2014).

[60] M. Panteli, P. Mancarella, "Modelling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events", *IEEE Systems Journal*, PP(99), pp. 1-10, (2015).

[61] W. Kroger, E. Zio, "Vulnerable Systems", *Springer*, (2011).

[62] M. Panteli, P. Mancarella, "the grid stronger, bigger, smarter", IEEE, *Power & Energy*, pp. 58-66, may/june (2015).

[63] P. Hines, J. Veneman, B. Tivnan, "Smart Grid: Reliability, Security, and Reslieincy", (2014).