Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 28 (2014) 565 – 574

Procedia Computer Science

Conference on Systems Engineering Research (CSER 2014)

Eds.: Azad M. Madni, University of Southern California; Barry Boehm, University of Southern California; Michael Sievers, Jet Propulsion Laboratory; Marilee Wheaton, The Aerospace Corporation
Redondo Beach, CA, March 21-22, 2014

Resilience Analysis of Soft Infrastructure Systems

Mayada Omer[a]*, Ali Mostashari[b], Udo Lindemann[a]

[a]*Technical University of Munich, Institute of Product Developmment, 85748 Garching, Germany*
[b]*Stevens Institute of Technology, School of Systems and Enterprises, Hoboken NJ 07030-5991, USA*

Abstract

Infrastructure resilience is often associated with the ability of the hard infrastructure or physical system to cope with severe disruptions; however, the institutions and enterprises that make up the soft infrastructure systems are also prone to crises. Incorporating resilience aids systems to cope with crises and recover from disruptive events, which is not possible without an organizational foundation that is able to cope with and respond to crisis. Additionally, metrics enable stakeholders to assess the effectiveness of resilience strategies and show their added value.
This paper outlines a methodology for assessing resilience of soft infrastructure using social network analysis. The methodology is applied to the National Intelligent Transportation System (ITS) where the logical architecture is viewed as a network, and the centrality measures are used to define the system's resilience metrics.

Keywords: Resilience metrics, organizational networks, soft infrastructure system, social network analysis

* Corresponding author. Tel.: +49-89-289-15155; fax: +49-89-289-15144.
E-mail address: mayada.omer@pe.mw.tum.de

doi:10.1016/j.procs.2014.03.069

1. Introduction

Infrastructure resilience is often associated with the ability of the hard infrastructure or physical system to cope with severe disruptions; however, the soft infrastructure, that is, the institutions and enterprises that are crucial for social and economic continuity are also prone to crises and must be well equipped to overcome them.
Increasing the resilience of soft infrastructures is not a simple matter of drafting scenarios of how to react to crisis; the emergency plans are ineffective without establishing an organizational culture that is aims to achieve resilience. It is also important to evaluate the current resilience and investigate the effectiveness of strategies that contribute to a resilient organization.
Up to date, there are several guidelines and methodologies to help understand organizational resilience and risk mitigation solutions. However, there is limited research that quantitatively assesses resilience of soft infrastructure systems. This paper attempts to fill this gap using a resilience quantification approach that is based on the organizational structure. The organizational structure is viewed as a directed graph, and social network analysis techniques are applied to obtain resiliency values under disruptive events. The resilience metrics allow system developers to estimate the current resilience of the system, and they serve as a bench mark for assessing the effectiveness of resilience strategies and show their added value.
In the transportation infrastructure, the hard infrastructure refers to the physical components such as the roads and bridges. The Intelligent Transportation System (ITS) is a type of governance soft infrastructure that improves the transportation networks by integrating existing communication technologies to the transportation infrastructure. This paper analyzes the resilience of the ITS proposes metrics for measuring its resilience.
The organization of this paper is as follows: The first section of the paper is a literature review of the factors that contribute to organizational resilience. The paper will then go into the details of the resilience assessment process and a case study will be used to demonstrate the applicability of the proposed approach.

2. Resilience in Organizational Systems

The traditional meaning of a system's resilience implicates its ability to bounce back, that is, its ability to recover quickly to continue to perform its task after occurrence of disruptions (1–3). Several suggestions have been put forward by which a system can be made resilient, for example, by making a system less vulnerable to disruptions, or application of adaptive responses in the face of threats, or ideally, a combination of both (4). Execution of resilience strategies requires an organizational foundation that would enable it to behave in a resilient manner. Several key points have been identified from literature that contribute to resilience of organizations shown in Fig. 1.

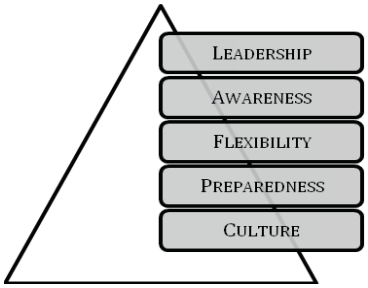

Fig.1. Factors for Achieving Organizational Resilience (5)

- **Leadership**

This is the most important element in organizational resilience, enterprise leaderships is about setting priorities, making commitments and the ability to make the right decisions about the courses of actions to take when faced with adverse situations (6).

- **Awareness**

Resilient organizations monitor change that occurs within the organization and hence are able to identify disruptions in advance. Data gathering provides the management with the current state of affairs and reveal the extent of problem as well as how prepared the organizations is to deal with it (7).

Good communication is key to raising awareness. An organization with a strong communications infrastructure can more easily detect disruptions and alert the responsible persons.

- **Preparedness/Emergency Planning**

Organizations can actively anticipate problems and prepare for them by building a team that is able to imagine different possibilities and is able to apply inventive solutions (8). Frequently deployed and even necessary schemes in emergency planning are the emergency drill-response exercises (6). These exercises prepare the organization to deal with problems by training individuals in the courses of action to take in the event of emergencies.

- **Flexibility**

Flexibility allows organizations to adapt to new problems. Resilience through flexibility is achievable by allowing individuals in the organization to make decisions (7). Flexibility is also achieved by creating redundancy or backup systems. Cross-training within an organization allows individuals to substitute for one another to a certain extent in cases of emergencies.

- **Culture**

Resilience is achieved through a culture that is built on trust and accountability (9); engaging individuals at all levels, by developing a sense of shared purpose encouraging a culture that is more aware of its environment and supporting communication through the organizations (7,8). Organisational culture is believed to be the key to managing crisis, and that the organization culture that makes it crisis-prone or crisis prepared (10).
In organizational theory, loose coupling is a conceptual tool that coordinates the interactions between actors and specifies a certain course of action. Grote (11) suggests the application of loose coupling in organizations to enhance resilience.

3. Resilience Analysis of Soft Infrastructure Systems

Organizational systems are no different from physical systems, as they too are prone to disruptions that limit their capability of executing their intended functionality. The concept of time to recovery is of particular importance, and it is often dictated by the arrangement of the organizational entities and their relationship to each other, that is, the organizational structure. At the occurrence of disruptive events, the system's performance degrades at the initial impact, it then continues to degrade until the recovery efforts are implemented and the performance gradually goes back to its original level or close to it (12), more resilient systems are able to return to their original state in the shortest time possible.
So far, there is limited research of metrics that quantifies resilience of soft infrastructure systems. This paper attempts to fill this gap by proposing resilience metrics by viewing the organizational structure as a directed graph where the organizational entities are the network nodes and the relationship between the entities are the network links. The analysis process is carried out using a 3-stage process, where each stage is made up of a series of steps. Fig. 2. shows a high level description of the analysis framework. The outlined framework aids decision makers to analytically quantify the system's resilience, identify the most critical segments of the network and assess the effectiveness of resilience strategies.

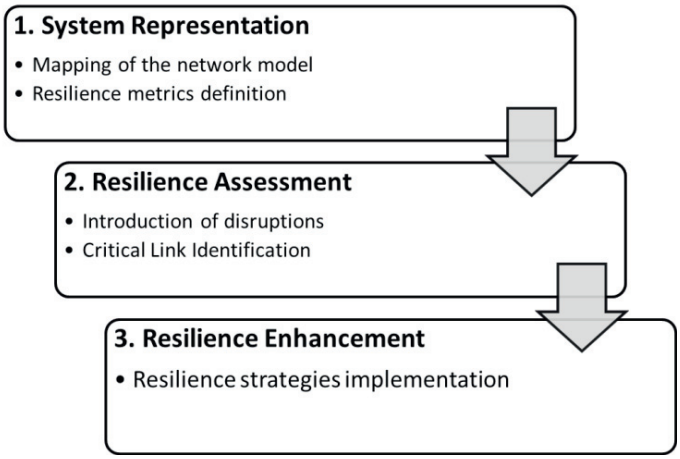

Fig. 2. Resilience Analysis Process

In the first stage, the system is represented by a network model and the resilience metrics are defined. In the second step, hypothetical disruptions are imposed on the system in the form of link disruptions in order to evaluate the impact of disruptions on the resilience metrics. The third step of the analysis process investigates the impact of resilience strategies on the predefined resilience metrics.
In the following sections, the resilience analysis process is applied to the National Intelligent Transportation System (ITS) architecture (5).

3.1. Stage 1 - System Representation

3.1.1. Mapping the Network Model

The system chosen for conducting the resilience analysis is the national ITS architecture. The national ITS architecture provides a framework for planning, programming, and implementing intelligent transportation systems. It is made of three layers; the Institutional Layer, the Transportation Layer and the Communications Layer. The institutional layer includes institutions, policies and processes required for the implementation, operation and maintenance of the ITS. The Transportation Layer defines the physical and logical architectures that include details of the subsystems and interfaces as well as the functionality required for each transportation service. The Communications Layer described how the sub-systems or system elements communicate with each other.

In this paper, the resilience analysis process is applied to the logical architecture of the Transportation Layer. The logical architecture includes detailed information of the functions as well as the shared information flow between them. Functions in the logical architecture are known as processes and the shared information between the functions are the data flows. The logical architecture is made up of several hierarchical levels; each level is described by a Data Flow Diagram (DFD).

The resilience analysis is based on the reactions of the system to emergency situations. Fig. 3 shows the emergency interactions extracted from the National ITS logical architecture(13).

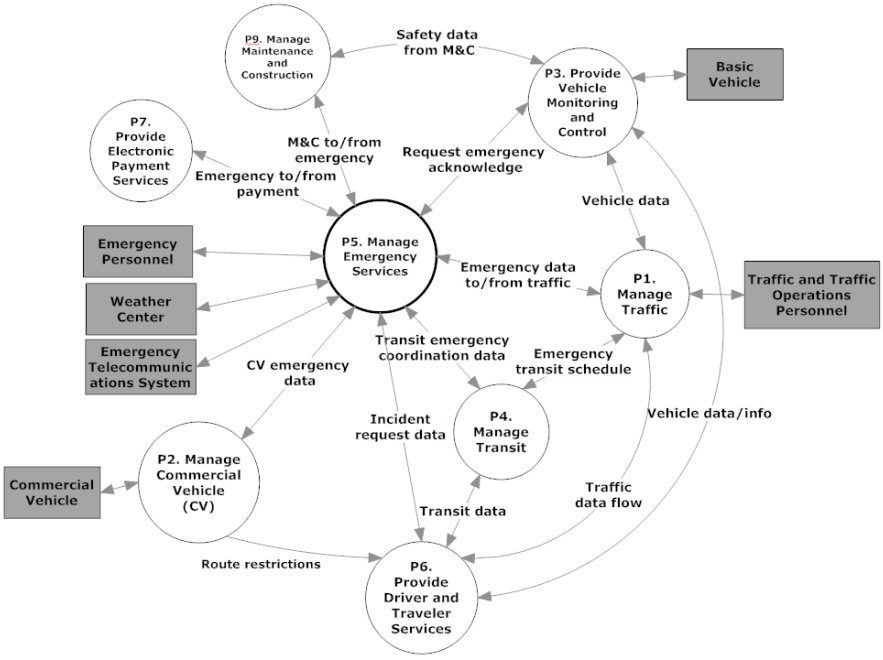

Fig.3. Emergency Interactions Extracted from the National ITS Logical Architecture
Source: http://www.iteris.com/itsarch/html/menu/laindex.htm

The equivalent network model for the emergency operation is shown in Fig. 4.

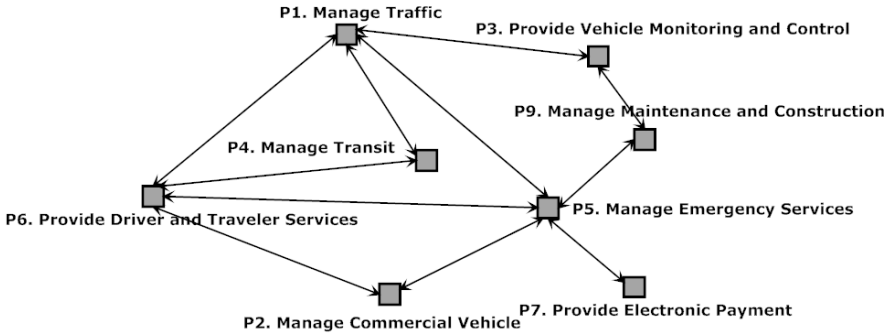

Fig.4. Network of Emergency Operations

3.1.2. Resilience Metrics Definitions

Soft infrastructure systems are non-physical systems and thus require a modelling approach that is targeted for social systems. Social network analysis is an analysis technique that is based on graph theory where social relationships are viewed as nodes and links. For organizational systems, the nodes in the social network represent the organizational entities and the links represent the relationship (e.g. information flow) between them.
A social network is characterized in terms of its centrality measures that describe the importance or popularity of a node in a network. The three most important centrality measures are degree, closeness and betweeness. Degree centrality refers to the number of direct connections to a node. Closeness centrality determines how accessible a

node is to the rest of the network and betweeness centrality determines how often a node lies in the shortest path between other nodes in the network (14).

A considerable amount of research focused on investigating the network resilience using social network analysis where the resilience was analysed by removing network links and nodes. The network centrality measures were used to determine the best strategies for investigating resilience. For example, the betweeness centrality is a measure of how often a node lies in the shortest paths between other nodes in the network. Networks with a higher average node betweeness are less resilient since one node lies in numerous paths (15).

We propose to use closeness centrality as a resilience measure. The closeness centrality determines how accessible one node is to the rest of the network. Since the essence of resilience is recovery time, we added a time factor to the traditional definition of the closeness centrality measure, in order to determine the amount of time it takes the flow to reach the node.

We measure resilience as the ratio of the closeness centrality of the network before a disruption, and after a disruption. Therefore, the resilience value varies from 0 to1 with 1 as the maximum attainable resilience. This relationship for measuring resilience has been applied to physical infrastructure system (16,17), this paper demonstrates the applicability of this relationship to soft infrastructure systems. Assuming that the time it takes for information to travel between nodes *i* and *j* is *t*, we propose that the closeness centrality of node *v* can be measured as shown in Equation (1). The information flow time depends on the type of network under analysis, and the type of operation that has to be executed. Thus, it can vary from a few milliseconds to several minutes.

$$C_c(v) = \frac{\sum_{\substack{s \in V \\ s \neq v}}^{n} d_G(v,s) \bullet t}{n-1} \tag{1}$$

Where

d_G is the geodesic distance between node i and node j

v are the nodes in the network

t is the time it takes for information to flow from node i to node j

n is the number of nodes in the network

The closeness centrality resilience R_{cc} is given by Eq. (2) as the ratio between the closeness centrality resilience before and after shock. As t_{after_shock} approaches infinity, the Resilience R_{cc} approaches 0.

$$R_{cc} = \frac{C_c(v)_{before\_shock}}{C_c(v)_{after\_shock}} \tag{2}$$

Where

$$C_c(v)_{before\_shock} = \frac{\sum_{\substack{s \in V \\ s \neq v}}^{n} d_G(v,s) \bullet t}{n-1} \tag{3}$$

and

$$C_c(v)_{after\_shock} = \frac{\sum_{\substack{s \in V \\ s \neq v}}^{n} d_G(v,s) \bullet t_{after\_shock}}{n-1} \tag{4}$$

3.2. Stage 2 – Resilience Assessment

3.2.1. Critical Nodes Identification

The degree centrality of a node was introduced by Freeman (18), he defined it to be the number of direct links that are connected to the node. Borgatti defines it as the number of paths of length one that emanate from a node (19). A disruption that causes the node with the highest degree to collapse will result in the maximum number of severed links, therefore, we identify those nodes to be the critical network nodes.

A standardized value of the degree centrality of a node is calculated by summing up the links connected to that node and dividing by the sum of the rest of the nodes in the network as shown in Equation (5).

$$C_D(v)_{after\_shock} = \frac{\sum_{i=1}^{n} a(v,s)}{n-1} \quad \text{for} \quad s \in V, \tag{5}$$

Where

a is a link connected to node v,
V are the nodes in the network,
k is the number of nodes connected to node v, and
n is the number of nodes in the network.

Another measure that is frequently used to determine the most important nodes in the network is the eigenvector centrality. It is a more sophisticated version of the degree centrality as it takes into account the type of direct link that is connected to a node. A higher node eigenvector values means that the node is connected to other "more important" nodes in the network (20). However, the eigenvector centrality can only be applied to symmetric networks.

3.2.2. Disruption Scenarios

The resilience of the network is assessed by introducing of hypothetical disruptions to the network. Under normal operating conditions, the resilience value is 1. This means that the network is functioning in the expected manner. Depending on how resilient a network is, a disruption will deteriorate the functionality, and will make the resilience metric approach 0. Therefore, more resilient networks have resilience values of 1 or close to it.
The disruptions are introduced in the form of decreasing the capacity of the link or severing the link completely. Reducing the number of links will consequently increase the workload in the remaining links. As a result, the time it takes for the data flow to be sent or received increases. There are several studies such as that of Andre (21) that try to establish a relationship between the increase in workload and time to task completions, their research shows that there is an almost linear relationship between the workload and time to task completion, after a variable threshold of time, resources are exhausted and an increase in workload and breakdown in performance are likely to occur. For the sake of simplicity, we assume that there is a linear relationship between the increase in workload and the time to complete the task; this relationship is defined by Equation (6). However, a more sophisticated mathematical functions such as an exponential function maybe more suitable for describing the relationship between workload and time to task completion.

$$t_{after\_shock} = \lambda t \tag{6}$$

Where λ is the coefficient that reflects the increase in time as a result of increasing the workload and t original information flow time. The closeness centrality resilience is measured by substituting the values of t and t_{after_shock} determined by Equation (6) in Equation (2).

3.2.3. Stage 3 - Resilience Scheme Identification

Resilience schemes allow the network to recover and resume normal functionality in the shortest time possible. In cases of link disruptions, one strategy is to utilize available link capacities for rerouting purposes in addition to their normal work load. This is facilitated by resource allocation and collaboration between the organizational entities.

4. Case Study Results

The program UCINET was used to create the network model (shown in Fig. 2) and to perform the social network analysis.
The degree centrality score was used to determine the most critical node in the network. The node with the highest degree centrality score has the largest number of direct links and the impact of a disruption is maximized if that particular link is affected. Since the network is focused on emergency operations, node P5 "Manage Emergency Services" has as expected the highest possible score, and is therefore the most critical node. The degree centrality scores of the rest of the network nodes are between 57.1 and 14.3, this range of values are much lower than the score of P5. This is an indication that the network is centralized around P5, therefore, disruptions on this node would almost disintegrate the network. Fig. 5 shows the degree scores of all the network nodes.

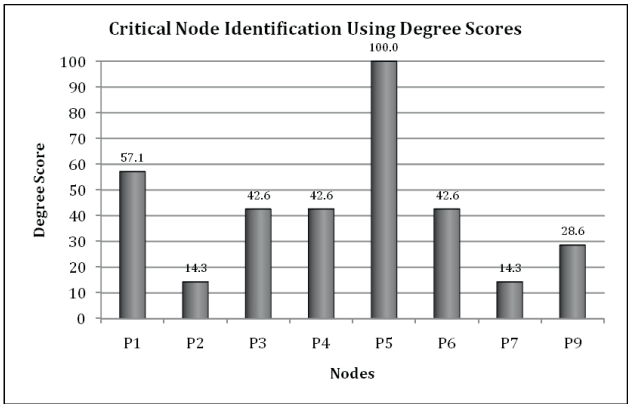

Fig. 5. Critical Node Identification using Degree Scores

The sources of disruptions vary in nature and severity. Three sources of disruptions that result in traffic congestions and loss of time and money are the vehicles on the road such as the basic vehicle and the commercial vehicle as well as an increase in the traffic volumes. The emergency information obtained from these three sources is linked to the ITS network by the processes P1, P2 and P3 as shown in Fig. 6 The vulnerability analysis shows that the most critical node in the network is node P5, therefore, the disruption scenarios were introduced to the links that connect node P5 to node P1, P2 and P3. The disruptions are introduced by deleting network links.
Deleting the link between P1 and P5 increases the time it takes to transfer the information between P1 and P5 since the information has to travel over a longer path as well as the delay due to increasing workload volumes. The delay was measured by assuming a value of 1.1 for λ in Equation (6). This value was chosen to add a small increase in the data transfer time. Using Equations (2)-(4), the closeness resilience metrics for P1 and P5 was calculated to be 0.699 and 0.795 respectively.
Fig. 6 shows the closeness centrality resilience values of P5 when the link between node P5 and nodes P1, P2 and P3 are disrupted in turn.

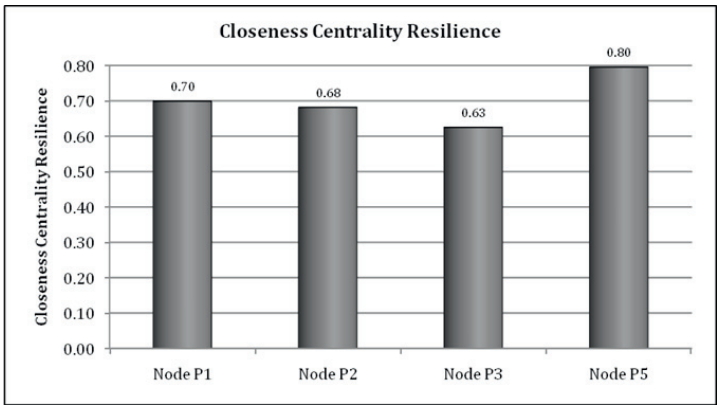

Fig. 6. Closeness Centrality Resilience Values for Nodes P1, P2, P3 and P5

Deleting the link between P1 and P5 in the network model shown in Fig. 4 increases the time it takes to transfer the data between them, since the data has to travel over a longer path. Additionally, it incurs overall network delays due to increasing workload. The delay was measured by assuming a value of 1.1 for λ in Equation (3). Using Equations (1)–(3), the closeness resilience metrics for P1 and P5 were calculated to be 0.68 and 0.80, respectively. The resilience values are shown in Fig. 3.

Resilience strategies allow the system to be as resilient as possible, that is, to keep the resilience values as close as possible to 1. There are two possible scenarios for enhancing resilience with regards to the network structure. In the first scenario, the basic structure of the network remained unchanged. In this case, routing the information over the existing nodes entails reducing the time it takes for transferring the information along the shortest path. In order to maintain a resilience value of 1, the time for transferring the information of the links over the shortest path must be no longer than $0.8t$, which is 20% faster than the normal rate. The graphs shown in Fig. 7. show the closeness centrality resilience with different λ values. The improvement in the resilience metrics values is around 20% for each of P1, P2 and P3 when λ is set to 0.8. P5 exhibits an extremely resilient behaviour for values of λ less than 0.85, the resilience value exceeds 1.

The second scenario reorganizes the network by adding extra links between the disrupted node and the rest of the nodes that are not directly connected so as not to lose the information flow.

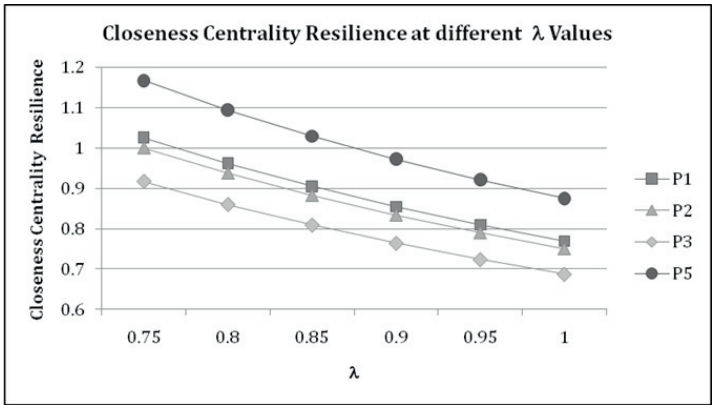

Fig. 7. Closeness Centrality Resilience at different Lambda Value

5. Conclusion

The logical and physical architectures of soft infrastructure systems define their structure, that is, the main functions and how the functions work together as well as the external entities that interact with the system. In this

case study we demonstrated how the logical architectures can be viewed as network system and based the analysis on social network analysis techniques. In social networks, the nodes represent the actors and the links represented the information flow between the actors. Similar logic can be applied to organizational systems where the nodes represent the main functions or processes of the enterprise and the links represent how the functions interact with each other.

There are several measures for quantifying social networks that include degree centrality and closeness centrality. The closeness centrality metric was used for measuring the resilience since it is an indication of how well the information flows through the network. In addition to the traditional definition of the closeness centrality, the link time factor λt was introduced to represent the amount of time it takes for information to flow from one node to another. The degree centrality measures how well a node is connected; this metric was used to identify the most critical nodes in the network that would cause the maximum network damage when disrupted.

Applying this methodology for measuring resilience of organizational networks requires a well-defined physical and logical architectures. Organizational networks are often complex and have several processes running in parallel and a disruption may impact only some of the processes. A resilience analysis requires careful identification of the impacted systems and subsystems.

References

1. Fiksel J. Designing Resilient, Sustainable Systems. J. Environ. Sci. Technol. 2003;37(23):5330–9.
2. Folke C, Carpenter S, Elmqvist T, Gunderson L, Holling C, Walker B. Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations. A J. Hum. Environ. [Internet]. 2002;31(5):437–40. Available from: http://www.ima.kth.se/utb/mj2694/pdf/Folke.pdf
3. Rose A, Liao S-Y. Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions. 2005 Feb 45(1):75–112.
4. Dalziell EP, McManus S. Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. Int. Forum Eng. Decis. Mak. Stoos, Switzerland;
5. Omer M. The Resilience of Networked Infrastructure Systems: Analysis and Measurement. World Scientific; 2013.
6. O'Rourke TD. Critical Infrastructure, Interdependencies, and Resilience. Eng. Threat Nat. Disasters. 2007;37(1). Available from:
7. Wreathall J. Properties of Resilient Organizations: An Initial View. In: Hollnagel E, Woods DD, Leveson N, editors. Resil. Eng. Concepts Precepts. 2006. p. 275–85.
8. Johnson-Lenz P. Six Habits of Highly Resilient Organizations. People Place. 2009;1(3).
9. Bell M. The Five Principles of Organizational Resilience. 2002.
10. Mitroff II, Pauchant T, Finney M, Pearson C. Do (some) organizations cause their own crises? The cultural profiles of crisis-prone vs. crisis-prepared organizations. Organ. Environ. 1989 Jan 1;3(4):269–83.
11. Grote G. Rules management as source for loose coupling in high-risk systems. Resil. Eng. Perspect. Remain. sensitive to possibility Fail. Ashgate Publishing Ltd; 2008.
12. Sheffi Y. The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage. The MIT Press; 2007.
13. Architecture Development Team: National ITS Architecture - Logical Architecture,Volume I. Research and Innovative Technology Administration - US Department of Transportation (USDOT); 2012
14. Freeman L. The SAGE handbook of Social Network Analysis. Scott J, Carrington PJ, editors. SAGE publications Inc.; 2011.
15. Newman MEJ. The structure and function of complex networks. SIAM Rev. 2003;45:167–256.
16. Omer M, Nilchiani R, Mostashari A. Measuring the Resilience of the Global Trans-oceanic Cable System. IEEE Syst. J. 2009;3(3):295–303.
17. Omer M, Mostashari A, Nilchiani R, Mansouri M. A Framework for Assessing Resiliency of Maritime Transportation Systems. Marit. Policy Manag. J. 2012;39(7):685–703.
18. Freeman L. Centrality in Social Networks: Conceptual Clarification. Soc. Networks. 1979;1:215–39.
19. Borgatti SP. Centrality and network flow. Soc. Networks. 2005;27(1):55–71.
20. Newman MEJ. The New Palgrave Encyclopedia of Economics. In: Blume L., Durlauf S., editors. Math. networks. 2008.
21. Andre. Theoretical workload performance plot as a function of time. 2001.