Review

A metric and frameworks for resilience analysis of engineered and infrastructure systems

Royce Francis *, Behailu Bekera

Department of Engineering Management and Systems Engineering, The George Washington University, 1776 G St., NW #101, Washington DC, USA

ABSTRACT

In this paper, we have reviewed various approaches to defining resilience and the assessment of resilience. We have seen that while resilience is a useful concept, its diversity in usage complicates its interpretation and measurement. In this paper, we have proposed a resilience analysis framework and a metric for measuring resilience. Our analysis framework consists of system identification, resilience objective setting, vulnerability analysis, and stakeholder engagement. The implementation of this framework is focused on the achievement of three resilience capacities: adaptive capacity, absorptive capacity, and recoverability. These three capacities also form the basis of our proposed resilience factor and uncertainty-weighted resilience metric. We have also identified two important unresolved discussions emerging in the literature: the idea of resilience as an epistemological versus inherent property of the system, and design for ecological versus engineered resilience in socio-technical systems. While we have not resolved this tension, we have shown that our framework and metric promote the development of methodologies for investigating "deep" uncertainties in resilience assessment while retaining the use of probability for expressing uncertainties about highly uncertain, unforeseeable, or unknowable hazards in design and management activities.

Contents

* Corresponding author. Tel.: +1 412 780 6453, +1 202 994 7541 (department office); fax: +1 202 994 0245.
 E-mail addresses: seed@gwu.edu, royce.francis@alumni.cmu.edu (R. Francis), btty@gwmail.gwu.edu (B. Bekera).

1. Introduction

Increased acknowledgment of the role of resilience in augmenting risk management practice has introduced some exciting changes into the systems engineering discipline. Despite an increased prominence of the role of system resilience in various sectors of systems engineering over the past few years, substantial diversity remains among the definitions of resilience. Consequently, frameworks adopted in order to quantitatively or qualitatively assess resilience exhibit little standardization and may offer unclear guidance to systems engineers and managers.

In this paper, we review the literature to provide guidance to infrastructure system engineers by comparing risk analysis to resilience analysis. We then propose a metric for resilience measurement that incorporates three resilience capacities, absorptivity, adaptability, recoverability, with the uncertainty in models of initiating events such as natural hazards or other disruptive events. We conclude the article by discussing the role of risk and resilience analysts in exploring deep uncertainty when managing complex engineered systems.

2. Risk vs. resilience assessment

2.1. Risk assessment overview

In engineering, typically, there are two factors that play a central role in risk assessment: the likelihood an event deemed undesirable occurs and the consequences, given the occurrence of that event. Conditional on the occurrence of an event, the consequences are also characterized by a probability distribution over their severity. In risk assessment, the emphasis is often on assessing the expected harm from the event occurring while not necessarily emphasizing the accrual of benefits to stakeholders. There are three determinants of risk: hazard (disruption), exposure and vulnerability. First, we point out that for the purpose of this discussion probability represents the degree of belief after accounting for all available knowledge that a set of events might manifest themselves. In addition, the laws of probability help operationalize the rules of logic applicable to engineered systems at risk. While probability often provides a language for representing uncertainty, uncertainty and probability are not equivalent. These ideas are drawn from the authors' interpretations of Kaplan [1], Pearl [2], Morgan and Henrion [3], and Schachter [4]. Next, we define a hazard as an event or set of events of concern to system owners, managers, operators, or stakeholders the occurrence of which could compromise the operation and identity of the system. The exposure to this hazard is thought of as the conjunction of the properties of the process generating the event (s) and the system properties or behaviors subjecting it to the event(s). Because the properties of the generating process are generally not known in advance, they are described in the language of probability. The behaviors or system properties subjecting the system to the event(s) may be either deterministic, or probabilistic. The probabilistic approach is especially useful when compressing aleatory variability for analytical purposes. Finally, we define vulnerability as the joint conditional probability distribution of system failure and event(s) consequences given that an adverse event has occurred. In other words, vulnerability

depends not only on exposure to an event, but also on the degree to which normal system reliability is compromised during an event.

This conceptualization of risk is modeled on the ideas of Kaplan [1] concerning the risk triplet. A risk triplet includes a scenario, the likelihood of the manifestation of that scenario, and the consequences of events within that scenario. Instead of defining risk as a number, risk is defined in this more expansive approach to show more explicitly the role of management ideas, beliefs, and background knowledge in determining risk. Kaplan, writing from a Bayesian perspective, has developed a framework where risk is more an epistemic approach to the behavior of the system than a description of the physical states and properties of the system. Other authors, including Aven and Zio [5], have taken a similar approach. On the other hand some authors, including Haimes [6], argue that risk is an inherent property of an engineered system. Haimes defines risk as the measure of probability and severity of consequences [6]. Modeling the system with a specific event scenario and evaluating the consequences as functions of the threat, the vulnerability and resilience of the system and the time of the event have a central role in this approach. Suffice it to say that for the purpose of this article, our ideas about risk more closely follow those of Kaplan, Aven and others who highlight that risk descriptions are based in the extant knowledge and conceptualization of the system at a given point in time. This dependence of the risk conceptualization on current knowledge is explicitly discussed by Schachter [4].

Understanding the nature of and reducing the level of risk pertaining to an organization in general or a particular system within an organization are the major tasks in risk assessment. But we also need mechanisms to make a system or an organization more resistant, effective and durable in the face of risk. The challenge lies in developing comprehensive mechanisms for endowing a system with necessary capabilities so as to cope with changing circumstances and recover quickly and efficiently from a shock event. Systems are faced with continuously changing operating environments due to the dynamics of endogenous as well as exogenous variables. As this happens, the nature of shock events also takes a variety of forms calling for more rigorous, continuous and holistic analysis of their organization and its risk management practices. The concept of resilience may enable the organizational philosophy changes needed to manage risk from a holistic picture and ensure safety and efficiency throughout the life cycle of the system.

2.2. Opportunities for augmenting risk analysis practice with resilience analysis

Resilience analysis is distinguished from risk assessment in several ways. Principally, conventional risk assessment methods are used to determine the negative consequences of potential undesired events, and to mitigate the organization's exposure to those undesirable outcomes. Risk as a measure of potential loss of any type and is associated with the uncertainty about and severity of the consequences of a disruptive activity [7]. In contrast, resilience is an endowed or enriched property of a system that is capable of effectively combating (absorbing, adapting to or rapidly recovery from) disruptive events. The resilience approach emphasizes an assessment of the system's ability to (i) anticipate and

absorb potential disruptions; (ii) develop adaptive means to accommodate changes within or around the system; and (iii) establish response behaviors aimed at either building the capacity to withstand the disruption or recover as quickly as possible after an impact. Anticipation refers to the ability of a system or an organization to forecast the complete set of risk triplets and prepare itself accordingly in order to effectively withstand disruptions. One way to prepare is by building-in reserve capacity that may be exploited when the system is in need. Adaptability is also a crucial aspect of resilience to be assessed. Unlike risk assessment, the resilience approach acknowledges the dynamic nature of complex systems and postulates the ability of the system to flexibly accommodate potential shocks without irreversible or unacceptable declines in performance, structure and function. In fact, adaptability of a system could also mean changes in the current practices, policies and rules in order to triumph in the face of imminent disruption of some sort. Once the disruption occurs, the system attempts to quickly recover. For many scenarios of concern, it may be inevitable that the system incurs loss. Preparing for these adverse events as if they are inevitable requires that regular evaluation of operational procedures, safety procedures and policy guidelines, risk assessment methods, and counter measures are key aspects of resilience assessment.

The concept of resilience has evolved considerably since Holling's foundational definition [8], and many definitions of resilience currently exist, preventing a universal understanding of resilience. We conducted a survey of resilience definitions, and present several categories of resilience definitions in Table 1, including critical infrastructure resilience; resilience as a safety management paradigm; organizational resilience; socio-ecological resilience and coupled ecological-engineered systems; and economic resilience. Table 1 includes a brief summary and key characteristics of each definition referenced. One anonymous reviewer of this article pointed out that some definitions of resilience are in competition with the term robustness. In engineering, robustness is often used synonymously or in place of resilience to value engineering designs. In fact, the simplified example presented later in this article closely approximates this view. These definitions are discussed in more detail in Appendix A.

3. Resilience assessment framework

The evolution of the concept of resilience naturally yields the development of a resilience assessment framework. This framework, illustrated in Fig. 1, consists of five components: system identification, vulnerability analysis, resilience objective setting, stakeholder engagement and resilience capacities.

3.1. System identification

A basic requirement of a resilience assessment is the identification of the system under study. System identification entails definition of the system domain; delineation of fundamental and strategic objectives; identification and characterization of physical, chemical, spatial, or social characteristics; and identification of analytical goals and objectives.

3.2. Vulnerability analysis

After system identification, the analyst or organization must determine the disruptive event(s) of concern. The disruptive event(s) is an event or set of events which make the system's normal operating state susceptible to disruption. A multitude of equivalent terms are used in the literature, including hazards, threats, shocks, perturbations, disturbances, disasters, and anomalies. Because the

occurrence of disruptive events cannot be perfectly predicted due to epistemic or aleatory uncertainty, it is important to evaluate the vulnerability of the system to disruptive events in terms of their likelihoods.

After assessing the likelihood of the disruptive events to which the identified system is vulnerable, it is important to incorporate temporal dynamics into the analysis. This is an aspect in which our framework diverges from traditional risk assessment. Several recent authors have also indicated the importance of explicitly incorporating a time dimension into the definition of resilience, especially Haimes [6,9,10]; however, metrics for resilience often do not include the time dimension. Because we are concerned not just with disruptive events and their attendant likelihoods, but also the system's resistance to and recovery from these events, the resilience assessment must explicitly incorporate time into the analysis. The dynamic aspect of resilience analysis refers not only to the timing of the disruptive event but also to the timing of the resilience actions selected. A vulnerability assessment would then dictate the appropriate resilience action to be taken. These actions could be reinforcing a system's resistance to shock events, reorganizing resources and making structural adjustments to accommodate likely changes or enhance preparedness for recovery operations.

Vulnerability analysis at regular intervals is a key to recognizing disruptive events in advance and continuously self-evaluating and learning from incidents. Evaluating models adopted for the purposes of competence and using the feedbacks to enhance future preparedness is becoming overly challenging due to ever increasing system complexity but still provides an opportunity for piercing insights despite increased system complexity. Through continual assessment of the system's resilience, weaknesses may be proactively identified. The most important piece of vulnerability assessment in the resilience analysis paradigm is continual questioning of the organization's risk model, and recognition that in complex systems catastrophic failures may be inevitable Table 2.

3.3. Resilience objective setting

The ultimate goal of resilience is the continuity of normal system function. Normal system function is to be defined according to the fundamental objectives obtained in system identification. These fundamental objectives guide the analyst or organization through the navigation of multiple objectives extant in normal system function. Multiple objectives are important due to the temporal dimension of vulnerability analysis. A certain set of resilience actions may be delegated on the basis of dimensions of the system function prioritized for recovery. For example, in resilience analysis the decision context for resilience actions might be limited to a predetermined time immediately following system disruption. In this way, the analyst or organization may evaluate resilience actions in a different frame from their overall strategic decision processes.

3.4. Stakeholder engagement

Stakeholders are an integral part of resilience analysis and management. In the case of critical infrastructure, for instance, the NIAC recommends coordination among varying levels of government and Critical Infrastructure and Key Resources sectors for efficient recovery of regular services during disruption [11]. This coordination needs to span the time periods pre-, during and post-disruption to make sure that potential threats are identified and treated on time to bolster mitigation capability. In order to facilitate continuous coordination between the private and public sector, the Australian government, for example, has established the Trusted Information Sharing Network, which enables owners and operators to discuss their vulnerabilities in

Table 1
A brief survey of resilience definitions from different disciplinary perspectives.

Infrastructure systems	Key properties
Infrastructure 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 [51]	• Ability to anticipate • Ability to absorb • Ability to adapt • Ability to recover
In the context of critical infrastructure, resilience refers to: • Coordinated planning across sectors and networks • Responsive, flexible and timely recovery measures, and • The development of an organizational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly [12]	• Coordinated planning • Responsiveness • Flexibility • Timely recovery • Minimum level of service while undergoing changes
Resilience is the ability of a system to recover from adversity, either back to its original state or an adjusted state based on new requirements; building resilience requires long-term effort involving reengineering fundamental processes, both technical and social [70].	• Ability to recover • Back to its original state or an adjusted state • Reengineering fundamental process, both technical & social
Safety Management system	
Resilience refers to the ability of an organization to anticipate, circumvent threats to its existence & primary goals and rapidly recover [71].	• Ability to anticipate • Ability to circumvent threats • Recover rapidly • Preserve identity & goals
Organizational system	
Resilience is the ability to recognize & adapt to handle unanticipated perturbations that call into question the model of competence, and demand a shift of process, strategies and coordination [72].	• Ability to recognize unanticipated perturbations • Ability to adapt • Evaluate existing model of competence and improve.
Resilient organizations are therefore characterized by a balance of stability and flexibility that allows for adaptations in the face of uncertainties without losing control [73].	• Balance of stability and flexibility • Adaptive capacity in the face of uncertainties • Self-control
It is also organization's ability to efficiently adjust to harmful influences rather than to shun or resist them [74].	• Ability to efficiently adjust
Capacity of an organization to recognize threats and hazards and make adjustments that will improve future protection efforts and risk reduction measures [11]	• Capacity to recognize threats • Capacity to prepare for future protection efforts • Ability to reduce likely risks
Resilience is the system's ability to sustain a shock without completely deteriorating; that is, most conceptions of resilience involve some idea of adapting to and bouncing back from a disruption [50]	• Ability to sustain a shock • By adapting to and • Bouncing Back
Social-ecological system	
Resilience is the ability of the system to maintain its identity in the face of change and external shocks & disturbances. Component of the system, the relationship among these components and the ability of these components & relationships to maintain themselves constitutes system identity [75]	• Ability to retain system identity (structure, interrelationships and functions)
Resilience is a measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables [76]	• Persistence to change • Ability to absorb change • Retain relationships between people or state variables
Resilience is defined as the capacity of a system to absorb disturbance and reorganize while undergoing change so as to still retain essentially the same function, structure, identity and feedbacks [77]	• Ability to absorb disturbance • Re-organize while undergoing change • Retain the same function, structure, identity & feedbacks
Economic system	
Economic resilience refers to the inherent & adaptive responses to hazards that enable individuals and communities to avoid some potential losses. It can take place at the level of the firm, household, market, or macro economy. In contrast to the pre-event character of mitigation, economic resilience emphasizes ingenuity and resourcefulness applied during and after the event [78]	• Ability to recover • Resourcefulness • Ability to adapt
Resilience is the ability of the system to withstand either market or environmental shocks without losing the capacity to allocate resources efficiently [79]	• Ability to withstand • Without losing the capacity to allocate resources efficiently
Resilience is the capacity for an enterprise to survive, adapt, and grow in the face of turbulent change [41]	• Capacity to survive • Capacity to adapt

Table 1 (*continued*)

Infrastructure systems	Key properties
Social System	
Resilience is the ability of groups or communities to cope with external stresses and disturbances as a result of social, political, and environmental change [80].	• Ability to cope with stress
Resilience is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must [81].	• Capability to maintain current function, structure • Degrade gracefully
Uncategorized	
Resilience is the ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions [11]	• Ability to resist • Ability to absorb • Ability to recover
Resilience is the ability of a system to withstand a major disruption within acceptable degradation parameters and to recover within acceptable time and composite costs and risks [9].	• Ability to withstand • Sustain acceptable degradation • Recover quickly
Resilience is the capacity of the system to tolerate disturbances while retaining its structure and function [41].	• Capacity to tolerate • Retain function & structure
Resilience refers to how well the system adapts and to what range or source of variation [82].	• Adaptive capacity • Latitude: range of variation
Engineering resilience is the time of return to a global equilibrium following a disturbance. Ecological resilience is the amount of disturbance that a system can absorb before it changes state [83].	• Time of return to global equilibrium • Amount of disturbance absorbed before change of state
Resilience refers to the ability of systems, infrastructures, government, business, and citizenry to resist, absorb recover from, or adapt to an adverse occurrence that may cause harm, destruction, or loss of national significance [11].	• Ability to resist, • Ability to absorb • Ability to recover • Ability to adapt to harmful events
Resilience is the ability of a social or ecological system to absorb disturbances while retaining the same basic structure and ways of functioning, the capacity for self-organization and the capacity to adapt to stress and change. Resilience in business terms can be defined as the ability of an organization, resource or structure to sustain the impact of a business interruption and to recover, resume its operations and provide at least minimal services [84].	• Ability to absorb disturbance • Retain structure & functions • Re-organizing capacity • Adaptive capacity to change • Sustain/withstand impact • Recovery • Back to acceptable performance
Resilience can be understood as the ability of the system to reduce the chances of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (re-establish normal performance) [85].	• Ability to reduce failure chances • Ability to absorb shocks • Ability to recover quickly

a non-competitive platform [12]. The ultimate goal is to effectively coordinate available resources, skills and past experience against potential disruptions to the performance of the system.

3.5. Resilience capacities

The proposed resilience paradigm might be implemented via the set of resilience capacities outlined above: absorptive capacity, adaptive capacity, and recovery and restorative capacity. These three pillar capacities give rise to what we called the resilience triangle as illustrated in Fig. 2.

3.5.1. Absorptive capacity

Vugrin et al. define absorptive capacity as the degree to which a system can absorb the impacts of system perturbations and minimize consequences with little effort [13]. In practice, though, it is a management feature depending on configuration, controls, and operational procedures. System robustness and reliability are prototypical pre-disruption characteristics of a resilient system [14]. Designing a production system with adequate buffer capacity to overcome potential blocking of a production line is, for example, an absorptive endowment. Absorptive capacity is attained through the practice of adverse event mitigation in many systems.

3.5.2. Adaptive capacity

While absorptive capacity is the ability of a system to absorb system perturbations, adaptive capacity is the ability of a system to adjust to undesirable situations by undergoing some changes. Adaptive capacity is distinguished from absorptive capacity in that adaptive systems change in response to adverse impacts, especially if absorptive capacity has been exceeded. A system's adaptive capacity is enhanced by its ability to anticipate disruptive events, recognize unanticipated events, re-organize after occurrence of an adverse event, and general preparedness for adverse events.

3.5.3. Recovery/restorative capacity

Restorative capacity of a resilient system is often characterized by rapidity of return to normal or improved operations and system reliability [14]. This capacity should be assessed against a defined set of requirements derived from a desirable level of service or control. In practice, recovery efforts may be daunting because of a likely conflict of interests. More specifically, it may be difficult not only to assess the costs of recovery actions, but stakeholders may not agree on the benefits accrued through recovery. The case of Hurricane Katrina offers an illustration. As a result of Hurricane Katrina, the United States Congress approved a total of $81.6 billion
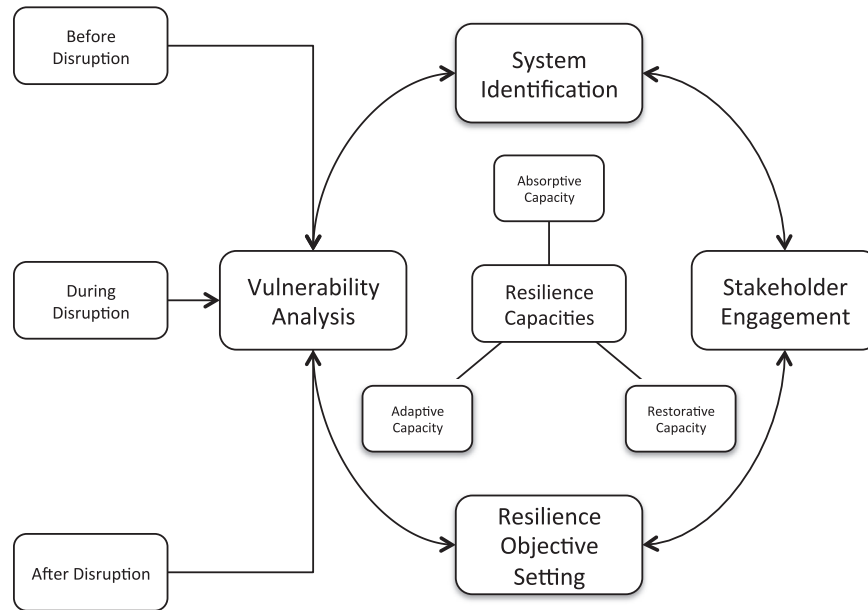
Fig. 1. Resilience framework. This framework consists of five components: system identification, vulnerability analysis (before, during and after disruption), resilience objective setting (identifying goals such as normal performance or basic identity to be achieved or sustained) stakeholder engagement (coordination, cooperation & information sharing) and resilience capacities.

Table 2
Project area descriptive figures.

Miles of circuit line	9.6 mi
Depth of Micropolis area inland	1 mi
Project area	0.5 mi^2
Number of residential customers	446
Number of commercial, industrial, other customers	88
Hurricane category (surge zone)	3 (east of railroad), 5 (west of railroad)

Fig. 2. The resilience triangle showing three major capacities that make up the resilience capacity of a system.

in supplemental disaster appropriations in FY2005 and FY2006. Because of such a large investment the Congress had an oversight interest in the ways these funds are spent and how government agencies and private organizations respond to the funding. On the other hand, significant local expertise and resources were required from stakeholders who might have viewed such large-scale federal intervention warily. Such bureaucratic interdependency creates

tradeoffs identified by Weiss *vis-á-vis* cost, speed, authority, and responsiveness to local and national goals that may be difficult to navigate [15]. In addition, navigating these tradeoffs might be obscured by mistrust or ambiguity about the trustworthiness of government agents or other citizen stakeholders [16]. Hence restorative capacity may be compromised if inadequate investments are made due to disagreements among stakeholders.

4. Measuring resilience

Although we have devoted most of our discussion to the management principles involved in resilience, a metric reflecting these principles is needed for decision support and design. It has been acknowledged that quantitative metrics are required to support resilience engineering. One approach identifies organizational resilience indicators such as top management commitment, Just culture, learning culture, awareness and opacity, preparedness, and flexibility [17]. While these indicators are useful in assessing overall readiness of an industrial process or organization, they do not provide a way to quantify the three essential resilience capacities we have identified. Others have proposed quantitative metrics based on system functionality [18,19], but we propose some additions to these previous approaches. In this section, we propose a resilience metric that incorporates the three resilience capabilities and the time to recovery. Let S_p be the speed recovery factor, F_o the original stable system performance level, F_d the performance level immediately post-disruption, F_r^* be the performance level after an initial post-disruption equilibrium state has been achieved, and F_r be the performance at a new stable level after recovery efforts have been exhausted. Moreover, assume that these quantities are reflective of specific organization's background knowledge, and time of disruption indicated by the subscripts t_δ, and K. The basic idea of resilience might be expressed as a resilience factor, ρ_i:

$$\rho_i(S_p, F_r, F_d, F_o) = S_p \frac{F_r}{F_o} \frac{F_d}{F_o}$$

$$\text{where } S_p = \begin{cases} (t_\delta/t_r^*)\exp[-a(t_r-t_r^*)] & \text{for } t_r \geq t_r^* \\ (t_\delta/t_r^*) & \text{otherwise} \end{cases}$$
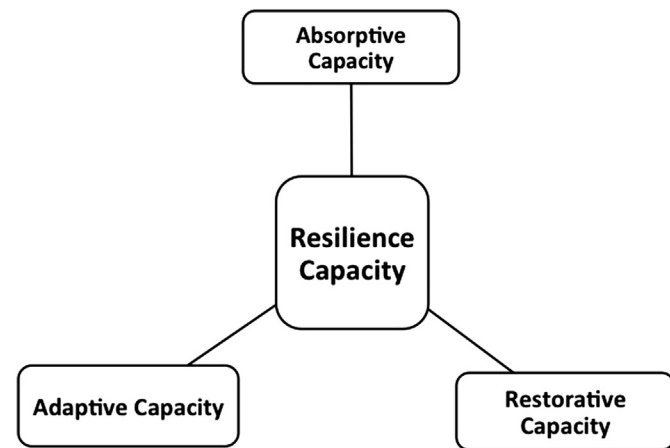
t_δ = slack time

t_r = time to final recovery (i.e., new equilibrium state)

t_r^* = time to complete initial recovery actions

a = parameter controlling decay in resilience attributable to time to new equilibrium

Fig. 3 illustrates these concepts. We define slack time as the maximum amount of time post-disaster that is acceptable before recovery ensues. In other words, we want to make sure that an initial set of actions has been taken to stabilize the system at some intermediate state. Time to recovery, on the other hand, is the length of time post-disaster until a system is brought back to reliable and sustainable performance in the long term. The resilience factor explicitly incorporates the time to recovery by comparing the time required for initial actions to be completed to a slack time for post-event recovery, while incorporating a decay factor to account for increases in the time it takes to reach the final post-disruption state. If the initial recovery takes longer than the slack time then the resilience metric decreases. If the initial recovery is quite efficient, but the system takes a long time to recover after initial stabilization actions, the resilience metric also decreases. Additionally, we have expressed the hardness of the system (absorptive capacity) in terms of the proportion of original system functionality (performance) retained immediately post-event, F_d/F_o. On the other hand, we have expressed the adaptive capacity of the system as the proportion of original system functionality (performance) retained after the new stable performance level has been achieved, F_r/F_o. The interpretation of these two factors is simple: the more functionality retained relative to original capacity, the higher the resilience. Notice that this factor is not constrained on [0,1], meaning that improvements in post-event functionality are possible. To better understand these ratios, consider a case where a heavy storm knocks power out. In this case, F_d/F_o, refers to the proportion of normal service level maintained despite the storm. Suppose that the utility provider distributes electric generators as a temporary solution (adaptive process) to the outage in some areas and, in the meantime, conducts impact assessment before launching recovery efforts aimed at restoring everything to normal. Such an adaptive process brings the utility to a new initial (transitional) performance level, F_r^* and provides substantial information on its preparedness to mitigate loss of functionality due to adverse events. Depending on the damage level, recovery process efforts may take up to a few weeks or even months.
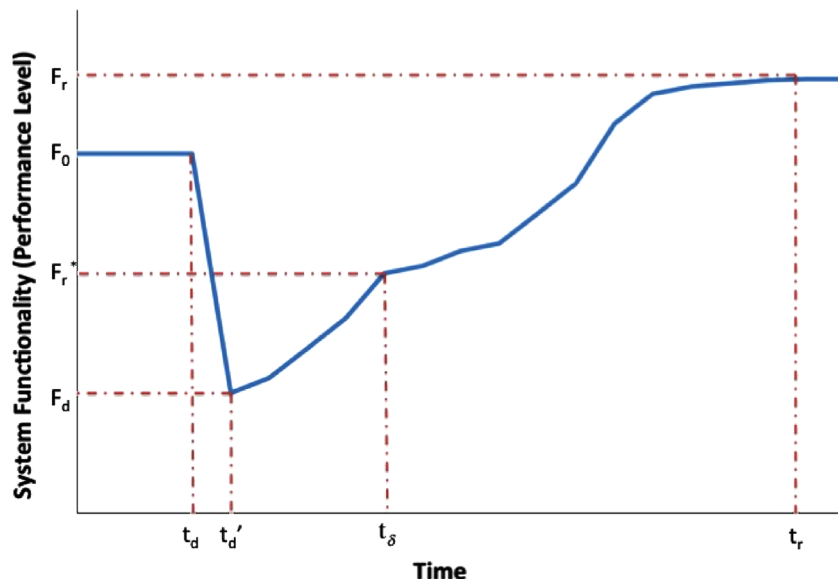
Eventually, the utility system may be able to restore most of its services thereby achieving a new equilibrium. Hence, F_r/F_o would mean the proportion of the normal service level retained at the new equilibrium. System performance at any given point may be quantified in a number of ways, depending on the type of the system. The Multidisciplinary Center for Earthquake Engineering Research (MCEER) suggested a specific approach that may also be extended to other systems. The MCEER's resilience framework consisting of attributes such as robustness, redundancy, resourcefulness and rapidity enables characterization of system functionality (performance) of the system at a particular point in time [20]. These attributes in return give rise to quantifiable variables that can be combined to depict how well a system is doing at any given point in time. According to MCEER, disaster resilience, for example, may be measured by combining system failure probabilities, consequences of the failures and time it takes to optimally recover from the impacts of a disaster [21]. In the case of the metric presented in this paper, the combination may indicate system performance at a given point and that can be compared with original stable state performance level to compute the resilience factor.

Suppose one wants to extend this by incorporating the fragility of the system conditional on event i occurring. Here, we define fragility as the probability of system failure, μ. Let $f(.)$ be the probability density function for system failure. Suppose further that system failure is a function of a parameter vector $\mathbf{z}$. The fragility of the system under event i is

$$f(\mu|\mathbf{z}_i)$$

This can be combined with the resilience factor as follows:

$$f(\mu|\mathbf{z}_i) \cdot \rho_i(S_p, F_r, F_d, F_0)|_{t_d, K}$$

This idea, the combination of fragility and resilience, leads to the derivation of a measure of expected system functionality degradation, ζ. It is the result of integrating over the compound process generating the hazard. Because resilience actions might be expected to influence (causally) the fragility of the system, this quantity can be included as a weighting factor in a subsequent decision-analytic (e.g., risk-aversion or utility-based) framework. Note that this metric would not be a resilience metric, per se, but a weighted resilience factor.

This discussion suggests two additional metrics: (i) an entropy-weighted measure of resilience for incorporating subjective

Fig. 3. The relationship between time and system functionality. After initial disruption, an initial slack time for post-disruption actions is allotted. The final equilibrium state is assessed after a new equilibrium has been achieved.

probabilities about potential disruptions; and (ii) the expected system functionality degradation. Concerning the latter, ζ is the combination of fragility and resilience weighted by the probability of occurrence of the event D_i:

$$\zeta = \sum_i \Pr[D_i] \cdot f(\mu | \mathbf{z}_i) \cdot \rho_i(S_p, F_r, F_d, F_0)$$

The entropy-weighted measure of resilience for group decision support is a bit more involved. It suggests that we should be concerned not only about the consequences of highly improbable events (since they will be more catastrophic), but also that we should care about the extent to which experts or stakeholders disagree on the likelihood of those events. Suppose the probability of a disruption, D, is given as the function of a random parameter λ [e.g., $D_i \sim \text{Poisson}(\lambda_i)$]. The distribution of the "true" value of this parameter might be estimated via expert elicitation. Moreover, this expert-elicited distribution might have a parameter (or set of parameters) ϕ. In the language of probability, we can use the law of total probability to obtain the probability distribution of event D_i conditional on the expert-elicited distribution of the value of the parameter λ (see [22,23] for more details):

$$\Pr[D_i | \phi] = \int \Pr(D_i | \lambda_i) \cdot \Pr(\lambda_i | \phi) d\lambda_i$$

We then incorporate the entropy in this distribution into the resilience definition. While entropy has found some use in the engineering community as a measure of diversification impact attributable to a project portfolio [24], we employ Shannon entropy as a metric to help address deep uncertainty [25–31] in resilience analysis. In many disciplines entropy has been used as a measure of population diversity or disorder. We choose to use entropy in its more fundamental notion: entropy is the degree of "surprise" in the state of a random variable, multiplied by its probability of occurrence. When evaluating resilience under deep uncertainty, we want to more heavily weight the performance of the system under "surprising" conditions when compared with the most likely conditions.

There are a couple reasons for incorporating entropy into the resilience definition. The first is the idea that we want to combat the possibility of being overconfident that we are prepared for even the most highly improbable events. If an event is highly improbable, its occurrence may initiate unforeseen conditions that defy adequate preparation. The more improbable an event, the more unlikely we will be prepared for its consequences. On the other hand, if experts disagree, we may not take adequate precaution due to unclear mandates on what should be done. Note that the overconfidence we are referring to is in the sense that we may have not devoted enough resources to the problem due to disagreement among managers and key stakeholders or experts. This is different from the overconfidence in probability estimation attributable to cognitive biases addressed by proper scoring rules, etc. [32]. Of course, proper calibration must be ensured in the underlying elicitation protocol.

With these thoughts in mind, recall that the entropy in the joint distribution of the event generation model, model parameters, and expert (or prior) parameters is [2,33]:

$$h(D, \lambda, \phi) = h(D | \lambda, \phi) + h(\lambda | \phi)$$

where

$$h(D | \lambda, \phi) = - \iiint \Pr(D | \lambda, \phi) \log (D | \lambda, \phi) dD \, d\lambda \, d\phi$$

and

$$h(\lambda | \phi) = - \iint \Pr(\lambda | \phi) \log (\lambda | \phi) d\lambda \, d\phi$$

The first term on the right hand side is the Shannon entropy in the event generation model given the expert elicited distribution on the model parameters; the second term is the Shannon entropy in the expert-elicited distribution on the parameter of the event

generating process. We can construct an entropy-weighted resilience metric by incorporating $h(D, \lambda, \phi)$ into the system resilience metric as a multiplicative factor:

$$\eta_i = -\sum_i \rho_i(S_p, F_r, F_d, F_0)|_{t_d, K} h(D_i, \lambda_i, \phi)$$

$$= -\sum_i \rho_i(S_p, F_r, F_d, F_0)|_{t_d, K} [\Pr(D_i | \lambda_i, \phi) \log (D_i | \lambda_i, \phi) + \Pr(\lambda_i | \phi) \log (\lambda_i | \phi)]$$

This metric frames the resilience concept in the following ways:

1. We have defined a basic metric for resilience, the resilience factor $\rho_i|_{t_d, K}$, that incorporates speedy recovery, and the resilience capacities adaptability, absorptivity, and recoverability; and
2. We have defined resilience as a probabilistic concept combining expert (e.g., subjective) knowledge of the underlying adverse event generating process with assessments of recoverability, hardness, and adaptability. This expert knowledge is a proxy for anticipation and preparedness.
3. To evaluate resilience actions or investments over a project life cycle, we have proposed an entropy-weighted decision support metric, η, and an expected value formulation ζ, that includes the resilience factor, system fragility, and the probability of disruption.

These metrics contribute to the ongoing discussion within the community by synthesizing the discipline of probabilistic risk analysis with resilience engineering. Furthermore the metric, η, more heavily weights system resilience to extreme events by changing the contribution to the expected performance metric. Each simulation's contribution to the metric, η, is the system performance characteristic for that simulation run multiplied by the Shannon information in the event imposed on the system during that simulation. To illustrate this, consider the familiar additive form of the expected value function used in multi-attribute decision problems:

$$E[X] = \Pr(X) \cdot U(X)$$

here, X is the event of interest, and $U(X)$ is the consequence of observing a specific value of X. In this case, the contribution of the consequence $U(X)$ to the decision metric $E(X)$ is $\Pr(X)$. In essence, this form weights the consequences of the most likely outcomes of X much more than the consequences of the more extreme outcomes of X. Often times, however, it may be most interesting to emphasize system performance under the most extreme conditions. The metric proposed above, η, contributes the following to the decision metric:

$$\eta(X) = -\Pr(X) \log (X) \cdot U(X)$$

When using η, extreme events are more heavily weighted than in the case of the expected value metric since the Shannon information factor increases their contribution to the decision metric. This is useful in the case of resilience and reliability. While the average reliability or resilience will be very high when the expected value is taken, it may be of most interest to decision makers to understand the reliability of the system under the most extreme conditions. The decision metric η is a step in this direction since the Shannon information for extreme events is much greater than the Shannon information for the most likely events.

5. Measuring resilience: an electric power example

In this section, we demonstrate the proposed resilience metric by applying this metric to the electric power network of a fictional city called Micropolis [34]. The electric power network for Micropolis is illustrated in Fig. 4, and key descriptive statistics for the project area are reported in Table 2. Our example evaluates an infrastructure hardening decision in which planners consider whether to place

overhead infrastructure east of the railroad (running next to the transmission line dividing the city down the middle) underground to reduce vulnerability to hurricanes. The fictional city project area is defined as a small North Carolina coastal city straddling Category 3 and Category 5 hurricane storm surge zones, with the city extending approximately 1 mile inland and 1/2 mile along the coast. The eastern area of Micropolis is primarily residential, with a small commercial/industrial area in the middle part of the eastern half of the city. Micropolis was developed by researchers at Texas A&M University in the United States to facilitate infrastructure risk and vulnerability research on realistic systems without risking the dissemination of infrastructure system information that may lead to increased public vulnerabilities. Micropolis is publicly available for download from TAMU at ⟨https://ceprofs.tamu.edu/kbrumbelow/Micropolis/index.htm⟩. One of the current authors has studied the use of Micropolis to evaluate undergrounding electric power infrastructure in hurricane prone regions [35]. The example discussed therein will be used to illustrate the application of the resilience metric described here. As a result, the reader is referred to Ref. [35] for more details about the configuration of this network. Only the most important details will be included here. Francis et al. [35] study three scenarios that form the basis of the calculations herein:

1. Scenario 1: underground all overhead infrastructure east of the railroad;
2. Scenario 2: underground overhead infrastructure east of the railroad in the commercial area only, leaving residential areas unaffected; and,

3. Scenario 3: leave network configuration as-is, making no changes to Micropolis' overhead infrastructure.

Recall from above that S_p is the speed recovery factor, F_o the original stable system performance level, F_d the performance level immediately post-disruption, F_r^* be the performance level after an initial post-disruption equilibrium state has been achieved, and F_r be the performance at a new stable level before recovery efforts begin. In our example, we make the following simplifying assumptions:

- We assume that $S_p = 1$.
- We assume that the system returns to its normal level of service, and that $F_r = F_o$.
- In illustrating this example, the only level of service measure we will consider is the number of customers affected. Thus, F_d/F_o is the proportion of customers whose service was affected by outages attributable to hurricanes.

Our resilience factor, ρ_i, becomes

$$\rho_i(S_p, F_r, F_d, F_o) = \rho_i(F_d, F_o) = \frac{F_d}{F_o}$$

Above, we described the extension of the resilience factor by incorporating the fragility of the system conditional on event i occurring. In our Micropolis example, we have defined component fragility curves conditional on hurricane wind speed and surge height. Thus, the fragility curves directly affect F_d since F_d depends on the failure of specific components in the system. As a result, instead of estimating $f(\mu|\mathbf{z}_i) \cdot \rho_i(F_d, F_o)$ directly, we report the
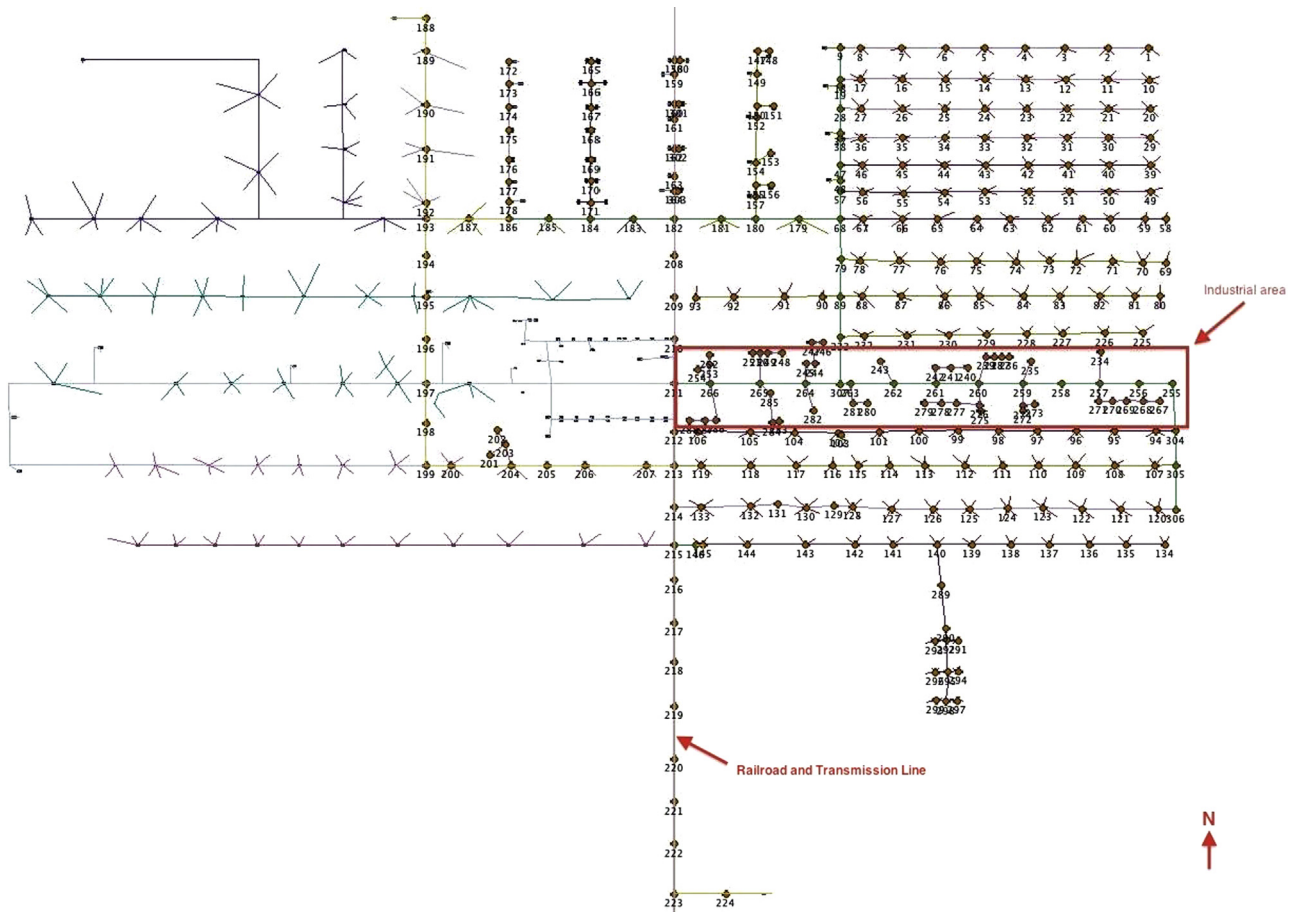

Fig. 4. Micropolis electric power network. Numbered nodes are overhead poles (primarily in the east portion of the city), while the rest of the network is underground. Micropolis has 446 residential customers, 88 industrial customers, commercial, or other customers in the project area served by approximately 9.7 circuit-miles of overhead electric power distribution line.

Table 3

Average absorptivity and entropy weighted resilience scores for residential and commercial districts, conditional on at least one hurricane occurring in the project-year.

	Residential average absorptivity	Residential weighted resilience score	Commercial average absorptivity	Commercial weighted resilience score	Simulated project-yrs w/hurricane
Scenario 1, underground zone 3	0.9744	4.3485	0.9935	4.4295	3257
Scenario 2, underground zone 3, commercial area only	0.9448	4.2005	0.9792	4.3507	3242
Scenario 3, no changes to system	0.8968	3.9780	0.9144	4.0573	3277

uncertainty in the resilience of the system by focusing on ζ_i, and reporting the distribution function on $\zeta_i = \Pr[D_i] \cdot f(\mu|\mathbf{z}_i) \cdot \rho_i(F_d, F_o)$. This approach to ζ_i closely resembles the risk triplet approach, where $\Pr[D_i]$ represents the probability of a hurricane occurring, $f(\mu|\mathbf{z}_i)$ is the probability that the system fails given the properties of the system and its components' configuration, and $\rho_i(F_d, F_o)$ is the consequence of the failure conditional on the hurricane. Note that, as written here, the resilience approach is distinct from life cycle cost analysis. Life cycle cost analysis may be used as another input to the resilience engineering process, but the assessment of expected system resilience we describe here does not directly require cost information. Both approaches, however, use the same system configuration and initiating event generation modeling to suggest inferences.

The final step in illustrating our example is to generate hurricanes to which the system might be subject. This involves two steps: first, we propose a mechanism or model describing the occurrence of hurricanes; second, we propose a model describing the parameters of the hurricane occurrence model. For the occurrence model, we assume the number of hurricanes in a given season has a Poisson distribution with a single parameter, λ. The number of hurricanes depends on three parameters, El-Niño Southern Oscillation (ENSO), Sea level pressure anomaly (SLP), and a temperature-related covariate CRU through a Poisson generalized linear model (GLM). This model's predictive accuracy and development is described in Ref. [35] and is based on climate data reported by Sabattelli and Mann [86]. This two-part model can be used to demonstrate the entropy-weighted measure. While we do not obtain expert-elicited probability distributions for the Poisson-GLM parameters, we can simulate from a joint "prior" distribution for ENSO, SLP, and CRU. We assume that these parameters have a joint multivariate normal distribution. From this distribution, the entropy in $\Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X})$ can be calculated as

$$h(\lambda_i|\mathbf{X}) = \int -\Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X}) \cdot \log[\Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X})] d\mathbf{X}$$

where $\mathbf{X}_i$ is one random draw from the joint "prior" distribution on ENSO, SLP, and CRU. We will assign a "prior" distribution for the coefficients in the link function for our hurricane generation model. The link function will then be used to compute λ for each hurricane season before that season is simulated. The contribution this makes to the resilience metric is based on the Shannon entropy in the hurricane model given ENSO, SLP, and CRU:

$$h(D_i|\lambda_i, \mathbf{X}) = -\log(D_i|\lambda_i, \mathbf{X})$$
$$= \int -[\Pr(D_i|\lambda_i, \mathbf{X}) \cdot \Pr(\lambda_i|\mathbf{X})] \log[\Pr(D_i|\lambda_i, \mathbf{X}) \cdot \Pr(\lambda_i|\mathbf{X})] d\mathbf{X}$$

We can now compute η_i by combining the entropy in λ with the entropy in the hurricane model, then multiplying by the resilience under each hurricane occurrence:

$$\eta_i = \rho_i(F_d, F_0) \cdot [h(D_i|\lambda_i, \mathbf{X}) + h(\lambda_i|\mathbf{X})]$$
$$= \int -\rho_i(F_d, F_0) \cdot \Pr(D_i|\lambda_i, \mathbf{X}) \Pr(\lambda_i|\mathbf{X}) \cdot \log[\Pr(D_i|\lambda_i, \mathbf{X}) \Pr(\lambda_i|\mathbf{X})]$$
$$-\rho_i(F_d, F_0) \cdot \Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X}) \cdot \log[\Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X})] d\mathbf{X}$$

and,

$$\eta = \iint -\rho_i(F_d, F_0) \cdot \Pr(D_i|\lambda_i, \mathbf{X}) \Pr(\lambda_i|\mathbf{X}) \cdot \log[\Pr(D_i|\lambda_i, \mathbf{X}) \Pr(\lambda_i|\mathbf{X})]$$
$$-\rho_i(F_d, F_0) \cdot \Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X}) \cdot \log[\Pr(\lambda_i|\mathbf{X}) \cdot \Pr(\mathbf{X})] dD \, d\mathbf{X}$$

In this example, we compute η via Monte Carlo integration.

The results of this approach are shown in Table 3. Table 3 illustrates the relationship between ζ and η for the residential and commercial customers in Micropolis. For these simulations, a hurricane occurred only 3257 of 50,000 simulated project-years (6.51%) in Scenario 1, 3242 of 50,000 in Scenario 2 (6.48%), and 3277 of 50,000 in Scenario 3 (6.55%). The results in Table 3 indicate that, as defined in this article, undergrounding electric power infrastructure in the districts of Micropolis east of the transmission line attains a higher resilience score and entropy resilience score. This result is true even for the option in which only undergrounding is pursued for the commercial district. These results are in contrast to the decision analysis conclusions obtained in Ref. [35] in which, from a life-cycle cost perspective, undergrounding the electric power infrastructure in Micropolis is never indicated as a more optimal outcome. This result shows that resilience and reliability analysis must be conducted in close consideration with life cycle cost analysis and analogous techniques, as the two techniques may lead to competing conclusions. In fact, one anonymous reviewer of this manuscript addressed this relationship. In some instances, while resilience, including the three dimensions presented above, is important in decision space, the cost of different levels of resilience may be at least as important. Moreover, different stakeholders may perceive the cost of different levels of resilience quite differently. These challenges have been the subject of investigations by Tsang, Lambert, and Patev [36] and Zhou et al. [37].

In this example, the resilience score, η, may not lead to a different conclusion than that indicated by the expected resilience score ζ, as both scores lead the decision maker to consider undergrounding electric power infrastructure a more highly rated approach to hardening Micropolis against hurricane storm surge. It is possible that for some systems, however, there may be large differences in the resilience factor, $f(\mu|\mathbf{z}_i) \cdot \rho_i(F_d, F_o)$, due to large differences in system fragility under extreme events. In these cases, there may be a much larger distinction among alternatives under consideration, and computing η may be a useful way to explore the uncertainty extant in the proposed models of the initiating event(s).

6. Summary

In this paper, we have undertaken a review of various approaches to resilience definition and assessment. Based on this review, we have proposed an alternative metric for measuring resilience that incorporates knowledge uncertainty as an integral input into evaluating system resilience.

Despite our efforts, some important challenges and disagreements have not been addressed. Among these, we will discuss (i) the idea of resilience as an epistemological property of the system [7,38]; and, design for ecological versus engineered resilience in socio-

technical systems [39]. We have hinted at these issues, but have not necessarily proposed a solution to these arguments.

The idea of design for ecological versus engineered resilience in socio-technical systems is an emerging concept that advocates the design of engineered systems based on the ecological principles of diversity, adaptability, interconnectedness, mutual evolution, and flexibility [39–42]. Investigators developing these ideas are motivated by the idea that irrevocable uncertainty leaves risk-optimized systems vulnerable to catastrophic failures attributable to unknowable or unforeseen events. As a result, efforts in design should be allocated to increase emphasis on "safe-fail" rather than "fail-safe" provisions. In the present authors' opinion, this point of view is compelling. In fact, we believe the engineering and infrastructure research and practice community has also recognized these problems and has developed some alternatives to traditional risk-based decision analysis and optimization including info-gap theory [43,44], and the recognition of deep uncertainties in portfolio evaluation [26,29]. The Fukushima disasters and Deep Water Horizon oil spill have highlighted the potential consequences of continuing in a fail-safe design philosophy.

Our discussion has not resolved this one way or the other, aside from recognizing that both sides are examining the same elephant. It is clear that catastrophic failures are unavoidable. In fact, this is rooted in the basic premises of probability theory. Both sides have recognized this. The disagreement, or mutual search if you will, is in regards to how we incorporate this irreducible ignorance into design and management. The present authors advocate somewhere in the middle, arguing for continued use of probabilistic thinking in a resilience analysis framework based on continual evaluation and innovation.

These comments lead to the next question: is resilience intrinsic to the system, or is resilience a management concept dependent on the configuration and rules of operation of the system, and belief about the relevant hazards? While it is clear from our discussion we propose that resilience is an outcome of the beliefs about the system, it is also compelling to think of resilience as inherent to the system. In systems where aleatory uncertainty dominates epistemic uncertainty, it may be more attractive to assume that resilience is dominated by system state manifestations and approach design problems from a perspective of engineered "fail-safe" resilience. Our interpretation of recent research, however, indicates that epistemic uncertainty is much more important to the design and operation of complex systems. Epistemic uncertainty not only influences hazard perception, but indirectly influences system configuration and operation based on the perceived hazards and operating conditions.

These thoughts leave us in an uncomfortable position regarding the roles of probability, uncertainty, and metrics in resilience analysis. While it may be attractive to use only the concepts of uncertainty in system design, mathematically we often use the language of probability to incorporate our intuition about uncertainty into decision making [45]. Furthermore, we generally agree that quantitative metrics help us refine objectives while clarifying understanding about complexity [46]. Metrics may provide a meaningful way to compress and communicate uncertainty while avoiding some of the information loss that may occur if only qualitative descriptions are used. We hope that our metric assists researchers and practitioners in finding a middle ground between uncertainty compression and uncertainty communication or resolution.

Acknowledgments

Appendix A. Toward a common definition of resilience

C.S. Holling first defined resilience as a measure of "the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables" [8]. The definition is so important in the field that, not only has it been mentioned virtually in all related literature, but it also embraces crucial aspects of resilience as defined today. It marked the beginning of a proactive and wide-ranging approach towards ensuring well-being of a system. The same author redefined resilience as "the ability of a system to maintain its structure and patterns of behavior in the face of disturbance" [47], placing more importance on the preserved aspects of the system despite disturbance. A third definition of resilience, which builds upon the first two was provided by Holling in 1996 states that "resilience is the buffer capacity or the ability of a system to absorb perturbations, or the magnitude of disturbance that can be absorbed before a system changes its structure by changing the variables and processes that control behavior [48]." Buffer capacity represents ways to build-in unused capacity in anticipation of increased stress on the system and as a proactive measure to absorb potential shocks. The issue of time is also formally introduced for the first time; absorption is explicitly referred as a pre-event phenomenon.

Holling's foundational work set the stage for other discipline-specific interpretations of the concept of resilience. In many engineering disciplines, the concept of resilience is tightly connected to the concept of risk. A recent exchange between two highly regarded risk and reliability researchers illustrates this intimate connection. Aven [7] defines resilience slightly differently in terms of the uncertainty about the type and severity of consequences attendant to the occurrence of an anticipated or unanticipated disrupteive event. After considering all available knowledge at a given point in time, a low probability of a system being endangered due to the event corresponds to high resilience of the system and vice-versa. Haimes [9], on the other hand, takes a slightly different approach and defines resilience as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time, and composite costs, and risks.

In 2002, Walker extended the meaning of resilience to include the ability to self-organize & adapt while undergoing changes [49]. In 2003, Kendra & Watchtendorf [50] added the notion of 'bouncing back from a disruption as another crucial aspect of a resilient behavior'. As the interest in understanding and applying the concept of resilience increased, particularly following the horrific 9/11 attacks and even more so in the wake of Hurricane Katrina, more definitions of a diverging nature have been offered from different system domains. Hence, the need for standardizing the meaning of resilience has become an important aspect of resilience studies. For example, the National Infrastructure Advisory Board (NIAC) argues that absence of a common definition of infrastructure resilience can prevent the efficient allocation of resources or transparent promulgation of security goals for the design of federal policies [51].

Montoya [52] identifies 45 different classes of attributes that have been linked with resilient behavior in systems and organizations. The author then aggregates these attributes following the theory developed throughout Ebeling [53] and Leenders et al. [54]. Montoya lists 14 classes of attributes most relevant to resilience according to their aggregated frequency distribution within 209 references. These are reduced time to repair (maintainability),

reliability, adaptability (flexibility), robustness (resistance), security (vulnerability issues), metrics and procedures, natural disasters, sustainability, resourcefulness and self-sufficiency, reactive vs. proactive measures, systems complexity networks, science and technology (knowledge), cross-function and efficiency [52]. Some of these can be combined further while others are salient factors affecting resilience of a system. For instance, the metrics and procedures and natural disasters attributes can be part of regular vulnerability analysis while resourcefulness may subsume knowledge (science and technology, skills etc.). Resilience activities are related to timeframes pertaining to before, during and after disruptive events. So, vulnerability analysis should also incorporate time because a particular action or combinations are recommended for a specific time period. In addition, cross-function surely depends on system complexity and measure of interdependence.

The concept of resilience has evolved considerably since Holling's foundational definition, and many definitions of resilience currently exist, preventing a universal understanding of resilience. Here, we discuss the evolution of the resilience concept by surveying several published definitions. The definitions we have considered appear in Table 1, including a brief summary and key characteristics of each.

Critical infrastructure resilience

Critical infrastructure, as defined by the US Government, refers to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [55] in [56]". Infrastructure systems are prone to a range of human-caused or natural disruptive events. Resilience, in this context, is described with ability to anticipate, absorb, adapt to and recover from the said events. Also, bringing the system back to its original state or an adjusted state and providing minimum level of services while undergoing changes are a necessary condition for resilience. Coordinated planning refers to stakeholders' role as in identifying and cooperating against common threats. The coordination aspect is essential for resilience, impacting recovery procedures and as a result should be considered in resilience planning.

Resilience as a safety management paradigm

Safety, as defined by MIL-STD-882 is the freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [57]. In the same standard, system safety is defined as the application of engineering and management principles, criteria and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of the system life cycle. The first definition of safety seems to suggest the traditional understanding of safety as a static system property. However, the later definition of systems safety implies that safety is something that may be *achieved* throughout all phases of system life cycle. This is in congruence with the resilience approach which emphasizes that safety is a dynamic process and something an organization or a system *does* [58]. Resilience engineering is distinguished from traditional safety management in that, instead of identifying and alleviating risk factors, it aims to build on strong dimensions of a system so as to compensate for poor design or management in case of unanticipated disruptions [59]. Seen from the resilience point of view, safety is a dynamic phenomenon demonstrating how a system performs in the face of disruptions, how it can dampen the impacts on and around the system, or how it can quickly reinstate itself with minimal or no damage. Resilience in the context of safety includes the ability to anticipate, circumvent and recover rapidly from events that threaten safety. In this respect, resilience allows for a more proactive approach for handling risk factors and ensuring safety throughout the lifecycle of a system.

While a resilient system is likely to be safe, the converse is not necessarily true. Safety may be obtained at the cost of other objectives, like a system operating at less than optimal performance for the sake of ensuring safety. A Dutch railway study pointed out that passenger safety was obtained by sacrificing goals, traffic volume and punctuality. This system has predefined safety operating zones; whenever a train goes outside this prescribed area everything in the railway system stops, regroups and only after the safe operating mode is returned that the system resumes operation [60]. This system may not be designed with enough adaptive capacity and thus, not resilience. But it acquires high-level passenger safety: clearly, resilience is about more than risk and safety combined.

Organizational resilience

Organizational resilience involves the capacity to recognize threats, evaluate the current risk analysis models used by the organization to be competitive, self-regulate, prepare for future protection efforts, and the ability to reduce likely risks as potential candidates of factors influencing the system's resilience.

The interest in organizational resilience has developed as system complexity continues to grow. There is an ever increasing need to view safety from a holistic view of a system. Consider the case of the Space Shuttle Columbia disaster. The Columbia Accident Investigation Board (CAIB) identified a variety of factors contributing to the disaster and explained how NASA came under criticism for risky decision making. David Woods identifies a number of general patterns in this case [61]. Drift toward failures as defenses erode in the face of production is one of the likely reasons for the disaster. With increasing emphasis on productivity it is easy to lose sight of safety checks. This suggests an inability to recognize imminent threats beforehand. Consequently, there is an apparent issue in finding the right balance between production level and working intensity. Avoiding these issues necessitates a mechanism to continuously *detect* how much of initial safety has been eroded at some regular interval. The CAIB reports uncovered existence of intense working habit targeted at completing project on time, thereby allowing system to capability to diminish over time. Resilience prevents this from happening by imposing ongoing safety measures calling for attention, remediation and continuous monitoring to enhance system safety.

NASA's failure to revise its model of risk assessment, especially related to foam events during the launch of space shuttles, is another issue identified as a prevailing problem in the CAIB report. NASA was getting overconfident due to previous success stories. A resilient organization is always on alert to *anticipate* new challenges to its activities and avoids complacency, leaving no room for an unexpected downward spiral.

Another crucial observation revealed a discrepancy in interoperation, coordination and communication among the people involved. It was noted that decisions were made on the basis of technical data marked by appreciable uncertainty without conducting cross-checks, thereby impairing the quality of organizational decision making. A resilient organization might, however, encourage effective exchange of information among all stakeholders.

Socio-ecological resilience (coupled ecological-engineered systems)

Socio-ecological systems reflect a highly interconnected relationship between society and ecosystems. Resilience of such a

system of systems depends on a wide range of factors stemming from the linkages between human societies and ecosystems. The factors include changes in the social, political and environmental situations. These factors cause stress and disturbance, which a community may overcome if it is truly resilient. The interaction between actors of both subsystems further complicates the matter and increases the vulnerability of the system. Socio-ecological resilience embodies the capacity of linked social–ecological systems to *absorb* recurrent disturbances in order to retain essential structures, processes and relationships [42]. Increasingly, researchers are approaching this conceptually by designing products or systems with *intrinsic* resilience rather than attempting to anticipate unforeseen shocks [39–41]. The intrinsic approach highlights the fact that knowledge about potential shocks is incomplete and may leave designed systems vulnerable to catastrophic failures. Consequently, researchers and engineers adopting the socio-ecological perspective of intrinsic resilience hope that "properties such as diversity, efficiency, adaptability, and cohesion [41]" will reduce the vulnerability of engineered systems in the event of unforeseen and unanticipated disruptions. In addition, Adger et al. argue that it also reflects the degree to which a complex adaptive system is capable of self-organization (versus lack of organization or organization forced by external factors) and the degree to which the system can build capacity for learning and adaptation [62].

Economic resilience

Economics is one of the areas where the phenomenon of resilience is least discussed [63]. Martin's review of the sporadic literature identifies four different dimensions of resilience relevant to economic systems in case of disturbances such as recession. These are resistance, recovery, re-orientation and resumption of the growth pattern prior to the disturbance. Resistance deals with the vulnerability to one or more of economic shocks, whereas recovery clearly stresses how quickly an economy bounces back to original performance. Re-orientation, on the other hand, refers to the ability to re-organize in an attempt to become more accommodating to anticipated or unforeseen shocks, and resumption captures the system's tendency to retain pre-shock economic performance.

In the context of the study of engineered or infrastructure systems, economic resilience has received much greater attention. On the one hand, we have already discussed the idea that infrastructure systems are susceptible to cascading failures [56,64,65]. These problems can be studied using economic analysis tools derived from Leontief's input–output approach to determine how inoperability in a subset of infrastructure systems affects the viability of others [66]. Additionally, it has been shown that infrastructure unreliability in natural hazards can compromise economic recovery. For example, Chang [67] and Chang and Shinozuka [68] have shown that natural hazard impacts to lifeline infrastructure may impose public costs orders of magnitude greater than private utility costs. Consequently, investment decisions based on private utility costs may not adequately ensure the system is designed to promote recovery of system function with respect to public or societal needs.

Summary

These definitions are the product of an evolution in the resilience concept that seems to be converging in the direction of a common definition, as these definitions share several common elements: absorptive capacity, recoverability, adaptive capacity, and retention of identity (structure and functions). Factors that affect resilience are robustness (ability to withstand a given level),

resourcefulness (level of preparedness to effectively combat an adverse event), redundancy (degree of substitutability of elements of a system), rapidity (ability to return to normal operating capacity in a timely manner), interconnectedness, cross-functional stakeholders, anticipative capacity, stakeholders' cooperation, capacity to recognize threats, evaluation of the model used to obtain and retain competence, capacity to prepare for future protection efforts, and ability to reduce likely risks [69]. In short, resilience is a conceptual framework composed of multiple dimensions. Absorptive, adaptive, and restorative capacities are at the center of what a system needs to do and how it needs to respond to perceived or real shocks. We denote these as the resilience capacities. The objective of resilience is to retain predetermined dimensions of system performance and identity in view of forecasted scenarios.

References

[1] Kaplan S. The words of risk analysis. Risk Analysis 1997;17(4):407–17.
[2] Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann; 1988 (revised second printing).
[3] Morgan M, Henrion M. Uncertainty.Cambridge: Cambridge University Press; 1990.
[4] Schachter RD. Model building with belief networks and influence diagrams. In: Edwards W, Miles RF, von Winterfeldt D, editors. Advances in decision analysis: from foundations to applications, 10. New York: Cambridge; 2007. p. 177–201.
[5] Aven T, Zio E. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering and System Safety 2011;96(1):64–74.
[6] Haimes YY. On the complex definition of risk: a systems-based approach. Risk Analysis 2009;29(12):1647–54.
[7] Aven T. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. Risk Analysis 2011;31(4):515–22.
[8] Holling CS. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics 1973;4:1–23.
[9] Haimes YY. On the definition of resilience in systems. Risk Analysis 2009;29(4):498–501.
[10] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis 2006;26(2):293–6.
[11] DHS Risk Steering Committee, "U.S. Department of Homeland Security Risk Lexicon," United States Department of Homeland Security. Washington DC; 2008.
[12] Commonwealth of Australia. Critical infrastructure resilience strategy. Canberra: Commonwealth of Australia; 2010.
[13] Vugrin ED, Warren DE, Ehlen MA. A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress 2011;30(3):280–90.
[14] Shinozuka M, Chang SE, Cheng TC, Feng M, O'Rourke TD, Saadeghvaziri MA, et al. Resilience of integrated power and water systems.Buffalo, NY: MCEER Research Progress and Accomplishments; 2004 (MCEER-04-SP01).
[15] Weiss NE. Rebuilding housing after Hurricane Katrina: lessons learned and unresolved issues, Congressional Research Service, Washington DC, RL33761; 2006.
[16] Anex RP, Focht W. Public participation in life cycle assessment and risk assessment: a shared need. Risk Analysis 2002;22(5):861–77.
[17] Shirali GA, Mohammadfam I, Ebrahimipour V. A new method for quantitative assessment of resilience engineering by PCA and NT approach: a case study in a process industry. Reliability Engineering and System Safety 2013;119 (C):88–94.
[18] Latora V, Marchiori M. Vulnerability and protection of infrastructure networks. Physical Review E 2005;71(1):015103.
[19] Henry D, Ramirez-Marquez JE. Generic metrics and quantitative approaches for system resilience as a function of time. Reliability Engineering and System Safety 2012;99:114–22.
[20] Bruneau M, Filiatrault A, Lee G, O'Rourke T, Reinhorn A, Shinozuka M, et al., White paper on the SDR grand challenges for disaster reduction multidisciplinary center for earthquake engineering research, Buffalo, NY; 2005.
[21] Multidisciplinary center for earthquake engineering research, "MCEER's Resilience Framework," ⟨http://mceer.buffalo.edu/research/resilience/resilience_10-24-06.pdf⟩; 2006. [Online]. Available from: ⟨http://mceer.buffalo.edu/research/resilience/resilience_10-24-06.pdf⟩. [accessed Oct-2012].
[22] Bedford T, Quigley J, Walls L. Expert elicitation for reliable system design. Statistical Science 2006;21(4):428–50.
[23] Wang W. Comment: expert elicitation for reliable system design. Statistical Science 2006;21(4):456–9.
[24] Joshi NN, Lambert JH. Diversification of infrastructure projects for emergent and unknown non-systematic risks. Journal of Risk Research 2011;14 (6):717–33.

[25] Walker WE, Lempert RJ, Kwakkel JH. Deep uncertainty.Delft: Delft University of Technology and RAND Santa Monica; 2012.

[26] Cox Jr LA. Confronting deep uncertainties in risk analysis. Risk Analysis 2012;32(10):1607–29.

[27] Karvetski CW, Lambert JH. Evaluating deep uncertainties in strategic priority-setting with an application to facility energy investments. Systems Engineering 2012;15(4):483–93.

[28] Hamilton, M., Lambert, J., Keisler, J., Holcomb, F., and Linkov, I. (2012). "Research and Development Priorities for Energy Islanding of Military and Industrial Installations." J. Infrastruct. Syst., http://dx.doi.org/10.1061/(ASCE)IS.1943-555X.0000133 (Oct. 12, 2012).

[29] Lambert JH, Karvetski CW, Spencer DK, Sotirin BJ, Liberi DM, Zaghloul HH, et al. Prioritizing infrastructure investments in Afghanistan with multi-agency stakeholders and deep uncertainty of emergent conditions. Journal of Infrastructure Systems 2012;18(2):155–66.

[30] Samaras C, Willis HH. Capabilities-based planning for energy security at department of defense installations.Pittsburgh, PA: RAND Corporation; 2013.

[31] Lempert RJ, Groves DG. Identifying and evaluating robust adaptive policy responses to climate change for water management agencies in the American west. Technological Forecasting and Social Change 2010;77(6):960–74.

[32] von Winterfeldt D, Edwards W. Decision analysis and behavioral research. Cambridge: Cambridge University Press; 1986.

[33] Whittaker J. Graphical models in applied multivariate statistics.New York: John Wiley & Sons; 1990.

[34] Torres JM. Micropolis: a virtual city for water distribution system research applications.TX: Texas A&M University, College Station; 2006.

[35] Francis RA, Falconi SM, Nateghi R, Guikema SD. Probabilistic life cycle analysis model for evaluating electric power infrastructure risk mitigation investments. Climatic Change 2010;106(1):31–55.

[36] Tsang JL, Lambert JH, Patev RC. Extreme event scenarios for planning of infrastructure projects. Journal of Infrastructure Systems 2002;8(2):42–8.

[37] Zhou Q, Lambert JH, Karvetski CW, Keisler JM, Linkov I. Flood protection diversification to reduce probabilities of extreme losses. Risk Analysis 2012;32(11):1873–87.

[38] Steen R, Aven T. A risk perspective suitable for resilience engineering. Safety Science 2011;49(2):292–7.

[39] Mu D, Seager TP, Rao PSC, Park J, Zhao F. A resilience perspective on biofuel production. Integrated Environmental Assessment and Management 2011;7(3):348–59.

[40] Park J, Seager TP, Rao PSC. Lessons in risk- versus resilience-based design and management. Integrated Environmental Assessment and Management 2011;7(3):396–9.

[41] Fiksel J. Sustainability and resilience: toward a systems approach. Sustainability: Science Practice and Policy 2006;2(2):14–21.

[42] Fiksel J. Designing resilient, sustainable, systems. Environmental Science and Technology 2003;37(23):5330–9.

[43] Ben-Haim Y. Info-gap decision theory: decisions under severe uncertainty. 2nd ed.Oxford, UK: Academic Press; 2006.

[44] Ben-Haim Y. Why risk analysis is difficult, and some thoughts on how to proceed. Risk Analysis 2012;32(10):1638–46.

[45] Epstein W. Unforeseen events, resilience, and probabilistic risk assessment, presented at the PSAM11/ESREL12, Helsinki, Finland; 2012. p. 1–45.

[46] Keeney RL. Value-focused thinking.Cambridge, MA: Harvard University Press; 1992.

[47] Schoon M. A short historical overview of the concepts of resilience, vulnerability, and adaptation. Workshop in Political Theory and Policy Analysis 2005:1–17.

[48] Gunderson LH, Holling CS, Light SS. Barriers and bridges to the renewal of ecosystems and institutions. New York, NY: Columbia University Press; 1995.

[49] Walker B, Carpenter S, Anderies J, Abel N, Cumming G, Janssen M, et al. Resilience management in social-ecological systems: a working hypothesis for a participatory approach. Conservation Ecology 2002;6(1):14–30.

[50] Kendra JM, Wachtendorf T. Elements of resilience after the World Trade Center disaster: reconstituting New York City's emergency operations centre. Disasters 2003;27(1):37–53.

[51] NIAC, National Infrastructure Advisory Council—a framework for establishing critical infrastructure resilience goals final report and recommendations; 2009.

[52] Montoya GA. Assessing resilience in power grids as a particular case of supply chain management.Wright-Patterson Air Force Base, OH: Air Force Institute of Technology; 2010.

[53] Ebeling CE. An introduction to reliability and maintainability engineering. New York, NY: McGraw Hill; 1997.

[54] Leenders M, Fearson H, Flynn A, Johnson PF. Purchasing and supply management. 12th ed.Boston, MA: McGraw-Hill-Irwin; 2001.

[55] U.S. President's commission on critical infrastructure protection, critical foundations: protecting America's infrastructures, {Critical Infrastructure Assurance Office}, Washington DC; 1997.

[56] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 2001;21(6):11–25.

[57] United States Department of Defense. Standard practice for system safety. AMSC N/A, AREA SAFT; 2000.

[58] Hollnagel E, Woods DD. Epilogue: resilience engineering precepts. In: Hollnagel E, Woods DD, Leveson N, editors. Resilience Engineering: Concepts and Precepts, no. Epilogue. Hampshire, UK: Ashgate; 2006. p. 347–58.

[59] Furniss D, Back J, Blandford A, Hildebrandt M, Broberg H. A resilience markers framework for small teams. Reliability Engineering and System Safety 2011;96(1):2–10.

[60] Hale A, Heijer T. Is resilience really necessary? the case of railways In: Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering concepts & precepts, 9. Hampshire, UK: Ashgate Publishing Company; 2006. p. 125–49.

[61] Woods D. Creating foresight: how resilience engineering can transform NASA's approach to risky decision making, Washington DC; 2003.

[62] Adger WN, Hughes TP, Folke C, Carpenter SR, Rockström J. Social–ecological resilience to coastal disasters. Science 2005;309(5737):1036–9.

[63] Martin R. Regional economic resilience, hysteresis and recessionary shocks. Journal of Economic Geography 2012;12(1):1–32.

[64] Rinaldi SM. Modeling and simulating critical infrastructures and their interdependencies. System sciences 2004:1–8.

[65] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliability Engineering & System Safety 2010;95(12):1335–44.

[66] Santos JR. Inoperability input–output modeling of disruptions to interdependent economic systems. Systems Engineering 2006;9(1):20–34.

[67] Chang S. Evaluating disaster mitigations: methodology for urban infrastructure systems. Natural Hazards Review 2003;4(4):186–96.

[68] Chang SE, Shinozuka M. Life-cycle cost analysis with natural hazard risk. Journal of Infrastructure Systems 1996;2(3).

[69] Bruneau M, Reinhorn A. Overview of the resilience concept. In: Proceedings of the 8th US national conference on earthquake engineering, San Francisco, CA; 2006. p. 1–9.

[70] McCarthy JA. From protection to resilience: injecting 'Moxie' into the infrastructure security continuum.Arlington, VA: Critical Infrastructure Protection Program at George Mason University School of Law; 2007.

[71] Hale A, Heijer T. Defining resilience. In: Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering: concepts and precepts, 3. Hampshire, UK: Ashgate; 2006. p. 35–40.

[72] Fujita Y. Systems are ever-changing. In: Hollnagel E, Woods DD, Leveson N, editors. Resilience engineering: concepts and precepts, 3. Hampshire, UK: Ashgate; 2006. p. 20–33.

[73] Grote G. Rules management as source for loose coupling in high-risk systems. In: Proceedings of the second resilience engineering symposium; 2006. p. 116–24.

[74] Woods DHE. Resilience-the challenge of the unstable.Burlington: Ashgate Publishing Company; 1–16.

[75] Cumming GS, Barnes G, Perz S, Schmink M, Sieving KE, Southworth J, et al. An exploratory framework for the empirical measurement of resilience. Ecosystems 2005;8(8):975–87.

[76] Holling CS. Resilience and stability of ecological systems. Annual review of ecology and systematics. 1973.

[77] Kinzig AP, Ryan P, Etienne M, Allison H, Elmqvist T, Walker BH. Resilience and regime shifts: assessing cascading effects. Ecology and Society 2006;11(1):20–42.

[78] Rose A. Defining and measuring economic resilience to earthquakes.Buffalo, NY: University of Buffalo NSF Earthquake Engineering Research Center; 1999.

[79] Perrings C. Resilience and sustainable development. Environment and Development Economics 2006;11(4):417.

[80] Adger WN. Social and ecological resilience: are they related? Progress in Human Geography 2000;24(3):347–64.

[81] Allenby B, Fink J. Toward inherently secure and resilient societies. Science 2005;309(5737):1034–6.

[82] Woods D, Cook R. Incidents-markers of resilience or brittleness? In: Hollnagel E, Woods DD, Leveson N, editors. Resilience Engineering: Concepts and Precepts. Hampshire, UK: Ashgate; 2006. p. 69–79.

[83] Gunderson L, Holling CS, Pritchard L, Peterson G. Resilience. In: Mooney H, Canadell J, editors. Encyclopedia of global environmental change, 2. Scientific Committee on Problems of the Environment; 2002. p. 530–1.

[84] Environment and Development Division, UNESCAP. Sustainability, resilience and resource efficiency, UNESCAP. Bangkok, Thailand; 2008.

[85] Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, et al. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra 2003;19(4):733–52.

[86] Sabbatelli TA, Mann ME. The influence of climate state variables on Atlantic Tropical Cyclone occurrence rates. J. Geophys. Res. 2007;112:D17114, http://dx.doi.org/10.1029/2007JD008385.