*Advances in Intelligent Systems Research, volume 153*

International Conference on Applied Mathematics, Modeling and Simulation (AMMS 2017)

# A Resilience Engineering Based Analysis Framework for Network Systems

Fuchun Ren, Jian Jiao*, Zihan Zhang and Tingdi Zhao

School of Reliability and Systems Engineering, Beihang University, Beijing, China

*Corresponding author

***Abstract*—Many real-world systems can be abstracted into network systems. They have made a great contribution to human daily life, however, risk and disadvantages of these network systems are also serious since a tiny fault may lead to a big disaster. So the ability of resilience that a system can response to an adverse disruption and recovery back to the normal condition after disruptions is needed for modern systems. This paper mainly proposed a resilience analysis framework based on the resilience engineering concept and numerical simulations are put forward based on a generated scale-free network. The simulation results reveal that factors of component reliability, failure propagation failure detection, and recovery strategy would indeed contribute to the resilience of network systems.**

***Keywords-resilience engineering; resilience analysis; network systems***

## I. INTRODUCTION

In modern society, many real-world systems, such as internet, transportation network and power grid system [1-3], can be abstracted into network systems. Basic network systems are usually constructed by nodes and edges where nodes represent fundamental system elements and edges represent interdependency relationships between them. In usual, they can be very large and complex and the reliable and safe operation of these networked systems are very necessary.

In the real world, many factors may threaten the performance of a network system. For example, the reliability of fundamental system elements is one basic factor determining system efficiency and safety. Methods like FMEA [4], FTA [5] are some of the traditional reliability analysis methods providing support to system reliability design. However, the stability of an individual component in networks is determined not only by its own intrinsic properties, but also by its interdependency relationships with other components. In another word, a local deviation in one component may trigger a cascading deviation in another component due to complex interdependencies [6,7] and usually this kind of cascading impact could be hard to accept, for example, the power grid blackout of North America in 2003 [8] in which a fault of three extra-high voltage transmission led to a cascading effect in power system affecting about 50 million people and caused an economic loss of 4 billion to 10 billion.

Real-world traumatic experiences reveal a fact that engineering a safer and more reliable system has been an important mission for the engineers and experts. Numbers of efforts have been put into practice to protect modern systems from severe failures and disruptions. However, this reliability engineering based work pays more attention to the goal of normal operation against failures. Only engineering and embedding reliability properties into modern system alone can no longer satisfy the constantly changing demand, moreover some intrinsic risks of modern systems are not able to get rid of, and sometimes incidents or accidents may happen when there is even no failure occurring since a dysfunction in the system may also threaten the normal operation of modern systems, for example, the U.S. F15 shot down "Black Hawk" helicopter by mistake in April 1994 could reveal that logic defects could lead to an accident even without physical failures due to system complexity and lack of "logic completeness". To guarantee the efficiency and safety, a demand changing from reactive safety and reliability to proactive safety and reliability is necessary. Then the resilience feature that a system can continue to work even a disruption occurs is needed for modern systems.

Before the tentative definition of resilience, a number of similar researches have been put forward using related terms. For example, the European research organization Resilience Alliance [9] has been exploring the dynamics of social-ecological systems since 1999 and the community of Information Systems for Crisis Response and Management (ISCRAM) [10] in crisis response field. Until 2006 a symposium was organized to debate the present and future of resilience engineering as the notion of resilience had gradually emerged as a logical way to overcome the limitations of existing approaches to risk assessment and system safety [11]. Then the term of resilience engineering got into the eye of public as an advancement of risk management theory and technology, which would provide a complement for beforehand mitigation efforts of prevention and protection since not all the incidents, or accidents could be perceived and prevented with the limitation of human cognition. Originally, resilience concept is proposed for the purpose of risk management, and embedding resilience into the system constructing work would provide a new assistance to achieve a robust and dependable system for system engineers. Now resilience has come to be a new property of system which gets universally discussed in diverse domains, such as social [12], economic [13] and engineering domain [14] in the past few years. While the original meaning of the word "resilience" is "bounce back", resilience mainly focuses on the ability of a system to prepare, response to an adverse disruption and recovery to the normal condition after the disruption.

This paper mainly proposes a resilience analysis framework based on the resilience engineering concept, four factors

component reliability, failure propagation failure detection, and recovery strategy are taken into account in the analysis framework. The remainder of this article is organized as follows. Section II proposes the resilience analysis framework on the basis of a discussion of some representative resilience definitions and measures. In section III, analyses of the resilience with numerical simulations are provided based on a generated scale-free network. Finally, a conclusion of this paper is provided in section IV.

## II. Definition and Measure of Resilience in Network Systems

In general, the definition of resilience is discipline depended and the measure of system resilience can be different with the perspective and interest. So at the front of this section, a discussion of some representative viewpoints of resilience definitions and measures is provided.

### *A. General Definition and Measure of Resilience*

For the definition of resilience, Bruneau et al. [15] defined resilience from four dimensions using the resilience triangle model: (1) robustness: the ability to prevent damage propagation through the system; (2) rapidity: the speed or rate at which a system return to its original state; (3) resourcefulness: the level of capability in applying resource; (4) redundancy: the extent to which carried by a system to minimize the likelihood and impact of disruptions.

To measure the network resilience of Internet, Sterbenz et al. [16] presented an architectural framework based on a two-phase strategy where six factors of defend, detect, diagnose, remediate, refine and recover contribute the network resilience. In short, this architectural framework accounts for the pre-disaster efforts of defend, and the recognition of faults with the post-disaster efforts of recovery. Based on this framework, Sterbenz et al. evaluated network resilience through a multilevel two-dimensional state space with operational and service dimensions. On the other hand, Omer et al. [17] proposed the ratio of closeness centrality of the network before and after a disruption as the resilience metric for infrastructure networks. Closeness centrality is a basic kind of network property that can represent the accessibility of a node to the rest of the network.

Differently, Vlacheas et al. [18] proposed an ontology method towards end-to-end network resilience which had direct relationships with the classes of threat, agent, domain, properties, threats and means. Resilience was enabled by cognitive aspects in the end-to-end resilience ontology, and it would help identify the principal network resilience concept. Chen and Miler-Hooks [19] quantified the transportation network resilience by the post-disruption excepted fraction of demand that can be satisfied within pre-determined recovery budgets. But, it is lack of the consideration of recovery time factor. And it paid more attention to the prepared work while the specification of recovery activity was barely discussed.

### *B. Resilience Engineering based Analysis Framework*

As discussed above, many differences can be seen that definition and measure varies with the perspective and interest. Therefore, there is no unified metric for the resilience and also there is no need to put them into one stiff form. In real world, some disruptive events are unpredictable and inevasible while the recovery strategies are put forwards with tradeoff of resource allocation.

In reference with Bruneau et al. four-dimension resilience definition way, in our opinion the robustness dimension of network systems resilience could be represented by the cascading failure effect after the disruptive event or self-reliability question; the rapidity dimension of network systems resilience is represented by time-dependent recovery strategy for the failure nodes; the resourcefulness dimension of network systems resilience is represented by cost of recovery strategy which can be unified into the unit of dollar; in this paper we just consider the resilience after a disruption so the redundancy dimension is excluded in network systems resilience.

Under the assumptions that all the components in network systems have a specific failure rate $\rho_i$, and the failure could propagate to its neighbors with a probability of $\sigma_i$, all the failures could be detected with a probability of $\tau_i$ at every time step, then a recovery strategy $RS_i$ would be put forwards with corresponding recovery time $t(RS_i)$ and resource consumption $d(RS_i)$ after the detection, then the system behavior after a disruptive event can be described as follow: firstly, some of the components in network systems are destroyed by the disruptive event and then some other components get failed due to interdependency relationships with initial destroyed components, this cascading failure phenomenon may last for a few steps and normal components would be infected sequentially, need to say, at each step along the evolution process a normal component may get failed subjecting to a failure rate which represents the reliability feature of the components. Further, to reflect the resilience property of system, recovery strategy should be put forward to help the failed components return back to normal, however, in actual, it would consume resource (time and money) to detect and maintain the failure. So with the limitation of resource, the resource allocation strategy would also contribute to the strength of system resilience.

In summary, four factors of component reliability, failure propagation, failure detection, and recovery strategy should be taken into account in the analysis framework. In reference with metric of network property in [18], in this paper, we propose the failure node ratio of the total number as a metric of the network performance and resilience is measured from the time dimension.

## III. Resilience Analysis with Numerical Simulation

In real world, network systems like the Internet, WWW are found to satisfy the feature of scale-free and can be described by scale-free network model [20]. The scale-free network with degree distribution P(k) gives a power-law behavior $P(k) \sim ck^{-\gamma}$ where P(k) is the probability that the degree of a node in the network is equal to k and $\gamma$ is scale-free network exponent assigned to a positive real number. Barabási and Albert (BA) argued that the generation of networks in the scale-free structure is based on two rules: growth and preferential

attachment [20]. In this section, we adopt a BA scale-free model which is constructed with the parameters n=1000, $m_0$=3, Δm=3, P(k)~$ck^{-\gamma}$ with c=0.4 and γ=1.32 to illustrate the resilience analysis of network systems. The degree distribution of the adopted scale-free network model is depicted in Figure 1 on log-log scales. In this section, the numerical simulation work is initialed by a failure of the node with the maximum degree, and the simulation results are averaged by 10 realizations.

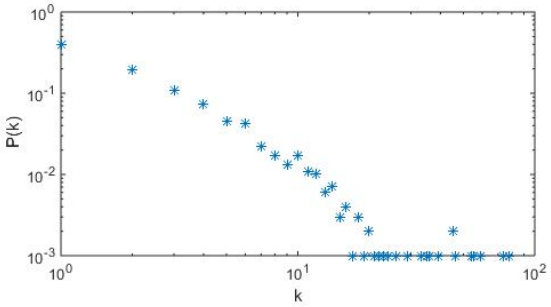


FIGURE I.NODE DEGREE DISTRIBUTION OF THE SCALE-FREE NETWORK MODEL.

### *A. Resilience Affected by Component Reliability*

It is assumed that all components in network systems have a specific failure rate $\rho_i$ which stands for a probability to keep normal at every time step if it was normal at the last time step. In the scale-free network model, to analyze the effect of component reliability for network resilience, we assign the component reliability value to 0.6, 0.7, 0.8, 0.9 and 0.99 (five different levels), and failure propagation probability $\sigma_i$ are all assigned to 0.8, and failure detection probability of $\tau_i$ are all assigned to 0.95, and a recovery strategy $RS_2$ with corresponding 2 recovery time step and 2 resource consumption is adopted.

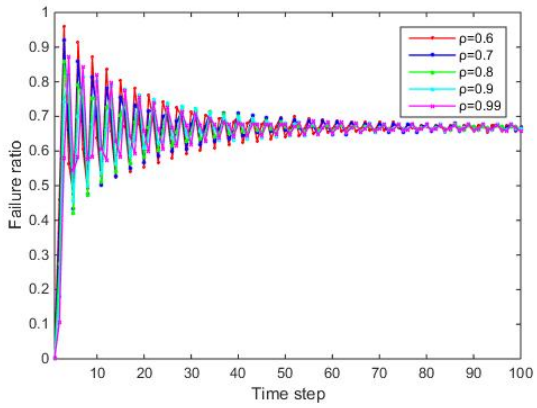


FIGURE II. THE RELATIONSHIP BETWEEN FAILURE RATIO AND TIME STEP WITH DIFFERENT FAILURE RATE $\rho_i$.

As shown in Figure 2, the failure ratios all have a vibration trend while at the first few steps the vibration is more severe, and after about 50 time steps it would become smooth, finally the failure ratios will come to a relative stable value between 0.65 and 0.68 with no difference with the failure rate $\rho_i$. But as shown in Figure 3, the total cost will reduce with failure rate.

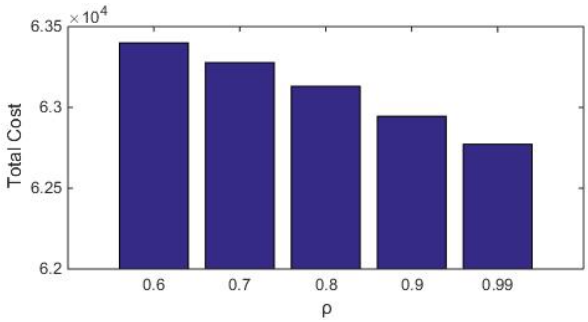


FIGURE III. THE RELATIONSHIP BETWEEN TOTAL COST AND DIFFERENT FAILURE RATE $\rho_i$.

The reason why final failure ratios are almost the same with no difference with the failure rate $\rho_i$ is that the failure propagation probability $\sigma_i$ is extremely high. To illustrate, we change the failure propagation probability $\sigma_i$ from 0.8 to 0.2, a lower level in contrast with the former. From the simulation result shown in Figure 4, we can see the difference of the final failure ratio which will reduce with the failure rate.

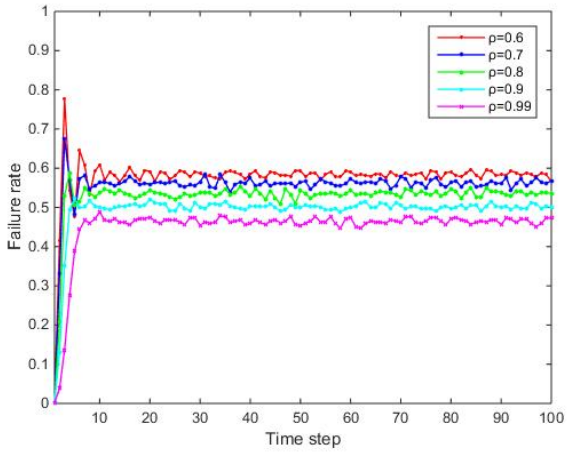


FIGURE IV. THE RELATIONSHIP BETWEEN FAILURE RATIO AND TIME STEP WITH DIFFERENT FAILURE RATE $\rho_i$ AND LOWER FAILURE PROPAGATION PROBABILITY

### *B. Resilience Affected by Failure Propagation*

To analyze the effect of failure propagation for network resilience, we assign the failure propagation probability $\sigma_i$ to 0.2, 0.4, 0.6 and 0.8 (four different levels), and the failure rate $\rho_i$ are all assigned to 0.95, and failure detection probability $\tau_i$ are all assigned to 0.95, and a recovery strategy $RS_2$ with corresponding 2 recovery time step and 2 resource consumption is adopted. As shown in Figure 5, the failure ratios all have a vibration trend which will be more severe with a higher failure propagation probability, after a sharp increasing, the vibration will become smooth rapidly when $\sigma_i$ equals 0.2 and 0.4 while it will consume more time when $\sigma_i$ equals 0.6 and 0.8. Finally the failure ratios will come to a relative stable value and there is a positive proportional relationship between failure ratio and failure propagation probability. On the other hand, the total cost will increase with the failure propagation probability as shown in Figure 6. So it is needed to decrease the failure

propagation probability as much as possible to protect the system.

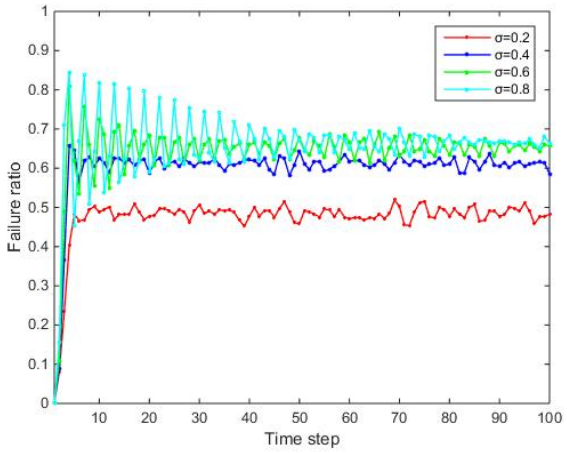


FIGURE V. THE RELATIONSHIP BETWEEN FAILURE RATIO AND TIME STEP WITH DIFFERENT FAILURE PROPAGATION PROBABILITY $\sigma_i$.

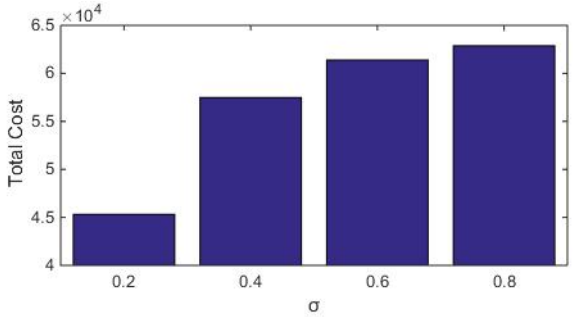


FIGURE VI. THE RELATIONSHIP BETWEEN TOTAL COST AND DIFFERENT FAILURE PROPAGATION PROBABILITY $\sigma_i$.

## C. Resilience Affected by Failure Detection

To analyze the effect of failure detection for network resilience, we assign the failure detection probability $\tau_i$ to 0.6, 0.7, 0.8, 0.9 and 0.99 (five different levels), and failure propagation probability $\sigma_i$ are all assigned to 0.2, and failure rate $\rho_i$ are all assigned to 0.95, and a recovery strategy $RS_2$ with corresponding 2 recovery time step and 2 resource consumption is adopted. As shown in Figure 7, the failure ratios will become very smooth after a sharp increasing, finally the failure ratios will come to a relative stable value about 0.5 which has a negative proportional relationship with the failure detection probability. On the other hand, the total cost will increase with the failure detection probability as shown in Figure 8. So it is helpful to increase the failure detection probability to promote the network system resilience. But as shown in Figure 8, the total cost will increase with failure detection probability, this is because more components would be maintained for a higher system efficiency with a more efficient detection in this simulation situation.

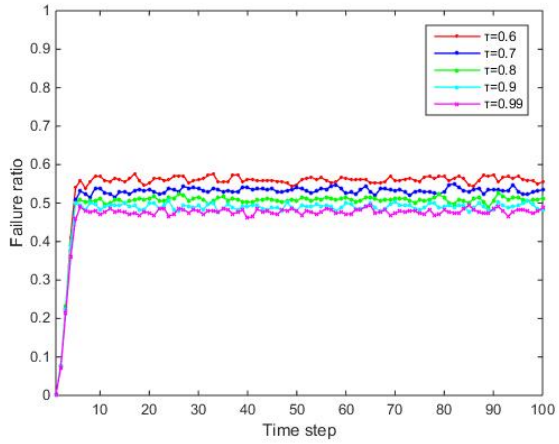


FIGURE VII. THE RELATIONSHIP BETWEEN FAILURE RATIO AND TIME STEP WITH DIFFERENT FAILURE DETECTION PROBABILITY $\tau_i$.

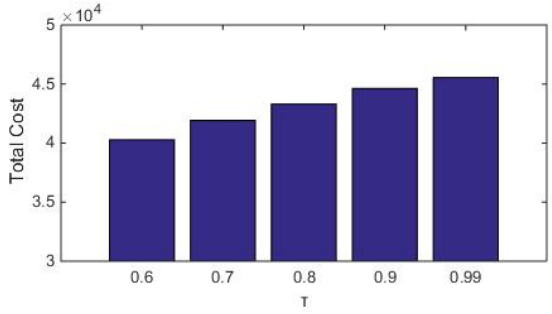


FIGURE VIII. THE RELATIONSHIP BETWEEN TOTAL COST AND DIFFERENT FAILURE DETECTION PROBABILITY $\tau_i$.

## D. Resilience Affected by Recovery Strategy

To analyze the effect of recovery strategy for network resilience, we assign the failure rate $\rho_i$ to 0.95, and failure propagation probability $\sigma_i$ are all assigned to 0.2, and detection probability $\tau_i$ are all assigned to 0.95, and four different recovery strategy are described as follow: (1) $RS_1$: after the detection all the failure components will be recovered with the recovery time $t(RS_1)=1$ and resource consumption $d(RS_1)=3$; (2) $RS_2$: after the detection all the failure components will be recovered with the recovery time $t(RS_2)=2$ and resource consumption $d(RS_2)=2$; (3) $RS_3$: after the detection all the failure components will be recovered with the recovery time $t(RS_3)=3$ and resource consumption $d(RS_3)=1$; (4) $RS_4$: after the detection the failure components will be recovered by $RS_1$, $RS_2$ or $RS_3$ by random. As shown in Figure 9, the failure ratios will become very smooth after a sharp increasing and there is a positive proportional relationship between failure ratio and failure recovery time. On the other hand, the total cost has a negative proportional relationship with the failure recovery time as shown in Figure 10 which interprets that a more efficient recovery strategy deserves a higher cost.

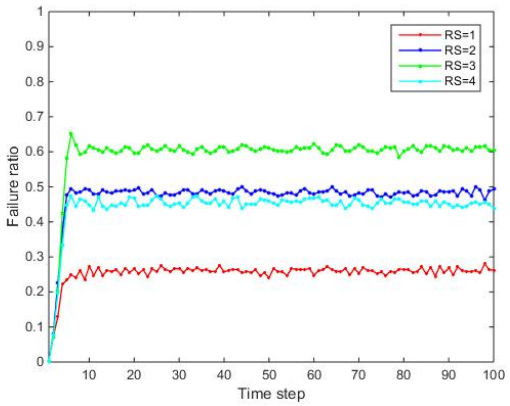


FIGURE IX. THE RELATIONSHIP BETWEEN FAILURE RATIO AND TIME STEP WITH DIFFERENT RECOVERY STRATEGY $RS_i$.

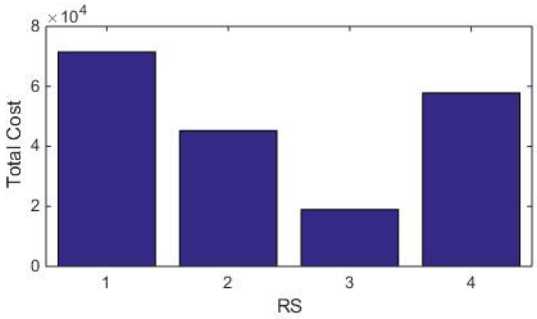


FIGURE X. THE RELATIONSHIP BETWEEN TOTAL COST AND TIME STEP WITH DIFFERENT RECOVERY STRATEGY $RS_i$.

## IV. CONCLUSIONS

This paper mainly proposed a resilience analysis framework based on the resilience engineering concept and numerical simulations are put forward based on a generated scale-free network. The simulation results reveal that factors of component reliability, failure propagation failure detection, and recovery strategy would actually contribute to the resilience of network systems.

Since the scale-free network with degree distribution P(k) gives a power-law behavior which means the degrees of some nodes are much higher than others, and the numerical simulation work is initialed by a failure of the node with the maximum degree, so the network resilience would be affected immediately and seriously due to failure propagation. What is more, the final resilience failure ratios are almost the same with no difference with the failure rate $\rho_i$ and failure detection probability $\tau_i$ if the failure propagation probability $\sigma_i$ level is extremely high, but when the failure propagation probability $\sigma_i$ level is low, high level of failure rate $\rho_i$ and failure detection probability $\tau_i$ would contribute to the resilience of network systems. For different recovery strategy, a more efficient recovery strategy requires a higher cost, i.e. a negative proportional relationship between resilience and failure recovery time. None of the failure ratios came back to zero in the simulation, so the recovery time should be shorter in the situation of high failure propagation probability and low failure rate probability.

## ACKNOWLEDGMENT

This paper was supported by National Basic Research Program of China (973 Program): 2014CB744904.

## REFERENCES

[1] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. U. Hwang, "Complex networks: Structure and dynamics," Physics reports, vol. 424, no. 4, pp. 175-308, 2006.

[2] R. Guimera, S. Mossa, A. Turtschi, and L. N. Amaral, "The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles," Proceedings of the National Academy of Sciences, vol. 102, no. 22, pp. 7794-7799, 2005.

[3] G. Caldarelli, "Scale-free networks: complex webs in nature and technology," OUP Catalogue, 2007.

[4] S. H. Teng and S. Y. Ho, "Failure Mode and Effects Analysis: An Integrated Approach for Product Design and Process Control," International Journal of Quality & Reliability Management, vol. 13, no. 5, pp. 8-26, 1996.

[5] W. E. Vesely, F. F. Goldberg, N. H. Roberts, et al, Fault Tree Handbook, Nuclear Regulatory Commission Washington DC, 1981.

[6] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," Chaos, vol. 17, no. 2, 2007.

[7] J. Lorenz, S. Battiston, and F. Schweitzer, "Systemic risk: in a unifying framework for cascading processes on networks," The European Physical Journal B-Condensed Matter and Complex Systems, vol. 71, no. 4, pp. 441-460, 2009.

[8] United States-Canada power system outage task force, Final report on the August 14th, 2003 blackout in the United States and Canada: causes and recommendations, United States Department of Energy and Canadian Department of Natural Resources, 2004.

[9] Resilience Alliance. Available at http://www.resalliance.org/.

[10] Information Systems for Crisis Response and Management (ISCRAM). Available at http://www.iscram.org/.

[11] E. Hollnagel, D. D. Woods, and N. G. Leveson, Resilience Engineering: Concepts and precepts, Aldershot: Ashgate Publishing, 2006.

[12] M. Keck and P. Sakdapolrak, "What is social resilience? Lessons learned and ways forward," Erdkunde, 2013.

[13] R. Martin, "Regional economic resilience, hysteresis and recessionary shocks," Journal of Economic Geography, 2011.

[14] B. D. Youn, C. Hu, and P. Wang, "Resilience-driven system design of complex engineered systems," Journal of Mechanical Design, vol. 133, no. 10, 2011.

[15] M. Bruneau, S. E. Chang, R. T. Eguchi, et al, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," Earthquake spectra, vol. 19, no. 4, pp. 733-752, 2003.

[16] J. P. G. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbarand, and J. P. Rohrer, "Modeling and analysis of network resilience," In Proceedings of the IEEE COMSNETS, Bangalore, India, 2011.

[17] M. Omer, A. Mostashari, and U. Lindemann, "Resilience analysis of soft infrastructure systems," Procedia Computer Science, vol. 28, pp. 565-574, 2014.

[18] P. Vlacheas, V. Stavroulaki, P. Demestichas, et al, "Towards end-to-end network resilience," International Journal of Critical Infrastructure Protection, vol. 6, no. 3, pp. 159-178,2013.

[19] L. Chen and E. Miller-Hooks, "Resilience: an indicator of recovery capability in intermodal freight transport," Transportation Science, vol. 46, no. 1, pp. 109-123, 2012.

[20] A. Barabási and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, no. 5439, pp. 509-512, 1999.