

International Symposium for Next Generation Infrastructure  
October 1-4, 2013, Wollongong, Australia

# Identifying Extreme Risks in Critical Infrastructure Interdependencies

K. Tai<sup>a\*</sup>  
A. Kizhakkedath<sup>a</sup>  
J. Lin<sup>a</sup>  
R.L.K. Tiong<sup>b</sup>  
M.S. Sim<sup>c</sup>

**Abstract:** Critical infrastructures like our power generation facilities and water supply form highly interconnected networks that are mutually dependent and any failure can cascade through the network, resulting in devastating impact on health, safety and the economy. These catastrophic events/disruptions can be triggered by environmental accidents, geological/weather phenomena, disease pandemics, etc. The disruptions can be caused/exacerbated by their being unexpected, but they may actually be expected if relevant data have been accounted for. To help account for and thereby anticipate such disruptions, one way is to identify potential unforeseen interdependencies among infrastructure components that can lead to extreme disruptions upon some failure in the network. This paper shows how a simulation model for cascading failures and a risk analysis/optimization approach can be applied to search for unforeseen interdependencies and failure points that give rise to the highest risk in a network.

**Key words :** Unforeseen interdependencies; Vulnerabilities; Risk analysis; Network analysis; Multi-objective optimization

## I. Introduction

Critical infrastructure refers to the assets, systems and networks comprising identifiable industries, institutions and distribution capabilities that provide a reliable flow of goods and services essential to the functioning of the economy, the government at various levels, and society as a whole<sup>1</sup>. Examples of critical infrastructure include facilities for energy/power generation, water supply, telecommunications, transportation, banking/financial services, security and health services, etc.<sup>2</sup>. They are highly interconnected and mutually dependent in complex ways, and the sudden unavailability of any of them or part thereof may cause loss of life, severe impact on health, safety or the economy<sup>3,4,5</sup>. The 9/11 terrorist attacks, the Indian Ocean tsunami of December 2004, the Hurricane Katrina devastation of the US Gulf Coast in 2005, the 2008 Global Financial Crisis, the 2011 Tohoku earthquake/tsunami and the severe flooding in Thailand late 2011 can be considered examples of such major disruptions/disasters.

---

<sup>a</sup> School of Mechanical and Aerospace Engineering, Nanyang Technological University, Singapore

<sup>b</sup> School of Civil and Environmental Engineering, Nanyang Technological University, Singapore

<sup>c</sup> Information Division, DSO National Laboratories, Singapore

\*Corresponding author: K. Tai ([mktai@ntu.edu.sg](mailto:mktai@ntu.edu.sg))

<http://dx.doi.org/10.14453/isngi2013.proc.44>

Within a single sector of critical infrastructure (e.g. the electric grid), as well as among various mixed-type or multiple-sector infrastructure (e.g. electric grid and water supply), the interdependencies among their various components can be highly complex and can be quantitative or qualitative in character. Compounding the challenge of analyzing these interrelationships is that access to the required information is difficult because a vast majority of infrastructure assets are owned by the private sector and there are significant barriers to sharing information between the private sector and the government<sup>3</sup>. Furthermore, while experts within a particular infrastructure sector may be able to identify the interdependencies within that sector to build a concise network model for analysis, it is a challenge to identify the interdependencies between different sectors. Interdependencies are most often classified into the following five types<sup>6,7</sup>:

- Physical - A physical or engineering reliance between infrastructures, e.g. material flow from one infrastructure to another.
- Information/Cyber - An informational or control requirement between infrastructures, e.g. a reliance on information transfer between infrastructures.
- Geospatial/Geographical - A relationship that exists entirely because of the proximity of infrastructures, e.g. a local environmental event affects components across multiple infrastructures due to physical proximity.
- Policy/Procedural - An interdependency that exists due to policy or procedure that relates a state or event change in one infrastructure sector to a subsequent effect on another sector, e.g. government's emergency mandatory orders on a particular area due to the influence of an event.
- Societal/Logical - An interdependency that an infrastructure event may have on societal factors, e.g. public opinion, public confidence, fear, and culture issues.

The challenging problem of modelling the relationship/network models of these complex systems have motivated much research<sup>8,9</sup>. However, even if accurate models were built, it is unclear if the far-reaching consequences of the 9/11 terrorist attacks or the 2011 Tohoku earthquake/tsunami could have been anticipated. Very often, some interdependencies are explicitly revealed only after the disasters or disruptions occur. For example, the Tohoku disaster left over twenty thousand confirmed dead, injured or missing, and millions more affected by lack of electricity, water and transportation<sup>10</sup>. Extensive agriculture landscape was flooded, train stations and railway network were damaged, a dam failed in operation, fire occurred at an oil refinery plant, electricity transmission lines, ship and crane, highway bridges were damaged, and a level-7 nuclear accident happened at the Fukushima nuclear power plant<sup>11</sup>. Also affected were the interrelated supply chain business networks between Japan and other countries. To cooperate with electricity conservation efforts, many factories producing high technology components stopped production lines to support blackout measures.

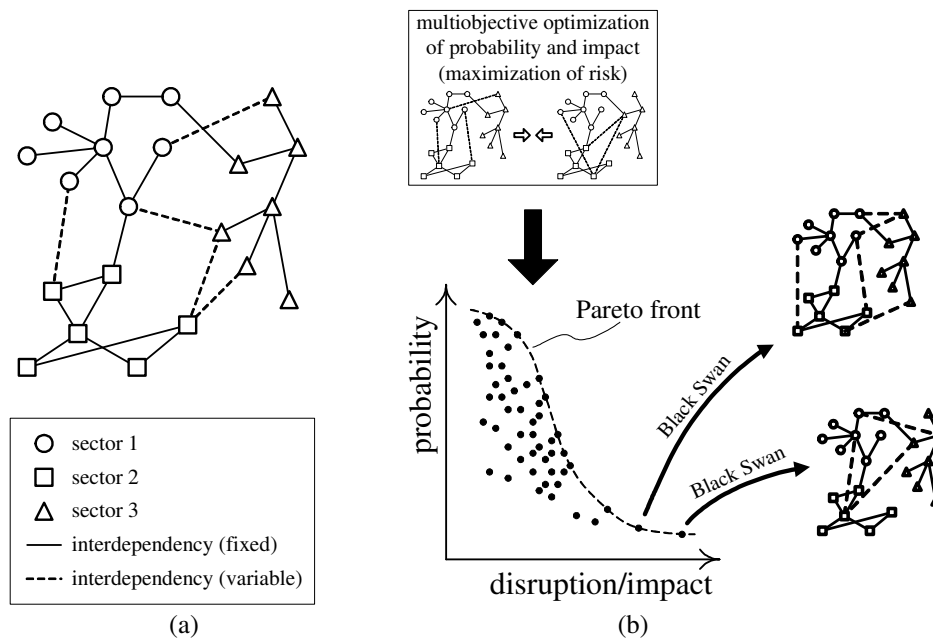
The idea that such high impact but highly unexpected events could actually have been expected if the relevant available data had been accounted for was put forth by Taleb<sup>12</sup> in his book "The Black Swan". Black Swan events are highly improbable events (outliers), and highly impactful, and can be caused and exacerbated by their being unexpected. However, in spite of being highly unexpected, it is natural that experts (and even casual observers) will retrospectively be able to construct explanations for their occurrence after they have

occurred, making them explainable and expected. In the context of critical infrastructure, this is similar to the interdependencies that are explicitly revealed only after major disruptions. As an example used by Taleb, the 9/11 attacks was an event that was a surprise to many observers with major impact/effects felt up to today on the heightened level of security and pre-emptive strikes against various parties. It is doubtful if any amount of modelling and analysis could have predicted how terrorist attacks on some commercial infrastructure could have led to the consequential shutdown of air-space, disruption of air travel around the world and the ensuing conflicts. It seems to imply how little our understanding of the complex systems in our society and physical world can help us guess what is going to happen next, and this Black Swan logic actually makes what we don't know far more relevant than what we do know.

Since it is a challenge to construct an accurate model of the network of critical infrastructure interdependencies/relationships and, anyway, our current limited awareness of the relationships may not be helpful to predict the highly improbable and high impact disruptions, it may be futile to go on to perform the required analyses on such models to predict the effects of those major disruptions. Hence, instead of analyzing a given infrastructure network to determine the effects of any failure, the overall aim should perhaps be to solve the inverse problem, i.e. to synthesize the network that will result in the most extreme disruptions due to some failure. This can be achieved by beginning with the set of infrastructure components, their known interdependencies and prescribed initial/boundary conditions and failure modes, and then apply optimization techniques to iteratively vary/modify the network with additional (unforeseen) interdependencies until the disruption effects are maximized. In this way, what is obtained will be a set of network models (with their associated interdependencies) that can potentially be realized in our real world and that will result in the most severe disruption effects due to various failures with associated probabilities. The resulting networks obtained can then be reviewed by a diverse team of experts to interpret the unforeseen interdependencies and potential scenarios that may lead to the realization of the disruptions computed for the network. As both the severity/impact of the disruptions and the probabilities of occurrence will both be computed as the criteria for the optimization, this represents a risk analysis approach of describing the problem and also a multiobjective optimization problem. Based on these ideas, this paper presents one way to investigate how the highly unexpected major disruptions (the Black Swan events) in our critical infrastructure systems can be anticipated by solving the inverse (optimization) problem of synthesizing infrastructure network interdependency models for extreme failure impact and probabilities. By investigating how the inverse problem can be formulated, the study in turn also explores the bounds (limits) of these extreme (catastrophic) disruptions that can arise from the interdependencies inherent in our critical infrastructures.

## **II. Optimization and Analysis of Infrastructure Network Disruptions**

The network model of critical infrastructures comprises the infrastructure assets/components (nodes) and the links representing their interdependencies, as illustrated in Figure 1(a) (for only three infrastructure sectors).



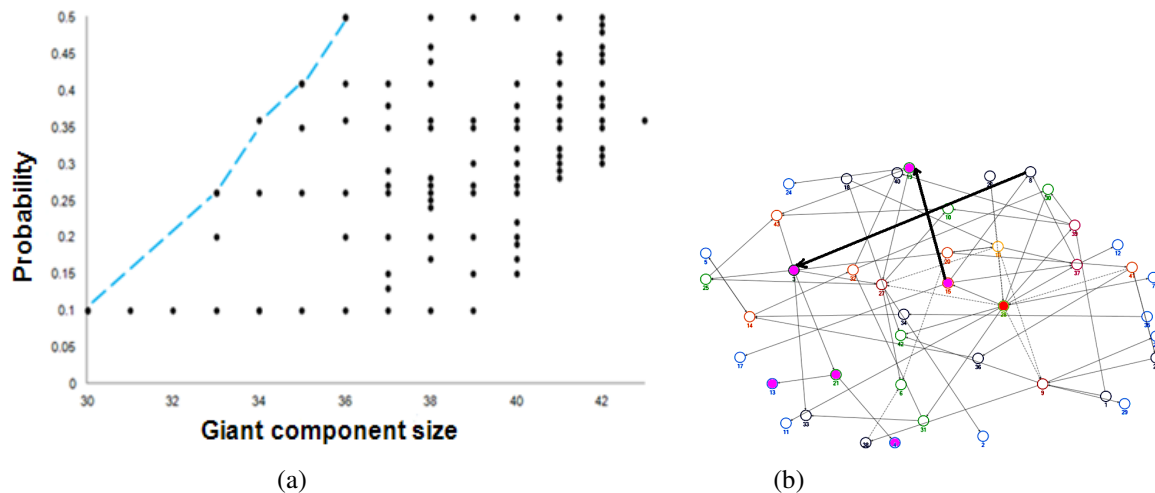
**Figure 1. (a) Critical infrastructure network model (b) Pareto optimal solutions of the multiobjective evolutionary optimization problem, with network solutions of extreme disruption representing Black Swan events.**

The study of the critical infrastructure vulnerabilities is based on a risk analysis framework, where risk can be defined as  $\text{risk} = f(\text{probability}, \text{impact})$ , i.e. as a function of the probability of a failure/hazard/threat resulting in an adverse event and the severity/impact of that event<sup>13,14,15,16</sup>. In the context of our problem, impact refers to the magnitude of the disruption in the network computed according to various metrics used in network theory such as, e.g. the giant component size<sup>17,18</sup>, using agent-based simulation<sup>19,20,21,22</sup>. Probability refers to the probability of the failures propagating/leading to the disruption. The optimization problem is therefore a problem of searching for networks and failures that maximize the two objectives of probability and disruption, with the decision variables being the unforeseen (variable) interdependencies and failure points within the network. With two objectives, an evolutionary algorithm<sup>23,24</sup> is used to iterate a population of solutions (i.e. a set of networks with corresponding failures) converging towards Pareto-optimality. In this way, optimization has been used to synthesize networks with the highest risk, while those with the extreme disruption impact can be considered the Black Swan events, as summarized in Figure 1(b).

### III. Results from Experimental Case Study

The proposed methodology was applied to an experimental case study with a network comprising 43 nodes with two variable (unforeseen) interdependencies added to the fixed (known) interdependencies. The results show that unforeseen interdependencies can indeed exacerbate the disruption consequences/impact, where impact is quantified by the giant component size (the smaller the size, the greater the impact). The plot in Figure 2(a) shows the optimal solution points obtained, with a line drawn through the Pareto-optimal solutions to represent the Pareto-front. The point at the lower extreme left is the Pareto-optimal solution with the greatest disruption (giant component size of 0.1), hence it can be interpreted as a Black Swan event, and it represents the scenario where failure occurs at node 30 and

where there are two unforeseen interdependencies as shown by the thick black lines added to the network in Figure 2(b).



**Figure 2. (a) Pareto-front of the multiobjective optimization of probability and disruption impact (giant component size) (b) Network with two unforeseen interdependencies added.**

#### IV. Concluding Remarks

By assuming that a significant part of the network interdependencies is in fact unknown (unforeseen), the proposed approach applies optimization to search for unknown interdependencies and failure points that will cause extreme events, thus leading analysts on a focused exploration of ‘what-if’ scenarios of high disruptive impact. In addition, it provides policymakers with a way to analyse the ‘trade-off’ between the high-probability/low-impact and the low-probability/high-impact events.

#### References

- <sup>1</sup>Clinton, W.J., “Executive order 13010 - Critical infrastructure protection”, *Federal Register*, Vol. 61, No. 138, 1996, pp.37347-37350.
- <sup>2</sup>Lewis, T.G., *Critical infrastructure Protection Homeland Security*, John Wiley & Sons, New Jersey, 2006. <http://dx.doi.org/10.1002/0471789542>
- <sup>3</sup>Rinaldi, S.M., “Modeling and Simulating Critical Infrastructures and Their Interdependencies”, *International Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS '04 - 2004 Hawaii International Conference on System Sciences* , Hawaii, USA, 5-8 January 2004, Vol. 2, 2004, pp. 20054-20062.
- <sup>4</sup>Dueñas-Osorio, L., Craig, J.I., Goodno, B.J., and Bostrom, A, "Interdependent Response of Networked Systems", *ASCE Journal of Infrastructure Systems*, Vol. 13, No. 3, 2007, pp.185-194. [http://dx.doi.org/10.1061/\(ASCE\)1076-0342\(2007\)13:3\(185\)](http://dx.doi.org/10.1061/(ASCE)1076-0342(2007)13:3(185))
- <sup>5</sup>Kroger, W., “Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools”, *Reliability Engineering and System Safety*, Vol. 93, No. 12, 2008, pp. 1781–1787. <http://dx.doi.org/10.1016/j.ress.2008.03.005>

- <sup>6</sup>Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K., “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies”, *Control Systems*, Vol. 21, No. 6, 2001, pp.11-25. <http://dx.doi.org/10.1109/37.969131>
- <sup>7</sup>Pederson, P., Dudenhoefter, D., Hartley, S., and Permann, M., “Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research”, Idaho National Laboratory, Idaho Falls, Idaho 83415, 2006.
- <sup>8</sup>Bagheri, E., and Ghorbani, A.A., “The State of the Art in Critical Infrastructure Protection: a Framework for Convergence”, *International Journal of Critical Infrastructures*, Vol. 4, No. 3, 2008, pp. 215-244. <http://dx.doi.org/10.1504/IJCIS.2008.017438>
- <sup>9</sup>Yusta, J.M., Correa, G.J., and Lacal-Arantequi, R., “Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art”, *Energy Policy*, Vol. 39, No.10, 2011, pp. 6100-6119. <http://dx.doi.org/10.1016/j.enpol.2011.07.010>
- <sup>10</sup>Japan Meteorological Agency, *Report of the 2011 off the Pacific coast of Tohoku Earthquake*, 2011, URL: [http://www.jma.go.jp/jma/en/2011\\_Earthquake.html](http://www.jma.go.jp/jma/en/2011_Earthquake.html)
- <sup>11</sup>The Gulf Today, *Japan's Afternoon of Horror*, 2011, URL: <http://www.webcitation.org/5xA4lpQXu>
- <sup>12</sup>Taleb, N.N., *The Black Swan: The Impact of the Highly Improbable*, Random House, 2007.
- <sup>13</sup>Open Geospatial Consortium, *Critical Infrastructure Protection Initiative, Phase 2*, 2002, URL: <http://www.opengeospatial.org/projects/initiatives/cipi2>
- <sup>14</sup>Committee of Sponsoring Organizations, *Enterprise Risk Management — Integrated framework*, Committee of Sponsoring Organizations, Chicago, USA, 2004.
- <sup>15</sup>Aven, T., *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities*, John Wiley, 2008.
- <sup>16</sup>Ferigato, C., and Masera, M., “Design of a Platform for Information Exchange on Protection of Critical Infrastructures”, *Lecture Notes in Computer Science, Critical Information Infrastructures Security*, Vol. 5141, 2008, pp. 337-348.
- <sup>17</sup>Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., and Havlin, S., “Catastrophic Cascade of Failures in Interdependent Networks”, *Nature*, Vol. 464, No. 7291, 2010, pp. 1025-1028. <http://dx.doi.org/10.1038/nature08932>
- <sup>18</sup>Lam, C.Y., Lin, J., Sim, M.S., and Tai, K., “Identifying Vulnerabilities in Critical Infrastructures by Network Analysis”, *International Journal of Critical Infrastructures*, Vol. 9, No. 3, 2013, pp. 190-210. <http://dx.doi.org/10.1504/IJCIS.2013.054978>
- <sup>19</sup>Brown, T., Beyeler, W., and Barton, D., “Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems,” *International Journal of Critical Infrastructures*, Vol. 1, No. 1, 2004, pp. 108-117. <http://dx.doi.org/10.1504/IJCIS.2004.003800>
- <sup>20</sup>Dudenhoefter, D., Permann, M., and Manic, M., “CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis”, *International Proceedings of the 38th Conference on Winter Simulation (WSC '06 Winter Simulation Conference, Monterey, CA, 3-6 December 2006)*, 2006, pp. 478-485.
- <sup>21</sup>Bagheri, E., Baghi, H., Ghorbani, A.A., and Yari, A., “An Agent-based Service-Oriented Simulation Suite for Critical Infrastructure Behavior Analysis”, *International Journal of Business Process Integration and Management*, Vol. 2, No. 4, 2007, pp. 315-326. <http://dx.doi.org/10.1504/IJBPM.2007.017756>
- <sup>22</sup>Kremers, E., Viejo, P., Barambones, O., and Gonzalez de Durana, J., “A Complex Systems Modelling Approach for Decentralised Simulation of Electrical Microgrids,” *International Proceedings of the 2010 15th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2010 15th IEEE International*

Conference on Engineering of Complex Computer Systems, Oxford, UK, 22-26 March 2010), 2010, pp.302-311.

<sup>23</sup>Deb, K., *Multi-Objective Optimization Using Evolutionary Algorithms*, Chichester, John Wiley, 2001.

<sup>24</sup>Ray, T., Tai, K., and Seow, K.C., "Multiobjective Design Optimization by an Evolutionary Algorithm", *Engineering Optimization*, Vol. 33, No. 4, 2001, pp. 399-424.  
<http://dx.doi.org/10.1080/03052150108940926>