# Exploring Resilience Measurement Methodologies

Ozgur Erol[1], Devanandham Henry[2], Brian Sauser[3]

School of Systems and Enterprises, Stevens Institute of Technology Hoboken, NJ USA

oerol@stevens.edu[1], devanandham.henry@stevens.edu[2], brian.sauser@stevens.edu[3]

**Abstract.** The new paradigm, known as “resilience engineering”, emphasizes the importance of measuring resilience and suggests the development of methodologies to analyze and prepare to improve the resilience of systems. In this paper we review existing resilience measurement methodologies, and provide a detailed discussion on the resilience measurement methodologies, challenges, and further implications. We define system’s resilience as the capacity to decrease vulnerability, the ability to change and adapt, and the ability to recover quickly from disruption. Using this definition, we identify metrics which evaluate, more specifically: (1) a system’s capability to decrease its level of vulnerability to expected and unexpected events, (2) its ability to change itself and adapt to changing environment; (3) its ability to recover in the least possible time in case of a disruptive event. Based on the discussed enterprise resilience metrics, we use several examples and evaluate a set of illustrative responses to common disruptions.

## Introduction

The concept of resilience has been become an important area of research within the growing body of literature on complex systems. Although, there is a good amount of scholarly literature defining the concept of resilience in various disciplines, there is a gap in the literature regarding a complete approach to measuring resilience. Given the increasing instances of unpredictable and unpreventable events, the need for resilient systems has been realized more than ever. In order to create and maintain resilient systems, it is important to define appropriate metrics that would help us to estimate the resilience of systems.

This paper builds on the previous work (Erol, Sauser et al. 2009) by the authors where they have discussed resilience in depth and defined it as a system’s capability to decrease the level of its vulnerability to expected and unexpected threats, its ability to change itself and adapt to its changing environment, and its ability to recover in the least possible time in case of a disruptive event. In this paper, the authors review the existing methodologies of measuring resilience and attempt to provide a foundation to develop a comprehensive methodology for measuring system resilience.

## What is Resilience?

The concept of “resilience” has been frequently used and discussed in the literature in a range of disciplines including materials science, ecology, organizational theory, economics, risk management, sociology, psychology, computer networks (Bonanno 2004); (Adger 2000); (Mallak 1999); (Callaway, Newman et al. 2000); (Arthur 1999); (Folke, Carpenter et al. 2002); (Starr, Newfrock et al. 2003); (Carpenter, Walker et al. 2001); (Holling 1973); (Fiksel 2003). The word resilience is defined as the ability "to recover from or adjust easily to misfortune or change" (Merriam-Webster). In psychology, resilience has been characterized as the positive capacity of individuals to cope with stress and catastrophic events and their level of resistance to future negative events. In materials science, resilience has been described as the physical property of a material to bounce back to its normal shape after a deformation. In computer networks, resilience has been expressed as an ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation (Hollnagel, Woods et al. 2006). The common aspect of all these definitions is that resilience is defined as a response to unexpected or unforeseen changes and disturbances, and an ability to adapt and respond to such changes.

Two understandings of resilience that are most useful can be found in the field of ecology and in the field of engineering. As a technical term, "resilience" appears to have originated from the field of ecology, where it has been defined as the ability of ecosystems to absorb and respond to disturbance (Holling 1973). Besides its extensive use in ecology, the concept of resilience has gained importance for engineered systems as a way to address their increasing complexity and to design systems that are capable of sustaining unanticipated failures without catastrophic losses. For engineered systems, resiliency has been defined as the ability of the system to withstand a disturbance and to recover while undergoing change and maintaining the same functionality (Gibbs 2009). Gunderson and Pritchard (2002) showed that there are two distinct approaches to resilience in the literature: engineering resilience is the speed of return to the steady state following a perturbation, which implies a focus on the efficiency of a set of functions; and ecological resilience is defined as the magnitude of disturbance that can be absorbed before the system restructures, which implies a focus on the survival of discrete functions. Engineering resilience suggests maximizing the efficiency of systems and processes to return to its desired state relatively easily and rapidly. Ecological resilience suggests designing flexible systems and processes that continue to function in the face of large disturbances, even though this may not maximize efficiency (Dalziell and McManus 2004).

Although each discipline provides a different definition and a perspective on resilience, the common aspect among these definitions is that resilience is a response to unexpected or unforeseen changes and disturbances, and an ability to adapt and respond to such changes. Resilience as a key concept also appears in interdisciplinary areas concerned with complex systems, such as enterprises, critical infrastructure systems, and ecosystems (Carpenter, Walker et al. 2001). From such perspectives, resilience is referred to as an inherent attribute of complex systems (Haimes, Crowther et al. 2008); (Holling 1973); (Hollnagel, Woods et al. 2006); (Rose and Liao 2005); (Westrum 2006); (Dalziell and McManus 2004); (ResilienceAlliance 2008); (van Opstal 2007); (Gibbs 2009); (Fiksel 2006); (Arsenault and Sood 2007).

## *A Systems Approach to Resilience*

Resilience is identified as an inherent attribute of a system in most of the definitions found in the literature. For example, Holling (1973) defines resilience as a system's ability to absorb external stresses. Hollnagel et al. (2006) define resilience as a system's capability to create foresight, to recognize, to anticipate, and to defend against the changing shape of risk before adverse consequences occur.  According to Rose and Liao (2005), resilience refers to the inherent ability and adaptive responses of systems that enable them to avoid potential losses. Westrum (2006) defines resilience as the capacity of a system to avert adverse consequences, minimizing adverse consequences, and recovering quickly from adverse consequences. Dalziell and McManus (2004) define resilience as a system's overarching goal of continuing to function to the fullest possible extent in the face of stress to achieve its purpose.  Haimes et al. (2008) suggest that resilience is the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time. The Resilience Alliance (2008) proposes that resilience is the amount of change that the system can undergo and still retain the same controls over function and structure, the degree to which the system is capable of self-organization, and the ability to build and increase the capacity for learning and adaptation. Van Opstal (2007) defines resilience as the capacity of complex systems to survive, adapt, evolve and grow in the face of turbulent change.

Another key aspect of these definitions is that resilience is defined as a system-wide attribute which focuses on the behavior of the system as a whole (Gibbs 2009).  Most of these definitions of resilience can be applied to any type of system—from natural to engineered.  Additionally, many researchers have agreed that creating resilience requires a holistic systems approach (Fiksel 2006); (Dalziell and McManus 2004); (Arsenault and Sood 2007) and we should investigate ways to identify any patterns of resilience observed in ecological systems and adapt them to engineered systems.

## *Relative Concepts of Resilience*

The concepts of vulnerability, adaptive capacity, and disruptive events are frequently used to define or measure the resilience of systems in the literature.

**Resilience and Disruptive Events.**  Disruptive events are defined as random events caused by internal and external factors affecting a system that have a negative impact on system operations. Sheffi and Rice (2005) define eight phases for disruptive events: preparation, occurrence of a disruptive event, first response, initial impact, time of full impact, preparation for recovery, recovery, and long term impact. The performance of the system fluctuates in proportion to the impact of the disruption.  The resilience of the system depends on how much change there is to the performance of the system during these phases, and the time lapse from the first impact of the disruptive event to full recovery. The preparation phase is the time period in which the system can foresee and prepare for the disruptive event.   There are two distinctive perspectives in the resilience literature regarding preparation for the disruptive events. From one perspective, resilience relies upon the anticipating unexpected disruptive events and designing solutions to eliminate errors (Hollnagel, Woods et al. 2006). The other perspective suggests that resilience relies more on detecting unexpected events sooner, when they can be more easily corrected, in addition to building the capacity to recover from  such events (Weick and Sutcliffe 2001).

**Resilience and Vulnerability.** Resilience of a system is measured by the level of its vulnerability to a specific risk (Berkes 2007); (Christopher and Peck 2004). Vulnerability is defined as being at risk and the likelihood of having disruptions (Christopher and Peck 2004).  The literature suggests that reducing vulnerability has a positive impact on the resilience of a system (Berkes 2007); (Sheffi and Rice Jr. 2005). Sheffi and Rice (2005) suggest that vulnerability assessment should be a part of strategic planning for resilience. They define the level of vulnerability as the probability of the occurrence of a disruption and the extent of the ensuing consequences.  As the probability of the occurrence of any disruption and the severity of the consequences increases, the system's vulnerability quotient will be higher.

**Resilience and Adaptive Capacity.** Adaptive capacity is a concept that has also been frequently associated with resilience (Goble, Fields et al. 2002); (Dalziell and McManus 2004); (Fiksel 2006); (Gallopin 2006); (Stevenson and Spring 2007); (Gibbs 2009). In order to enhance resilience, some have said that adaptive capacity should be increased even after a disruption. Walker et al. (2002) define adaptive capacity as an aspect of resilience that reflects learning; the flexibility to experiment and adopt novel solutions; and development of generalized responses to broad classes of challenges. Adaptive capacity has also been related to concepts of robustness, agility, and adaptability. Adaptive capacity indicates the ability of systems to revert to their initial state after partial damage, while robustness requires that systems do not get any damage (Zhang 2008). Robustness characterizes the ability to forego hyper-responses to changing environments while agility is the ability to change rapidly; whereas adaptability demonstrates the ability to adapt to changing environments while delivering the intended functionality under varying operating conditions (Fricke and Schulz 2005).

## Common Aspects and Challenges of Measuring Resilience

The new paradigm known as "resilience engineering" emphasizes the measurement of resilience. The practice of resilience engineering suggests the development of tools and methodologies to analyze, measure, and monitor the resilience of systems in their operating environment in order to improve a system's resilience vis-à-vis the environment, and to model and predict the short and long-term effects of change and operational management decisions on resilience (Woods and Hollnagel 2006). In this approach, measurement is a means of supplying the information to allow for better decisions. Through the analysis of related literature, we observed a few common aspects that were frequently discussed. Many of the existing resilience related work discussed the importance of meaningful and effective resilience metrics in order to assure and maintain resilience of a system.

**Systems View on Measuring Resilience.** A majority of resilience-related literature suggests taking systems approach as a basis to measuring resilience (Dalziell and McManus 2004), (Cumming, Barnes et al. 2005). Taking the systems approach – seeing the system as a whole and understanding the parts which constitute the system and identify the relationships help to identify the interrelationships and interdependencies in dynamic and complex systems. As a basis to measuring resilience, it is important to look at the organization in terms of its systemic properties, such as: (1) Articulation of the system purpose, and from that, defining the system boundary; (2) identification of the different components or elements that the system requires in order to achieve the system purpose; (3) examination of the relationships between these different components and elements to understand how they work together to achieve the system purpose; (4) review of how the system interacts with its environment, its influence on the environment, and how the environment effects change within the system (Dalziell and McManus 2004).

**Resilience as an Emergent Feature of the System.** There is a consensus in the literature that resilience is one of the emergent features of a system (Paries 2006; Haimes, Crowther et al. 2008). Haimes et al. (2008) define the emergent properties of systems as those system features that are not designed in advance, but evolve based on sequences of collected events that create the motivation and responses for properties that ultimately emerge into system features. How does this feature relate to the measurement of resilience? Since resilience is an emergent feature of a system, it cannot be directly measured within the as-is state of a system; but should be understood as an evolving feature of dynamic systems. System resilience is thus the interaction of the characteristics and capacities of a system, which will eventually evolve in the case of a disruptive event so it can help a system to adapt to its changing environment and recover from the impacts of the disruptive event. In order to measure resilience from this perspective, it is important to identify the inherent attributes of the system which will evolve and contribute to its ability to be resilient.

Haimes et al. (2008) also discuss the emergent characteristic of resilience in the context of a system of systems. They indicate that the system of systems performs functions and carries out purposes that do not reside in any component system, and that these behaviors are emergent properties of the entire system of systems and not the behavior of any component system. They also emphasize that component systems are typically designed independently (not as a part of a larger system), controlled autonomously, and then integrated in a distributed and loosely coordinated process. The emergent properties of a system of systems are therefore measurable to some extent, but only through knowledge of both component systems and their integration. Pariès (2006) also discusses the concept of emergence and explains that the larger system may show different characteristics than its subsystems. From this point of view, measuring the resilience of a system by considering its extended environment (i.e. its supply chain) requires a more comprehensive approach to understanding not only the attributes of the system but also the dynamics of the environments surrounding it.

**Inherent and Adaptive Characteristics of Resilience.** Rose and Lio (2005) distinguish two characteristics of resilience as inherent and adaptive, the former referring to resilience under normal operating conditions and the latter referring to the deployment of ingenuity and extra effort in crisis situations. They propose a mathematical optimization model for measuring resilience. The main purpose of distinguishing these two characteristics is to isolate them for the purposes of measurement. In particular, adaptive resilience had not yet been sufficiently understood and so Rose and Lio paid special attention to this type of resilience. In their model, they used simulated data and various scenarios to define and to measure adaptive resilience. In their model, resilience refers to post-disaster conditions, which are distinguished from pre-disaster activities to reduce potential losses through mitigation. Such an approach can be applied to measuring system resilience if certain attributes and metrics can be developed for defining the pre-disaster activities which are aimed to reduce potential losses. This approach also requires the development and analysis of post-disaster conditions and scenarios.

**Resilience as a Continuous Process.** Wreathall (2006) proposes developing measurements for resilience in terms of the processes necessary to build resilience. Creating resilience is not a one-time event, but rather spans over time from pre-event strategies to post-event recovery (Haimes, Crowther et al. 2008). Those processes related to resilience include the functions and tasks to prevent, protect, respond, and recover. According to Wreathall, through a comprehensive analysis of “what” has to be done and “how” it can be accomplished should be identified, performance measures should be attained. So what is the implication of this approach for measuring system resilience? System resilience is the outcome of a continuous processes including planning for resilience, responding to threats in the case of disruptions, and taking adaptive actions in order to recover. A thorough documentation and attained performance metrics can be used to measure the quality of outcome of those activities which lead to resilience of systems.

**Measuring Resilience against the Disruptive Event.** As discussed in the previous section, resilience-related actions can occur proactively, concurrently, or as a response to something that has already occurred (Westrum 2006). Therefore resilience becomes (1) the ability to prevent disruptive events, or (2) the ability to prevent consequences of that disruptive event becoming worse, or (3) the ability to recover from a disruptive event that has happened. For each perspective, several metrics can be identified For example, Rose and Liao (Rose and Liao 2005) propose to determine a quotient of failure probability, reduced consequences from failure, and reduced time to recover. Probability of failure is selected as a metric which indicates the ability to prevent disruptive events, reduced consequences from failure is a metric of the ability to prevent the consequences of that disruptive event, and finally the reduced recovery time is the metric for ability to recover from a disruptive event. Westrum (2006) classifies disruptive events based on their predictability, their potential to disrupt a system, and the origin of that disruptive event whether it is internal or external. A vulnerability map here may best exemplify the relative gravity of some disruptive events:

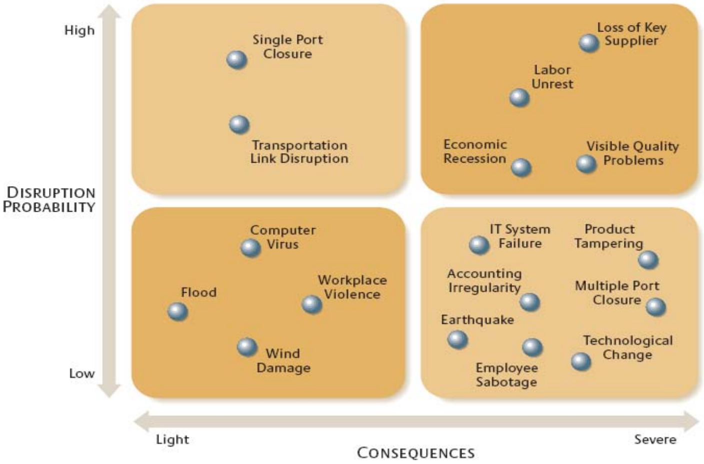

Figure 1 Vulnerability Map

Classifying the types of disruptive events or threats help to create preventive actions and to model how a system will react in case of that threat. Walker and Myers (2004) use a similar approach to create a database of threshold changes. Based on past events, a classification of disruptive events and their consequences can be used to model and to predict a resilience measure. A similar approach is used by Sheffi (2005). He proposes the use of vulnerability maps such as we see in **Error! Reference source not found.** help to visualize the relative likelihood of potential threats to an organization and the company's relative resilience to such disruptions.

**Measuring Resilience using Adaptive Capacity and Time Dimension.** Although the adaptive capacity of a system is a major determinant of its resilience, it should not be considered in a static manner (Woods and Hollnagel 2006); (Dalziell and McManus 2004). Ability to change and adapt can be a much more meaningful measure if the time dimension is considered (Carpenter, Walker et al. 2001). For example, Dalziell and McManus (2004) propose defining key performance metrics and then measuring resilience as a function of a system's vulnerability and its adaptive capacity within the desired time frame (**Error! Reference source not found.**). A similar approach can be applied to measure system resilience. Key performance indicators may have been designed and measured for normal operations. However, the challenge still resides in assessing the degradation as a result of a disruptive event.

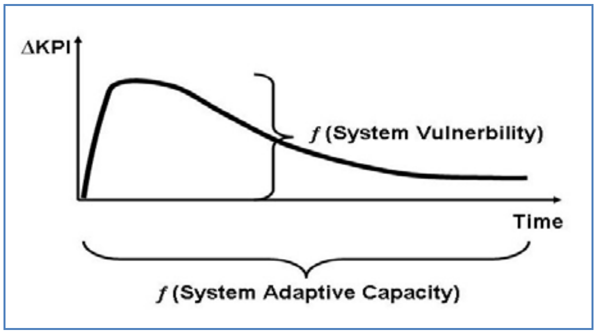

Figure 2 Resilience based on Adaptive Capacity and Vulnerability

Any system can sooner or later adapt to a changing environment, but the time it takes for such adaptation is also important from the perspective of resilience. Measuring adaptive capacity can only be a meaningful measure for resilience if the time dimension is considered, and the proper chronological model is applied in each case. For example, the time between the disruptive event and the system's first response to that event, or the time between the first impact and full recovery. The time dimension of resilience based on the phases of a disruptive event is illustrated by Sheffie's (2005) model for phases of disruptive event (**Error! Reference source not found.**).

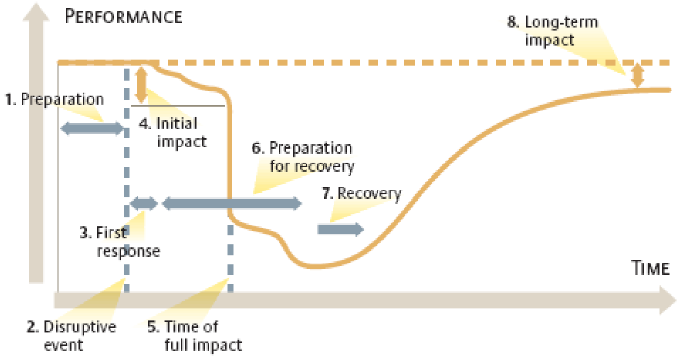

Figure 3 Phases of a Disruptive Event

## Selected Literature on Resilience Measurement Techniques

A common approach in measuring resilience related literature is to refer to other domains in which resilience metrics have been properly defined. For example many researchers look for ways to find similarities between the engineered systems and natural systems or eco-systems where the concept and the study of resilience has been advanced and identify the possibility of applying such methodologies which are used in other disciplines in to the study of resilience or organizations, enterprises, or other engineered systems (Cumming, Barnes et al. 2005). Methods for measuring resilience and the variables may differ from system to system or in other words resilience metrics are domain specific or system specific. A clear definition of resilience is important for measuring resilience.

We have reviewed literature from a wide range of disciplines in which some resilience metrics and measurement methodologies have already been proposed. Below, we provide a summary of the selected literature and the proposed resilience measurement techniques in the areas of psychology, ecology, materials science, organizational and enterprise resilience, and infrastructure and network systems.

## *Ecology*

***New Indices for Quantifying the Resistance and Resilience of Soil Biota to Exogenous Disturbances*** (Orwin and Wardle 2004) -- Ecological stability consists of two components - Resistance and Resilience. While many indices are used for both, most of these make interpretation / distinction difficult or are not applicable to some situations. For an index of resilience (or resistance) to work properly, there are several criteria to be met: i) It should increase monotonically as resilience (or resistance) increases; ii) It should give an identical value whether the response variable relative to the control (or baseline) is increased or reduced by z units iii) It should be bounded for both positive and negative values, and should not tend to infinity; iv) It should always be computable – a zero should not appear in the denominator of a fraction; v) Resilience should be standardized by the amount of change caused by the disturbance initially, and resistance by an undisturbed control soil. This paper proposes indices for resilience and resistance that satisfy the above criteria, while other existing measures fail to satisfy one or more of these criteria.

***An Exploratory Framework for the Empirical Measurement of Resilience*** (Cumming, Barnes et al. 2005) -- This paper proposes the concept of "identity" and define resilience as the system's ability to maintain its identity – where identity is defined as a property of key components and relationships (networks) and their continuity through space and time. In this paper, resilience is viewed as the ability of the system to maintain its identity in the face of internal change and external shocks and disturbances.

## *Enterprises / Organizations*

***Towards Modeling of Resilience Dynamics in Manufacturing Enterprises: Literature review and problem formulation*** (Yao, Jingshan et al. 2008) -- This paper presents a modeling framework to characterize the resilience of a manufacturing enterprise responding to disruptive events, using a network approach. The ability of an enterprise to withstand potentially high-impact disruptive events is known as resilience. This ability is characterized by the redundant or absorbing capacity of the enterprise to the event to dampen its impact, and its recovery capability to quickly resume production or transportation by redistributing its resources. A manufacturing enterprise can be structured as a network of nodes defining the supply chain from sources to customers. Modest disruptions are regular in any enterprise – so the disruptions that warrant resilience are significant either in degree of severity or duration. Four types of costs are considered, which are incurred when resilience is achieved through redundancy. Resiliency can be achieved by operational redundancy or inventory redundancy. One goal of the approach proposed in this paper is to understand the balance between these two.

***Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance*** (Dalziell and McManus 2004) -- This paper discusses the importance of measuring resilience as a key requirement to achieving resilience within an organization and towards creating resilience within a community. They identify key requirements to achieving resilience as i) the development of simple yet effective methodologies that organizations can use to evaluate resilience and strategies for organizations to improve resilience; ii) a common terminology to facilitate dialogue and debate within organizations about resilience priorities, and to enable communication between organizations about common issues and interdependencies in their resilience strategies; iii) metrics for evaluating resilience that are both meaningful to decision makers within organizations, and directly relevant to the overall goals and objectives of the organization. Key performance indicators (KPI's) are proposed, which are tangible measures by which the organization can track its performance against its stated objectives in order to measure organizational resilience. System vulnerability is the ease with which KPIs can be moved away from their desired levels; the time it takes for the system KPIs to recover as the function of the adaptive capacity of the system. Overall resilience of the system is formulated as the function of the area under the curve, which is the total impact on KPIs over the response and recovery period.

***Resilience Management: A Framework for Assessing and Improving the Resilience of Organisations*** (McManus, Seville et al. 2007) -- Resilience is defined as a function of an organization's i) situation awareness, ii) management of keystone vulnerabilities and iii) adaptive capacity. A set of 15 resilience indicators are provided, based on a case-study which involved ten different organizations. In addition, this study provides a Resilience Management framework for both evaluation and improving the resilience of individual organizations.

## Infrastructure Systems

***Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System*** (Omer, Nilchiani et al. 2009) -- This paper uses a network topology to propose a quantitative approach to define and measure resiliency of a telecommunication cable system. Resilience is defined as the ability of the system to both absorb shock as well as to recover rapidly from disruption. The concept of resiliency is closely associated with existing vulnerabilities and the amount of adaptive capacity. Base resiliency is defined as the ratio of the value delivery of the network after a disruption to the value delivery of the network before a disruption. The amount of information, that has to be carried though the network is defined as the measure of value delivery. Similarly, node-to-node resiliency is defined as the ratio of the value delivery between two nodes after a disruption to the value delivery between the two nodes before a disruption. These measures can be used to evaluate the damage when a link or a node is partially or completely down. Based on this, resiliency strategies can be developed, that would minimize the loss caused by a disruption.

One resiliency enhancement strategy is to fully utilize the resources available (residual capacities) and to re-route the information that would otherwise be lost. This would reduce the vulnerability of the system.

***Allocating Security Resources to a Water Supply Network*** (Qiao, Jeong et al. 2007) -- This paper proposes a method for allocating a security budget to a water supply network to maximize the minimum resilience for a predetermined attack level. An intentional attack on water infrastructure can be physical, cyber or chemical/biological. Physical destruction is the focus of this research. Resilience measurement evaluates network resistance to attacks, failures, and disasters. Post-attack consequences are measured by the maximum flow, shortest path, network connectivity, interconnectedness and / or the strength of the residual network. Earlier works on ‘network interdiction’ are discussed in this paper. Criticality identification detects those network components whose removal would seriously affect the operation of the network. This is the attacker’s problem, of trying to inflict the maximum damage possible. A term called “Attack Order” is introduced to indicate the maximum value on the number of components that can be simultaneously attacked. For any attack order, the maximum damage that can be caused can be identified, and this would indicate the minimum resilience of the system. This problem is formulated as a max-min linear programming (LP) problem with an objective to maximize the minimum resilience. Genetic Algorithms are also considered as an alternative, has and have some advantages in generating constraints that become computationally intensive in LP. An iterative solution procedure is defined and computed for different cases with various attack orders

***Methodology for Assessing the Resilience of Networked Infrastructure*** (Reed, Kapur et al. 2009) -- This paper outlines a methodology to evaluate engineering resilience and interdependency for subsystems of a multi-system networked infrastructure for extreme natural hazard events. This paper focuses on the contribution of power delivery systems to post-event infrastructure recovery.

A network model is derived from an eleven-system interdependent infrastructure with the power system in the center, radially connected to the other ten infrastructures. Fragility and quality are two resilience measures that are used. The formulation of these measures indirectly incorporates rapidity and robustness. Resilience is measured as the area under the quality curve Q(t) that takes a value of 1 when fully operable and 0 when inoperable. This approach is illustrated using data from hurricane Katrina, of power outages and restoration of these outages. The rate of recovery was investigated through the quality function.

***Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions*** (Rose and Liao 2005) -- This paper distinguishes two characteristics of resilience as inherent and adaptive, and it proposes a mathematical optimization model for measuring resilience. Inherent resilience is defined as the ability under normal circumstances and adaptive resilience as the ability in crisis situations, to draw upon ingenuity and extra effort. The main purpose of distinguishing these two characteristics is to emphasize the difference in measuring these two types of resilience as there is lack of empirical data for properly assessing adaptive resilience. Simulated data and various scenarios are used to define and measure adaptive resilience. In the model, resilience refers to post-disaster conditions, which are distinguished from pre-disaster activities to reduce potential losses through mitigation. It is proposed to measure resilience as a factor of failure probability, reduced consequences from failure, and reduced recovery time.

***Looped Water Distribution Networks Design Using a Resilience Index Based Heuristic Approach*** (Todini 2000) -- Urban water distribution systems are designed as a series of interconnected closed loops where water can flow in either direction. The problem is formulated as a vector optimization problem with cost and resilience as two objective functions. This produces a Pareto set of optimal solutions, as tradeoffs between cost and resilience. Surplus water supply is used to characterize resilience of the looped network, as this is an intrinsic capability of overcoming sudden failures. Increasing this measure of resilience, would lead to improved network reliability. The proposed heuristic design approach begins with a target value of resilience index, and then identifies the pipe diameters for each node-node connection.

## Networks

***Network Resilience: A Measure of Network Fault Tolerance*** (Najjar 1990) -- This paper studies the networks of multicomputer systems. It proposes network resilience and relative network resilience as two measures of network fault tolerance. Network fault tolerance is the maximum number of elements that can fail without inducing a possible disconnection in the network – it is traditionally expressed as the degree of the network. This is a very conservative measure, and does not account for the total number of nodes in the system and the probability of a disconnection. The proposed network resilience measures take these two factors into account. The maximum number of node failures allowed in a multicomputer system is called the degradable level D, constrained by the probability of disconnection. Network resilience NR(p) is a measure designed to provide this upper bound on D – it is defined as the maximum number of node failures that can be sustained while he network remains connected with a probability (1-p). The measure relative network resilience RNR(p) is defined as NR(p)/N, where N is the number of nodes in the network. Network fault tolerance is static measure that depends exclusively on the node degree and therefore the topology of the network. But network resilience is a probabilistic measure that also takes into account the size of the network.

***Resilience Metrics for Service-Oriented Networks: A Service Allocation Approach*** (Rosenkrantz, Goel et al. 2009) -- This paper identifies resilience metrics for service-oriented networks taking into account both the underlying topology of the network and the manner in which services are distributed. Edge resilience of a network is defined as the largest value k such that no matter which subset of k or fewer edges fails, the resulting sub-network is self sufficient. Node resilience is also defined in the same manner. These metrics would be useful in assessing the fault tolerance of a given network. Polynomial algorithms derived from graph theory and network theory are developed to determine edge and node resilience, and also to allocate resources in an optimal way so as to obtain edge-resilient and node-resilient networks.

## Psychology

***A Formal Assessment of Resilience**: **The Baruth Protective Factors Inventory*** (Baruth and Carroll 2002) -- The Baruth Protective Factors Inventory (BPFI) was developed to identify the presence of greater resilience in individuals. This is based on the theory that there are four delineated protective factors that contribute to resiliency – adaptable personality, supportive environment, fewer stressors and compensating experiences. Four items representative of each of these factors were identified. A table of 16 items to be scored using a Likert-type scale (1 to 5) is used to produce an overall resiliency score between 16 and 80.

***Development of a New Resilience Scale: The Connor-Davidson Resilience Scale (CD-RISC)*** (Connor and Davidson 2003) -- Resilience embodies the personal qualities that enable one to thrive in the face of adversity. It is a measure of stress coping ability, and could be an important target of treatment in anxiety, depression, and stress reactions. The biopsychospiritual balance or “homeostasis” of an individual gets disrupted at times, where adaptations or protective factors ineffective. Response to this disruption is a reintegrative process leading to one of four outcomes: there is an opportunity for growth and increased resilience; return to baseline homeostatis;

recovery with lose, establishing a lower level of homeostasis; a dysfunctional state.

The Connor-Davidson Resilience scale (CD-RISC) comprises 25 items, each rated on a 5-point scale (0-4) with a higher scores reflecting greater resilience.

***The Brief Resilience Scale: Assessing the Ability to Bounce Back*** (Smith, Dalen et al. 2008) -- The original and most basic meaning of resilience is to bounce or spring back. But resilience is also defined as resistance to illness, adaptation to stress, and functioning above the norm in spite of stress. Resilience however, is different from thriving, adaptation and resistance. The purpose of the brief resilience scale (BRS) is to develop a reliable scale for the fundamental unitary concept of resilience. The existing measures of resilience generally assess protective factors or resources that involve personal characteristics and coping styles and not resilience directly. BRS includes six items to assess the ability to bounce back or recover from stress. This is the only measure that specifically assesses resilience in its original and most basic meaning.

# Proposed Metrics for System Resilience

## *Recovery Time*

Arguably the most significant metric in a dynamic and diachronic model is recovery time, and in this section we will discuss more concrete examples in order to demonstrate the applicability of the measurement methodology we have been discussing. Recovery time can be considered as the time taken for a system to overcome disruption and return to its normal state. In order to measure recovery time, we need well defined start and stop points. The start point could either be (a) the occurrence of the disruption or (b) when the disruption affects the system – though in some cases, both these could happen at the same instant of time (e.g. a factory being hit by an earthquake). If it were (a), it also depends on the nature of the disruption - some could be instant (e.g. earthquake) while some others could be while some others could extend over a period of time (e.g. drop in sales). If the start point were to be (b), it brings in additional challenges in defining it properly. The precise instant at which a disruption affects a system would depend on the nature of the disruption and also if the effect is direct/primary (e.g. earthquake hitting an assembly plant) or indirect/secondary (e.g. earthquake hitting the manufacturing plant of a supplier). The stop point depends on the definition of the recovered state, which can be considered (in this section) to be equal to the normal state before the onset of the disruption. Hence the stop point would be the instant of time at which the sytem reaches its original state.

Recovery time can therefore be calculated as the time between the start and stop points, as defined above. We can consider two similar systems A and B operating at their respective normal levels of $L_1$ and $L_2$ respectively, as shown in **Error! Reference source not found.** with time on the x-axis and level on the y-axis. Let us assume that these two systems are affected by the same disruption. Hence the start point for both systems is $T_0$, however they may be considered (a or b). The systems A and B recover to their original levels at times $T_1$ and $T_2$ respectively. By our definition, stop points for the two systems A and B would be $T_1$ and $T_2$ respectively. Hence recovery times (RT) would be calculated as:

$RT_A = T_1 – T_0$

$RT_B = T_2 – T_0$

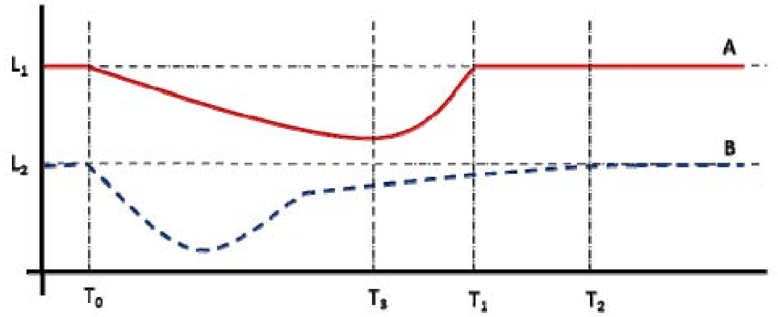

Figure 4 Comparison of Recovery Times

Therefore, from **Error! Reference source not found.**, it can be observed that system A has a shorter recovery time than system B. Recovery time could be used as an indicator of resilience. If we were to consider a shorter recovery time to indicate better resilience, then we can conclude that system A is more resilient than system B since $T_1$ is lesser than $T_2$. However, let us analyze how the two systems behaved after the disruption occurred. System A took a long time to get disrupted, but then it came back quickly to reach its original state $L_1$. On the other hand, system B got disrupted quickly and also came back as quickly close to its original state (i.e. 80%) but it took a long time to recover to its original level $L_2$. Now, let us consider the time instant $T_3$, as shown in **Error! Reference source not found.**. At that instant of time, system A is almost at its most disrupted state, while system B has recovered to about 80% of its original state after being impacted by the disruption. Hence at the instant of time $T_3$, it can be said that system B is more resilient than system A, which is different from our earlier conclusion. In addition, if we had defined the stop point for the recovery time calculation to be the time at which the system reaches 80% of its original state, then system B would have been identified to be more resilient than system A. Similarly, the manner in which start point gets defined, could also lead to different conclusions. While comparing two systems, we can possibly identify which system is more resilient at that instant of time. This conclusion is also applicable only at that instant. In future, the system that seemingly failed to recover from a disrupted state may actually do so, but slowly. Does it mean that the system is not resilient? Is it ever too late to exhibit resilience? This leads us to the issue of what an acceptable or typical recovery time could be, in the context of system resilience. Primarily, this would depend on the nature and intensity of the disruption and the damage it causes to the systems. In addition, recovery time could depend on many other factors like industry type (e.g. manufacturing or service), production capacity (in a manufacturing system) and system size and complexity (in a manufacturing or development system). It can therefore be seen that in order to use recovery time as an indicator of resilience, clear definitions of start and stop points are required, which in turn depend on the definition of the recovered state and of resilience. In addition, when two dissimilar systems are being compared, they must be brought to the same level reference before their resilience can be compared. The challenge still resides in identifying the stop and start points effectively.

### *Level of Recovery*

The level of recovery must also be accounted a fundamental factor in assessing resilience. This metric can be used in combination with the time factor to create a dimensional understanding of predictable outcomes for a particular system or system of system. There are differences in the definitions of resilience with respect to the level of recovery. Some definitions indicate (Hoffman 2007) that it is sufficient to recover to a minimum state - this means that the recovered level is lower than the original level. Some other definitions indicate that recovery level is the same as the original level while some others indicate that the recovered level is higher than the original level (Vogus and Sutcliffe 2007). It is evident that the level of recovery must be defined appropriately before using it to indicate resilience of a system. The level of recovery could be specified by comparing the recovered level to either the original level or the disrupted level (the lowest level reached). We can consider the scenario of two systems A and B as presented in **Error! Reference source not found.**. Time is on the x-axis, but is not considered in discussions here, and the level of performance is on the y-axis. For system A, the levels of performance corresponding to the initial, disrupted and recovered states are indicated by levels $L_1$, $L_3$, and $L_5$. The corresponding levels of performance for system B are $L_2$, $L_4$ and $L_6$. With respect to the original state, level of recovery (RL) could be calculated as the difference between the recovered level of performance and the original level of performance, with resilience being indicated by value of this difference. For the two systems A and B, recovery levels could be calculated as:

$RL_A = L_5 – L_1$

$RL_B = L_6 – L_2$

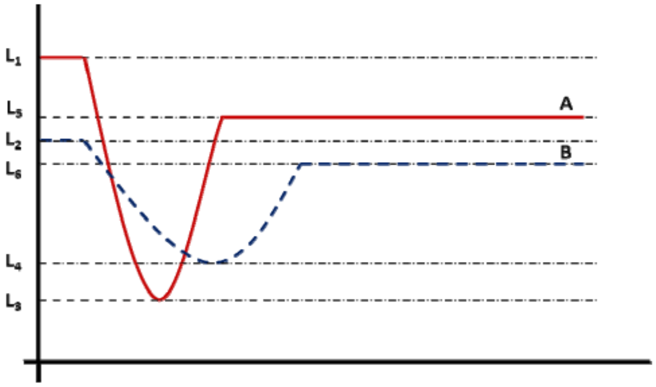

Figure 5 Comparison of Levels of Recovery

From **Error! Reference source not found.** it can be seen that $RL_B$ would be lower than $RL_A$. System B was able to recover is closer to its original level (i.e. 80%), while system A could not recover very close to its original level (i.e. 70%). Hence it could be concluded that system B is more resilient.

But when we calculate recovery levels with respect to the disrupted state, it leads to a different conclusion. When recovery level is calculated as the difference between the recovered level of performance and the disrupted level of performance, the values of systems A and B could be calculated as:

RLA = L5 – L3

RLB = L6 – L4

From **Error! Reference source not found.** it can be seen that $RL_A$ would be higher than $RL_B$. System A recovered by a larger amount from its disrupted state while system B did not recover by the same amount. Hence it could be concluded that system A was more resilient. System B suffered a lesser disruption that system A, but it recovered to a level closer to its original level than system A did. On the other hand, system A suffered a larger disruption and recovered by a larger amount from the disrupted state that system B. So, which system is more resilient? In order to use the level of recovery as an indicator for resilience, it must be calculated involving all the levels of performances of the original state, disrupted state and the recovered state. Some define resilience to be the capacity to tolerate disturbances – this means that there is no disrupted state (Fiksel 2003). This indicates that in addition to the three levels indicated above the potential disrupted state that was avoided should also be included in indicating the level of resilience. But further study is required to make these indications. In some other cases, the initial state itself could be a disrupted state or one full of challenges and difficulties – e.g. a startup or a small system that is competing with larger and well established systems.

## *Level of Vulnerability to Potential Disruptions*

The level of vulnerability to potential disruptions can also be an indicator of system resilience. It is important to note that a system that is resilient to one kind of disruption may not be as resilient to another type of disruption. This leads us to a possible definition of a measure of overall resilience of a system. This could be a function of the individual resilience of the system to various disruptions. As we begin to consider the integration of these correlated metrics of resilience, it would be very useful to examine concrete cases. In this way we could come to an understanding of both resilience and its opposite, that is, vulnerability to disruptions of various kinds:

**Scenario 1.** Immediately after the terrorist attacks of September 11, 2001, there was a sudden increase in US flags, lapel pins and other patriotic items. Wal-Mart noticed this and by the evening of 9/11/2001, it had ordered all US flags in its entire supply chain. Other retailers like Kmart and Target were too late to respond to the new demand, and their stocks emptied very quickly. So for some time, shoppers could find US flags only in Wal-Mart (Pal 2005).

**Scenario 2.** In 2002, a 10-day labor lockout shut down 29 ports on the US West Coast. This affected hundreds of cargo ships that had reached the pacific shores, and hundreds on the way and about to leave from ports in Asia. This disrupted supply chains of all companies that depended on the supply of goods via the west coast ports. Like most of these affected companies, Dell too was expected to be severely affected by the lack of parts, more so with its just-in-time manufacturing model. But the same model kept Dell constantly in touch with its suppliers and the port situation and predicted the port lockout. Dell then chartered 18 Boeing 747s to ship all the parts it needed from Asia, and survived the lockout without delaying delivery to even a single customer (Breen 2004). Other companies like Apple could not satisfy customer demands and took much longer to recover from the supply chain disruption due to the west coast port lockout.

**Scenario 3.** An earthquake that hit Taiwan on September 21, 1999, affected the supply of semiconductors to many computer manufacturers. Apple faced a shortage of chips and other critical components for its latest laptop and desktop models. Thousands of orders had already been placed, and it was too late to modify the configurations with other earlier versions of components. Apple was left with no choice but to refund payments, and this severely affected its sales figures. Dell on the other hand, faced a similar shortage of supply, but in its model there was much lesser time from order to supply and hence it did not suffer backlogs of thousand of orders. It offered only models that it had parts for, and hence sold only them – this enabled Dell to survive the disruption and also increase its sales in that quarter (Sheffi and Rice Jr. 2005).

**Scenario 4.** Lighting struck a Philips semiconductor plant in New Mexico on March 17, 2000 and caused a small fire that polluted the clean room facility and destroyed thousands of chips. These chips were being supplied to many companies including two cell phone giants Nokia and Ericsson. Nokia was about to rollout a new model, and it depended on chips from the affected Philips lab. Nokia immediately realized the potential damage due to this disruption, and went on fast track to collaborate with Philips and source the chips from other Philips plants located in other parts of the world. As a result Nokia avoided disrupting supply to any of its customers. Ericsson on the other hand, waited for the situation to be handled by Philips, and lost millions of dollars. It eventually was bought over by Sony (Sheffi 2005).

The four scenarios briefly describe how some companies were able to avoid or reduce the impact while others were majorly affected by the same disruption. It is possible to compare the responses of the two companies based on a set of criteria, and this could lead to a qualitative measure of the resilience of the companies. The level of vulnerability to certain types of disruptions can a meaningful metric if it can be integrated with the metrics that we have proposed which are level of and time to recovery.

## Discussion and Conclusions

This paper reviewed some of the existing resilience measurement methodologies from which to develop a comprehensive methodology for measuring system resilience. Although its importance has been frequently emphasized in the literature, there is a lack of proposed methodologies attempting to measure resilience. The challenge resides in the certain characteristics of the concept of resilience. First, measuring resilience is a difficult task which requires a thorough understanding of the complex interrelationships and interdependencies of a system and its environment. Second, resilience is an emergent attribute of a system, which may not be measured during the normal operation of the system. In order to measure resilience, it is important to identify the inherent attributes of the system which will evolve and contribute to its ability to be resilient. The dynamic rather than the static measurement of system attributes requires both new understandings of systems as well as new methodologies of measurement.

Most of the literature provide conceptual approaches to measuring resilience where few attempts for empirical measurement of resilience. One major reason for this is that resilience can only be measured with some variables which exist in the present that will determine system resilience at some point in the future. This also leads to the importance of selection of variables for a proper measurement of resilience. This is easy in disciplines like material science, but difficult in others. It is difficult to operationalize “resilience” due to its abstract and multidimensional nature. In most cases, especially when the complex systems are being studied, it is difficult to identify which variables should be measured.

In this paper, based on the literature review we emphasized the need to have well-defined quantitative and qualitative metrics in order to evaluate resilience. We proposed some quantitative metrics that took into account the dynamic, organic features of complex systems, and thus our methodology took into account the crucial parameters of recovery time, level of recovery, initial vulnerability, and potential loss averted. Further study will expand on the crucial area of correlation between the various aspects of system resilience. In addition, other categories of measurement will be necessary in order to more accurately assess reactions to particular disruptive events. It is easier to measure resilience when it seems to have been manifested over time, in commercial success stories. However, the field is open for new and comprehensive modes of measurement.

## References

Adger, W. (2000). "Social and ecological resilience: Are they related? ." Progress in Human Geography **24**(3): 347–364.

Arsenault, D. and A. Sood (2007). Resilience: A Systems Design Imperative. GMU-CIPP Critical Thinking Series. Fairfax, VA, Department of Computer Science, George Mason University.

Arthur, W. (1999). "Complexity and the economy." Science **284**(5411): 107-109.

Baruth, K. E. and J. J. Carroll (2002). "A Formal Assessment of Resilience: The Baruth Protective Factors Inventory." Journal of Individual Psychology **58**(3): 235-235.

Berkes, F. (2007). "Understanding uncertainty and reducing vulnerability: lessons from resilience thinking." Nat Hazards **41**: 283–295.

Bonanno, G. (2004). "Loss, trauma, and human resilience: have we underestimated the human capacity to thrive after extremely aversive events? ." American Psychologist **59**(1): 20-28.

Breen, B. (2004). Living in Dell Time. Fast Company. **88**.

Callaway, D., M. Newman, et al. (2000). "Network robustness and fragility: percolation on random graphs." Physical Review Letters **85** (25): 5468–5471.

Carpenter, S., B. Walker, et al. (2001). "From Metaphor to Measurement: Resilience of What to What?" Ecosystems **4**: 765–781.

Christopher, M. and H. Peck (2004). "Building Resilient Supply Chain." International Journal of Logistics Management **15**(2): 1-13

Connor, K. M. and J. R. T. Davidson (2003). "Development of a new resilience scale: The Connor-Davidson Resilience Scale (CD-RISC)." Depression & Anxiety (1091-4269) **18**(2): 76-76.

Cumming, G., G. Barnes, et al. (2005). "An Exploratory Framework for the Empirical Measurement of Resilience." Ecosystems **8**(8): 975-987.

Dalziell, E. P. and S. T. McManus (2004). Resilience, Vulnerability, Adaptive Capacity: Implications for System Performance. International Forum for Engineering Decision Making (IFED). Stoos, Switzerland.

Erol, O., B. Sauser, et al. (2009). "A Framework for Investigation into Extended Enterprise Resilience." Enterprise Information Systems **Accepted for publication**(In print).

Fiksel, J. (2003). "Designing Resilient, Sustainable Systems." Environmental Science and Technology **37**(23): 5330-5339.

Fiksel, J. (2006). "Sustainability and Resilience: Toward a Systems Approach." Sustainability: Science, Practice, & Policy **2**(2): 14-21.

Folke, C., S. Carpenter, et al. (2002). "Resilience and sustainable development: building adaptive capacity in a world of transformations." Ambio **31**(5): 437–440.

Fricke, E. and A. P. Schulz (2005). "Design for Changeability (DfC): Principles To Enable Changes in Systems Throughout Their Entire Lifecycle." Systems Engineering Journal **8**(4): 342-359.

Gallopin, G. C. (2006). "Linkages between vulnerability, resilience, and adaptive capacity." Global Environmental Change **16**: 293–303.

Gibbs, M. T. (2009). "Resilience: What is it and what does it mean for marine policymakers?" Marine Policy **33**: 322–331.

Goble, G., H. Fields, et al. (2002). Resilient infrastructure, IBM Global Services.

Gunderson, L. H. and L. J. Pritchard, Eds. (2002). Resilience and the Behaviour of Large-Scale Systems. SCOPE Series Washington DC., Island Press.

Haimes, Y. Y., K. Crowther, et al. (2008). "Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems." Systems Engineering **11**(4): 287-308.

Hoffman, E. (2007). Building a Resilient Business. Raptor Networks Technology Inc.

Holling, C. S. (1973). "Resilience and stability of ecological systems." Annual Review of Ecology and Systematics **4**: 1-23.

Hollnagel, E., D. D. Woods, et al., Eds. (2006). Resilience engineering: Concepts and precepts. Hampshire, Ashgate.

Mallak, L. (1999). Toward a Theory of Organizational Resilience. Portland International Conference on Technology and Innovation Management. PICMET, IEEE. **1:** 223.

McManus, S., E. Seville, et al. (2007). Resilience Management: A Framework for Assessing and Improving the Resilience of Organisations. New Zealand, Resilient Organizations.

Merriam-Webster Merriam-Webster Online Dictionary.

Najjar, W. a. J.-L. G. (1990). "Network Resilience: A Measure of Network Fault Tolerance." IEEE Transactions on Computers **39**(2): 174-181.

Omer, M., R. Nilchiani, et al. (2009). "Measuring the Resilience of the Trans-Oceanic Telecommunication Cable System." Systems Journal, IEEE **3**(3): 295-303.

Orwin, K. H. and D. A. Wardle (2004). "New indices for quantifying the resistance and resilience of soil biota to exogenous disturbances." Soil Biology and Biochemistry **36**(11): 1907-1912.

Pal, N. a. M. L., Ed. (2005). The Agile Enterprise: Reinventing Your Organization for Success in an On-Demand World. Emergence of the Agile Enterprise. New York, Springer-Verlag.

Paries, J. (2006). Complexity, Emergence, Resilience... Resilience Engineering: Concepts and Precepts. E. Hollnagel, D. D. Woods and N. Leveson. Aldershot, UK, , Ashgate Press, **:** 43-53.

Qiao, J., D. Jeong, et al. (2007). "Allocating security resources to a water supply network." IIE Transactions **39**(1): 95-109.

Reed, D. A., K. C. Kapur, et al. (2009). "Methodology for Assessing the Resilience of Networked

Infrastructure." Systems Journal, IEEE **3**(2): 174-180.

ResilienceAlliance (2008). Resilience Alliance Key Concepts. (www.resalliance.org).

Rose, A. and S. Liao (2005). "Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions." Journal of Regional Science **45**(1): 75-112.

Rosenkrantz, D. J., S. Goel, et al. (2009). "Resilience Metrics for Service-Oriented Networks: A Service Allocation Approach." Services Computing, IEEE Transactions on **2**(3): 183-196.

Sheffi, Y. (2005). The Resilient Enterprise. Overcoming Vulnerability for Competitive Advantage. Cambridge, Massachusetts, MIT Press.

Sheffi, Y. and J. B. Rice Jr. (2005). "A Supply Chain View of the Resilient Enterprise." MIT Sloan Management Review **47.1**(Fall): 41-48.

Smith, B. W., J. Dalen, et al. (2008). "The Brief Resilience Scale: Assessing the ability to bounce back." International Journal of Behavioral Medicine **15**(3): 194-200.

Starr, R., J. Newfrock, et al. (2003). Enterprise Resilience: Managing Risk in the Networked Economy. Strategy+Business, Booz & Company. **Spring 2003**.

Stevenson, M. and M. Spring (2007). "Flexibility from a supply chain perspective: definition and review." International Journal of Operations & Production Management **27**(7).

Todini, E. (2000). "Looped water distribution networks design using a resilience index based heuristic approach." Urban Water **2**(2): 115-122.

van Opstal, D. (2007). The Resilient Economy: Integrating Competitiveness and Security, Council on Competitiveness

Vogus, T. J. and K. M. Sutcliffe (2007). Organizational Resilience: Towards a Theory and Research Agenda. Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on.

Walker, B. and J. A. Meyers (2004). "Thresholds in ecological and social–ecological systems: a developing database." Ecology and Society **9**(2).

Walker, B., S.;, J. Carpenter, et al. (2002). "Resilience management in social-ecological systems: a working hypothesis for a participatory approach." Conservation Ecology **6**(1): 14-31.

Weick, K. E. and K. M. Sutcliffe (2001). Managing the Unexpected. San Francisco, Jossey-Bass.
Westrum, R. (2006). A typology of resilience situations. Resilience Engineering: Concepts and Precepts. E. Hollnagel, D. D. Woods and N. Leveson. Aldershot, UK, , Ashgate Press, **:** 49-60.

Woods, D. D. and E. Hollnagel (2006). Prologue: Resilience Engineering Concepts. Resilience Engineering: Concepts and Precepts. E. Hollnagel, D. D. Woods and N. Leveson. Aldershot, UK, , Ashgate Press, **:** 49-60.

Wreathall, J. (2006). Developing Models for Measuring Resilience. Dublin, Ohio, John Wreathall & Co., Inc.

Yao, H., L. Jingshan, et al. (2008). Towards modeling of resilience dynamics in manufacturing enterprises: Literature review and problem formulation. Automation Science and Engineering, 2008. CASE 2008. IEEE International Conference on.

Zhang, W. (2008). Resilience Engineering – A New Paradigm and Technology for Systems. Canada, University of Saskatchewan.

# Biography

**Ozgur Erol.** Ozgur Erol holds a B.S. degree in industrial engineering and a M.S. degree in engineering management from Istanbul Technical University, and a MBA degree from Saint Joseph's University. She is currently a Ph.D. candidate in the School of Systems and Enterprises at Stevens Institute of Technology and an adjunct professor at Saint Joseph's university. She has worked in the area of systems analysis, project management, and reengineering of information systems prior to joining the PhD program. Her research is in the area of enterprise resilience with a special concentration in extended enterprises and enterprise architectures. Ms Erol is a member of International Council on Systems Engineering and Institute of Industrial Engineers (IIE).

**Devanandham Henry.** Devanandham Henry is currently a Lecturer and Doctoral Candidate at the School of Systems & Enterprises, Stevens Institute of Technology. He was president of the INCOSE student chapter at Stevens during 2007-08. Before joining Stevens in 2006, he spent nine years with the Aeronautical Development Agency (Ministry of Defense, Government of India), He has a B.Sc. in Physics from the University of Madras (1994), a B.Tech. in Aeronautical Engineering from the Madras Institute of Technology, Anna University (1997) and an M.Tech. in Aerospace Systems Engineering from the Indian Institute of Technology – Bombay (2002).

**Brian Sauser.** Brian Sauser holds a B.S. from Texas A&M University in Agricultural Development with an emphasis in Horticulture Technology, a M.S. from Rutgers, The State University of New Jersey in Bioresource Engineering, and a Ph.D. from Stevens Institute of Technology in Project Management. He is currently an Assistant Professor in the School of Systems & Enterprises at Stevens Institute of Technology. Before joining Stevens in 2005, he spent more than 12 years working in government, industry, and academia both as a researcher/engineer and director of programs. His research interest is in the management of complex systems. This includes system and enterprise maturity assessment and the advancement of a foundational science of systems thinking. He is currently the Director of the Systems Development and Maturity Laboratory (http://www.systems-development-maturity.com), which seeks to advance the state of knowledge and practice in systems maturity assessment. He teaches courses in Project Management of Complex Systems, Designing and Managing the Development Enterprise, and Systems Thinking. In addition, he is a National Aeronautics and Space Administration Faculty Fellow, Editor-in-Chief of the Systems Research Forum, an Associate Editor of the IEEE Systems Journal, and the Associate Editor of the ICST Transactions on Systomics, Cybernetics, and e-Culture.