Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Infastructure Interdependencies Modeling and Analysis - A Review and Synthesis

Nan Xiao
SUNY - Buffalo, nanxiao@buffalo.edu

Raj Sharman
State University of New York at Buffalo, rsharman@buffalo.edu

H. Raghav Rao
mgmtrao@buffalo.edu

Shambhu Upadhyaya
Department of Computer Science and Engineering, State University of New York, Buffalo, New York,
shambhu@cse.Buffalo.EDU

Follow this and additional works at: http://aisel.aisnet.org/amcis2008

Infrastructure Interdependencies Modeling and Analysis - A Review and Synthesis

Nan Xiao

Department of Management Science & systems

SUNY Buffalo

nanxiao@buffalo.edu

H. R. Rao

Department of Management Science & Systems

SUNY Buffalo

mgmtrao@buffalo.edu

Raj Sharman

Department of Management Science & Systems

SUNY Buffalo

rsharman@buffalo.edu

Shambhu J. Upadhyaya

Computer Science and Engineering

SUNY Buffalo

shambhu@cse.buffalo.edu

ABSTRACT

The events of 9/11 and the occurrence of major natural disasters in recent years has resulted in increased awareness and renewed desire to protect critical infrastructure that are the pillars to maintaining what has become normal life in our economy. The problem has been compounded because the increased connectedness between the various sectors of the economy has resulted in interdependencies that allow for problems and issues with one infrastructure to affect other infrastructures. This area is now being investigated extensively after the Department of Homeland Security (DHS) prioritized this issue. There is now a vast extant of literature in the area of infrastructure interdependencies and the modeling of it. This paper presents a synthesis and survey of the literature in the area of infrastructure interdependency modeling methods and proposes a framework for classification of these studies. The framework classifies infrastructure interdependency modeling and analysis methods into four quadrants in terms of system complexities and risks. The directions of future research are also discussed in this paper.

Keywords

Infrastructure interdependency, modeling, literature review

INTRODUCTION

The human habitat is constantly evolving into a more connected society with provisioning of services within the society requiring greater dependence on highly-coupled critical infrastructure systems to deliver key services. For example, after analyzing the media reports of thirteen weeks following 9/11 events, Mendonca and Wallace (2006) found 46 out of 238 service disruptions during that period of time are caused by infrastructure interdependencies. The economy of a region and the well-being of the citizenry are therefore closely linked to the proper functioning of critical infrastructure systems. The final report of the President's Commission on Critical Infrastructure Protection (PCCIP) defines critical infrastructure as "the framework of interdependent networks and systems comprising of identifiable industries, institutions, including people and procedures, and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole." The national infrastructure protection plan (NIPP) defines 17 critical infrastructures as follows: Agriculture and food; water; public health; emergency services; defense industrial base; energy; information technology; banking and finance; telecommunications; dams; transportation systems; chemical; postal and shipping; national monuments and icons; government facilities; commercial facilities; nuclear reactors; materials, and waste. In addition, Barnes and Newbold (2005) view humans as a critical infrastructure due to the core role the humans' intelligence plays in the operations of infrastructure.

Ensuring the resilience and reliability of these infrastructures, which are vulnerable to natural disaster and man-made attacks, has proved challenging. One of the reasons is that the infrastructures are interdependent which leads to the fact that the failure of one infrastructure could cause serious consequences to others. In our research, we adopt the definitions of infrastructure interdependencies from (Rinaldi et al., 2001) as "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other."

The area of infrastructure interdependency has been studied from different perspectives. For example, Chang et al. (2007) develop a conceptual framework for characterizing the nature, extent and severity of the impacts of infrastructure failure interdependencies in disasters from the standpoint of impacts to the communities. (Zimmerman, 2004) identifies and codes news media reports relating to infrastructure interdependencies. A database on infrastructures is created and three measures for infrastructure interdependencies are proposed to facilitate the use of these data. Amin (2002) summarizes

interdependencies of electricity infrastructures, telecommunication infrastructures, and transportation infrastructures with other critical infrastructures. Our study, however, only focuses on *techniques used in modeling infrastructure interdependencies* and not on exploring other areas related to infrastructure interdependencies.

Modeling methods have received increasing attention in infrastructure interdependency research in that it will assists in understanding how a given infrastructure depends on others. This modeling effort requires multiple viewpoints and a broad set of interdisciplinary knowledge from a variety of areas such as computer science, economics, social science and public policy (Peerenboom and Fisher, 2007). In addition, Rinaldi (2004)identifies several factors leading to the complexity of infrastructure interdependencies modeling, such as lack of real-time data and metrics for risk assessment. Although great progresses have been made to analyze individual infrastructure, the science of infrastructure interdependencies is relatively new (Peerenboom and Fisher, 2007). Difficult issues related to system complexity and nonlinear behavior, uncertainty, and human factors, remain largely unanswered. Therefore, previous studies (Rinaldi, 2004; Rinaldi et al., 2001; Peerenboom and Fisher, 2007) have addressed the needs of infrastructure interdependencies modeling methods and called for the papers related to this topic. We respond to these calls by providing taxonomy of infrastructure interdependency modeling and analysis methods.

This paper attempts to provide a review and synthesis of previous study and propose a framework for infrastructure interdependencies modeling. The contributions of this study are twofold: First, this framework is able to guide researchers to select and apply the most appropriate models for their study. Second, this paper identifies some potential research directions which need further studies. As depicted in Figure 1, we classify the infrastructure interdependencies modeling studies into four quadrants in terms of the complexity and risk of the systems they examine. The rest of the paper is organized as follows: First we discuss system complexity and risk and then review typical infrastructure interdependency models. Next we discuss the applications of infrastructure interdependencies modeling in information system security. Finally we conclude with the summary of promising directions for future research.

	Low Risk	High Risk
High Complexity	Min et al. (2007) Gursesli and Desrochers (2003) Daskapan et al. (2004)	Rinaldi et al. (2001) Barton (2000)
Low Complexity	Michaud and Apostolakis (2006) Haimes (2005) Lee et al.(2007) Dudenhoeffer et al. (2006) Nozick et al. (2005) McNally et al. (2007) Brigl et al. (2003)	Lambert and Sarda (2005) Haimes (2002) Longstaff and Haimes, 2002 Staudinger (2006) Simpson et al. (2005) Bagheri and Ghorbani (2007)

Figure 1. The Framework of Infrastructure Interdependencies Modeling and Analysis Methods

COMPLEXITY AND RISK

Complexity and risk are two important characteristics of interdependent infrastructure systems. In this section, we review their applications in infrastructure interdependency and related modeling methods.

System Complexity

System complexities are usually caused by the intricate relationships among different elements of the system. The complexity of interdependent infrastructure systems could be measured by the number of subsystems, the ambiguity of their interdependencies, and the magnitude of cascading effects, etc. Complex systems modeling methods have emerged in infrastructure interdependency study recently. These methods build on the ground that a complex system consists of interacting agents that act on their limited and local information (Amaral and Uzzi, 2007). Complex systems modeling methods are suitable for infrastructure interdependencies study due to the following reasons: first, the overall performance of the whole system is affected and determined by the interconnected infrastructures, which play a similar role to the agents in complex system. Second, complex theory modeling provide effective tools to analyze the physical as well as related organizational and social-economic problem. Third, complex systems modeling utilize simulations tools to validate their model, which reduces the reliance on real data. Complex systems modeling methods differ from other modeling methods in the following ways: (1) Most of other modeling methods focus on the decomposition of a system, whereas complex systems

modeling use "system thinking" to analyze the system. (2) Most of other modeling methods aim to enumerate and quantify all kinds of risks associated with interdependent infrastructures, whereas complex systems modeling employs simulation tools to simulate the system behaviors under various circumstances.

System Risk

Infrastructure interdependencies increase the risk of impacts on services if natural or man-made disasters occur. Risk is defined by (Kaplan, 1997) as the function of scenario, likelihood and consequence. Peerenboom and Fisher (2007) propose a similar definition of risk as a function of threats, vulnerabilities and consequences, i.e., risk=threats*vulnerabilities*consequences. In their definition, threat is a function of intent and effective capability; vulnerability is the characteristics of an asset that render it susceptible to destruction, and consequence refers to both direct and indirect effects. Consistent with previous studies (Haimes, 2002; Longstaff and Haimes, 2002), we divide the risk-based modeling process into two phases: risk assessment and risk management. The modeling methods used in these two phases are detailed in the following sections.

Risk Assessment

In risk assessment phase, the researchers often attempt to answer the following three questions: what can go wrong? What is the likelihood that it would go wrong? What are the consequences(Kaplan, 1997)? In order to identify the risks exhaustively and assess them accurately, some frameworks for risk assessment have been proposed as follows.

Panzieri (2004) proposes a framework to analyze and prioritize resources to protect U.S critical infrastructure from terrorist attacks. This framework which provides procedures for risk assessment includes the following steps: characterize assets, determine consequence, define threats, assess vulnerabilities, and analyze system risk. Interdependencies analysis, as important part of this framework, is incorporated in each of these steps.

Moselhi et al. (2005) suggest a reliability-based approach to assess the risk of critical infrastructure systems. Their approach consists of interdependency identification, interdependent CIS reliability modeling, socioeconomic cost assessment, multi-objective optimization and sensitivity analysis, and a simulation and data collection prototype system. Based on this approach, a prototype simulation tools is developed and applied to transportation and telecommunication networks modeling.

Peerenboom et al. (2001) propose a framework for assessing the risks associated with infrastructure interdependencies. The framework includes five steps: characterize assets, determine consequences, define threats, assess vulnerabilities, and analyze system risk.

Lambert and Sarda (2005) propose a nine-stage framework to identify the risk of interdependent infrastructures. The first six stages address the iterative process of risk identification and the other three steps focus on risk management. Their framework includes a scenario identification algorithm for detecting and responding to knowledge about infrastructure risk.

Ezell et al. (2000) propose an infrastructure risk analysis model which includes four phases: identifying risks to the infrastructures, modeling the risks to the infrastructures, assessing the infrastructures, and managing the risk to the infrastructures. In the first phase, the system is decomposed along the dimensions of function, component, structure, state, and vulnerability, and then a ranking of vulnerabilities and threats is established. In the second phase, the probability of the consequence under each scenario is evaluated. In the third phase, the conditional expected values for damages, consequences, or losses are calculated to quantify the risk associated with the extreme events. In the fourth stages, alternative approaches of improving system performance are generated for decision making.

Based on the frameworks above, we find infrastructure interdependencies risk assessment usually includes three steps: scenario selection, infrastructure interdependencies identification, and vulnerability assessment. In the following section, we will review the modeling and analysis methods used in these three steps.

Step 1: Scenario Selection

 A scenario is a precise narrative or other description of a potential avenue of risk to the infrastructures (Lambert and Sarda, 2005).

Wei (1991) proposes failure mode, effects, and criticality analysis for scenario identification. The procedures of their approach are as follows: (1) documenting all probable failures, (2) determining the effect of each failure, (3) identifying single failure points, and (4) ranking each failure in accordance to a severity classification.

Based on multi-attribute utility theory and graph theory, Michaud and Apostolakis (2006) present a methodology to rank the elements of a water-supply network. Accident scenarios are generated and their corresponding consequences are evaluated and ranked using value tree. A value tree, also called the "objective hierarchy", captures the objectives of decision makers

that could be affected by a scenario. A value tree has two tiers. The fist tier represents the impacts and the second tier represents the performance measures of each impact.

Lambert and Sarda (2005) report an approach to identify dependency scenarios in hurricane recovery. In their approach, data are collected by interview and document analysis and then are classified according to the functional units. The dependency scenarios are measured and compared to determine their priorities of being fixed.

Step 2: Infrastructure Interdependency Identification

Rinaldi et al. (2001) define three types of infrastructure interdependency failures: cascading failures, escalating failures, and common cause failures. Each failure is caused by different types of relationships between infrastructures. Identifying infrastructure interdependencies will enhance our understanding of the impacts of one infrastructure's disruption on other infrastructures and facilities the predictions of the systems' behaviors as a whole.

Mendonca and Wallace (2006) illustrate how to use public reports to identify and assess the infrastructure interdependencies through content analysis. In their study, they utilize the New York Times as the data source to study the impacts of the 9/11 terrorist attack on critical infrastructures in New York City. Their approach includes the following steps: identifying and classifying the articles reporting the incidents and associated disruptions by coding and entering them into a database. Then the disruptions to services provided by critical infrastructure were assessed and compared. A matrix, whose entry represents the number of impacts involving any two infrastructures, was create and the correlations between the infrastructures are calculated to evaluate the interdependencies. At last, the number of disruptions resulting from interdependencies is counted.

Step 3: Vulnerability Assessment

Ashparie et al. (2005) develop a value hierarchy to evaluate trade-offs between the different objectives of system. The values in the hierarchy are obtained through interviews with stakeholders and the internal documentation. The author further divided the objectives of the system into three components: operation cost, operational performance objectives and security. A utility function is developed based on this value hierarchy and decomposition.

Risk Management

In risk management phase, the following three questions need to be answered: what can be done and what options are available? What are the associated tradeoffs in terms of all cost, benefits, and risks? What are the impacts of current management decisions on future options (Haimes, 1998)? Altay and Green (2006) identify four typical activities of disaster operations management: mitigation, preparedness, response, and recovery. Infrastructure interdependencies research, as a sub-stream of disaster management research, also focuses on the decision making in these activities.

INFRASTRUCTURE INTERDEPENDENCY MODELING

There is a huge body of literature focuses on infrastructure interdependency modeling. Those studies draw on theories and methodologies from various research fields such as computer science and engineering, and they usually combine the complex system modeling and risk modeling. This section reviews several typical modeling methods which have been heavily used in infrastructure interdependency studies.

Agent-based Model

Rinaldi et al. (2001) propose that critical infrastructures, which are collections of interacting components, could be treated as complex adaptive systems (CASs)- a special case of complex systems. A CAS is a collection of intelligent agents which adapt to events and surrounding, interacting both competitively and cooperatively for the goods of system. From this perspective, infrastructures are composed of the components which are able to learn from past experiences and adapt their future behavior.

Agent-based model is an effective approach to explore CASs. Agent-based model is a computational model which simulates the interactions of multiple agents. Physical components of infrastructures can be modeled as agents to allow analysis of their states. The agents could also simulate the decision and policy makers involved in infrastructure operations. Using these models, we could examine the consequence of the infrastructure disruptions and the resilience of the industries and firms.

Barton (2000) introduces a model of infrastructure interdependencies employing agent-based approach. This model is developed by Sandia National Laboratory. The original model is called Aspen model in which each agent represents real-life decision-makers such as banks, households, manufacturing firms, and government agents. Each agent behaves like its real world counterpart to simulate their actions and sends message to each other to stimulate the complex interactions between their counterparts. Aspen-EE (Aspen Electricity Enhancement) model extends Aspen model by including the rules and agents

of electric power and gas infrastructure. The operation of each agent in Aspen-EE depends on the electricity agents and gas agents.

Systems Dynamic Model

Another promising modeling approach is systems dynamic. System dynamic, developed by Jay Forrester in early 1960s, is an approach to understand the complex systems. System dynamic is grounded in the theory of nonlinear dynamic and feedback control and has been widely used in the areas like ecology, economics, and engineering. A system dynamic model includes three components: causal loop diagrams, stock and flow diagrams, and equations. Causal loop diagrams visually capture the causal process between the variables at high level. Stock and flow diagrams consists of four elements: stock, flow, converter, and connector. Based on the stock and flow diagrams, equations are derived to further identify the quantitative relations between the variables. The simulation models then are built to enable users to see how system responds when the conditions changed.

Min et al. (2007) propose a model which employs system dynamics and nonlinear programming to determine how to allocate limited resource to physical infrastructures and to economic sectors under disruption. Electric power, natural gas, and petroleum model are built to capture the critical processes required to deliver products and services. The aggregate inventories and flows of materials/services are modeled as stocks and flows in SD model, respectively. These SD models enable analysts to examine how the economic impacts propagate through infrastructure network. Based on these models, experiments are conducted to compare the performance of three resource allocation algorithm in disaster scenarios.

HHM Model

Haimes (2002) provides a holistic risk assessment and management framework to model the risks of terrorism. He utilizes hierarchical holographic modeling (HHM) to identify the infrastructure interdependencies and the multidimensional risks associated with them. HHM provides a tool to collect and synthesize the information related to risks. The philosophy of HHM is that multiple decompositions could help us to understand the interconnectedness and interdependencies of large-scale and complex systems. A typical hierarchy of HHM consists of head-topic, subtopic and sub-subtopics, etc(Longstaff and Haimes, 2002). The exhaustive topic identification needs the involvement of stakeholders, decision-makers, and domain experts, along with careful search of journal, reports, and internet. Staudinger (2006) further extends the HHM framework and compared its performance with other methods.

IIM Model

Based on Leontief's input-output model, which describes the equilibrium behavior of both national and regional economies and the degree of interconnectedness among various economic sectors, Haimes (2005) propose an inoperability input-output model (IIM) to characterize interdependencies among sectors. The principle assumption of IIM is that the level of economic dependency is the same as the level of physical dependency. One of the most important advantages of this model is that it is able to utilize the Bureau of Economic Analysis (BEA) database, which includes the production and consumption of commodities of about 500 sectors, as well as regional input-output Multiplier systems, which is a set of regional data. There are two kinds of IIM—static IIM and dynamic IIM. Static IIM defines the equilibrium state of the sectors, while dynamic IIM describes the process of the economy system state reaching the equilibrium and can be transformed into a static model through equivalent static inoperability. IIM provides a tool for accessing (1) direct economic impacts of certain infrastructure disruption, (2) trade-offs between reduction in economic losses and associated cost to carry out various recovery options.

Linear Programming

Linear programming has been used in infrastructure interdependency to explore those questions like how to allocate limited resources to mitigate the impacts of disaster and how to invest to optimize the operations of infrastructures. For example, the aim of the study conducted by(Lee et al., 2007) is to support emergency response organizations(EROs) at various levels to set priorities of restoration activities when an extreme event affect more than one infrastructures. This paper identifies five types of interdependencies: input, mutually dependent, co-located, shared, and exclusive-or. They use three mathematical programming models to examine the input interdependent system in normal state, disruption state and recovery state. To illustrate these models, cases of infrastructure interdependencies arising following the events of 9/11 are analyzed.

Network Flow

Network flow has been employed by previous studies to visualize and capture the infrastructure interdependencies. Dudenhoeffer et al. (2006) describe infrastructures as a network composed of nodes and edges. Nodes denote source, produces and consumes; Edges between two nodes denote a direct level of dependence between them. A set of mathematical formalisms are developed to define different types of interdependencies. They also introduced a software framework named

the Critical Infrastructure Modeling System (CIMS), which uses an agent-based approach to model infrastructure elements and support the interdependency evaluation and analysis.

Nozick et al. (2005) also represent interdependent infrastructures through networks. They develop a mathematical framework to represent interconnected infrastructure networks. Their work also includes algorithms to estimate performance and optimize investment. This framework treats uncertainty in the capacity of links in the networks as a key characteristic and uses measures to reflect network performance. In their model, the arcs represent the connections between infrastructures and their capacities capture the relationships between the infrastructures. Markov and semi-Markov processes are employed to model the evolution of capacities on network links.

Other Models

Gursesli and Desrochers (2003) use Petri nets to capture the relationships between independent infrastructures. Their study illustrates how to model the interdependencies and the vulnerabilities using place invariants (P-invariants), and how to select recovery strategies using transition invariants (T-invariants)

Simpson et al. (2005) develop a framework to evaluate the social and economic impact on a community in response to an extreme event. This framework employs fragility curves to measure the conditional probability of various infrastructures reaching or exceeding a particular damage state. Although the framework provides valuable information to support resource allocation and disaster preparedness, lacking of historical data makes fragility curves developing difficult for some infrastructures and constrains its applications.

INFRASTRUCTURE INTERDEPENDENCIES AND INFORMATION SYSTEM SECURITY

Infrastructure interdependencies have great impacts on information system security. On one hand, widely-used information systems have increased interdependencies between infrastructures. On the other hand, decision makers rely on a variety of information systems to support the analysis of interdependencies and mitigation of their consequences. In addition, some infrastructure interdependency modeling methods have been applied in information systems studies to investigate interdependencies between software, hardware and business processes. In this section, we will review some examples of such studies.

McNally et al. (2007) introduce an ontology-based information system which could represent and visualize critical infrastructure interdependencies. This system consists of five subsystems: users, a user interface, a database management systems, a model based management systems, and a knowledge base management system. By using object-oriented technologies, the knowledge base management system provides the capacities of knowledge representation and knowledge visualization. This information system could be used to define the hierarchical structure of system, specify the properties and functions of the system and understand the interdependencies of the systems.

Brigl et al. (2003) present a three-layer graph-based model for modeling hospital information system. The three layers include: the domain layer, which describes the enterprise functions of a hospital, the logical tool layer, which describes the software application functions, and the physical tool layer, which describes the hardware components. These three layers together are able to describe the interdependencies between the elements in different layers, especially interdependencies between business processes and communication processes.

Inspired by complex systems modeling introduced in section 2.2, Daskapan et al. (2004) propose a distributed defense system. In their systems, each computing entity (CE) is treated as an self-organized 'cell' which is responsible of regularly cloning and dispatching the process to its neighboring CEs. This system improves the ability of resource sharing and the level of security.

Bagheri and Ghorbani (2007) propose a UML-based model to profile the different aspects of the critical infrastructure systems. This model consists of five high-level sub-models: ownership and management model, structure and organization model, resource model, risk model, and relationship model. This model is evaluated in terms of characteristics of critical infrastructure systems and the results show it can cover required dimensions and provide efficient means and tools for analysis. Min et al. (2007) use IDEF0 to describe the exchange of information between the individual infrastructures. More than 5000 variables and parameters are included in their model.

CONCLUSIONS AND FUTURE RESEARCH

References	Level of Analysis	Infrastructure Studied	Modeling Method	Scenario
(Ashparie et al., 2005)	National level	Electric power, water, healthcare network	Simulation	N/A
(Simpson et al., 2005)	Local(Community) level	Communities' social/economic system	Fragiligy curve	N/A
(Lee et al., 2007)	Local level	Telecommunications, power	Mathematical Programming, Network flow	9/11 events
(Moselhi et al., 2005)	Local level	Not specified	Reliability-based approach	N/A
(Haimes, 2002)	Multiple levels	Homeland system	HHM	Terrorist attacks
(Haimes, 2005)	National level and regional level	Not specified	Inoperability input-output model	Terrorist attack
(Mili et al., 2004)	Local level	Electronic power	Game theory	nature-generated hazard and man-made hazard
(Nozick et al., 2005)	National level	Natural gas distribution network and electricity distribution network	Network flow	N/A
(Newman et al., 2005)	Local level	Power transmission system	Coupled CASCADE model and complex system model	N/A
(Ehlen and Scholand, 2005)	National level	Electronic power and other infrastructures	Agent-based	N/A
(Dudenhoeffer et al., 2006)	N/A	Not specified	Agent-based	Scenarios are generated by (1)manipulating individual nodes or edges and (2) developing baseline scripts
(Min et al., 2007)	National level	Electric power Natural gas petroleum	System dynamic IDEF0Nonlinear optimization	Power disruption
(Zimmerman, 2004)	Local level	Various infrastructure	Event database	N/A
(Gursesli and Desrochers, 2003)	Local level	Electric power and other infrastructure	Petri net	Power disruption

Table 1. The summary of Literature on Infrastructure Interdependencies Modeling Methods

We summarize the references related to infrastructure interdependency modeling and analysis in table 1. From the table we can see that most of the current research mainly focuses on lifeline infrastructures like electricity power infrastructure, water infrastructure, gas infrastructure. The reason could be that those infrastructures have more direct impacts on our daily lives and the data from these sectors are more easily to obtain. In contrast, other infrastructures like banking and finance, commercial facilities, and government facilities, receive relatively less attentions. However, these infrastructures are of critical importance to disaster mitigation and recovery as well. Thus, research on interdependencies of these infrastructures could be a potential direction.

Another finding from the table is that most of exiting research use one or two methods, few of them use three or more than three methods. However, as pointed out by Baker et al.(2002), a single method or perspective could not adequate enough to capture the behaviors of complex systems; therefore, further study may explore how to integrate these models to improve the models' accuracy.

Rinaldi et al. (2001) classify interdependency into four types: physical interdependency, cyber interdependency, and geographic interdependency. From our literature survey, we found that the research on cyber interdependency is scarce. The reason is that cyber interdependencies are relatively new and are difficult to identify and measure. Therefore, further study may focus on cyber interdependency and related issues. Kim et al. (2005) outline the objects of research in this direction. The short term objective is to model and simulate the cyber interdependency between critical infrastructures. The long term objective is to design information sharing mechanisms for protection of cyber interdependencies within critical infrastructures. Such mechanisms include network protocols and communication models.

REFERENCES

1. Altay, N., & Green, W. G. (2006). OR/MS research in disaster operations management. *European journal of operational research*, 175(1), 475-493.

2. Amaral, L. A. N., & Uzzi, B. (2007). Complex systems—A new paradigm for the Integrative study of management, physical, and technological systems. *Management science*, 53(7), 1033-1035.

3. Amin, M. (2002). Toward secure and resilient interdependent infrastructures. *Journal of Infrastructure Systems*, 8(3), 67-75.

4. Ashparie, Y. M., Bashorun, O. P., Kouch, G. J., Siegel, G. R., & Stoyanov, P. T. (2005). Infrastructure Analysis System (IAS). *Proceeding of the 2005 Systems and Information Engineering Design Symposium*, Charlottesville, VA, USA, University of Virginia.

5. Bagheri, E., & Ghorbani, A. A. (2007). UML-CI: a reference model for profiling critical infrastructure systems. Working paper.

6. Baker, A. B., Eagan, R. J., Falcone, P. K., Harris, J. M., Herrera, G. V., Hines, W. C., et al. (2002). A Scalable Systems Approach for Critical Infrastructure Security. Sandia National Laboratories. Retrieved October 25, 2007, from http://www.prod.sandia.gov/cgi-bin/techlib/access-control.pl/2002/020877.pdf

7. Barnes, J., & Newbold, K. (2005). Humans as a Critical Infrastructure: Public-Private Partnerships Essential to Resiliency and Response. *Proceeding of the first IEEE International Workshop on Critical Infrastructure Protection*, November 3-4, Darmstadt, Germany.

8. Barton, D.C., and Stamber, K.L. (2000). An Agent-Based Microsimulation of Critical Infrastructure Systems. *Proceeding of the 8th International Energy Forum*, Las Vegas, NV, USA.

9. Brigl, B., Wendt, T., & Winter, A. (2003). Modeling interdependencies between business and communication processes in hospitals. *Studies in health technology and informatics*, 95, 863-868.

10. Chang, S. E., McDaniels, T. L., Mikawoz, J., & Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. *Nat Hazards*, 41, 337-358.

11. Dudenhoeffer, D. D., Permann, M. R., & Manic, M. (2006). CIMS: a framework for infrastructure interdependency modeling and analysis. *Proceedings of the 2006 Winter Simulation Conference*, Monterey, California, USA, 478-485.

12. Ehlen, M. A., & Scholand, A. J. (2005). Modeling Interdependencies between Power and Economic Sectors using the N-ABLE™ Agent-Based Model. *Proceeding of Power Engineering Society General Meeting*, June 12-16, San Francisco, California, USA.

13. Ezell, B. C., Farr, J. V., & Wiese, I. (2000). Infrastructure risk analysis model. *Journal of infrastructure systems*, 6(3), 114-117.

14. Gursesli, O., & Desrochers, A. A. (2003). Modeling Infrastructure Interdependencies Using Petri Nets. *Proceeding of IEEE International Conference on Systems, Man and Cybernetics*, Hague, Netherlands, 1506-1512.

15. Haimes, Y. Y. (1998). Risk modeling, assessment, and management. New York: Wiley.

16. Haimes, Y. Y. (2002). Roadmap for modeling risks of terrorism to homeland. *Journal of infrastructure systems*, 8(2), 35-41.

17. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Lian, C., & Crowther, K. G. (2005). Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. *Journal of infrastructure systems*, 11(2),67-79.

18. Kaplan, S. (1997). The words of risk analysis. Risk analysis, 17(4), 407-417.

19. Lambert, J. H., & Sarda, P. (2005). Terrorism scenario identification by superposition of infrastructure networks. *Journal of infrastructure systems*, 11(4), 211-220.

20. Lee, E. E., Mendonça, D. J., Mitchell, J. E., & Wallace, W. A. (2007). Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach. *IEEE transactions on system, man, and cybernetics-part c: applications and reviews*, 37(6), 1303-1317.

21. Longstaff, T. A., & Haimes, Y. Y. (2002). A Holistic Roadmap for Survivable Infrastructure Systems. *IEEE Transactions on system, man,and cybernetics-part A: systems and Humans,* 32(1), 260-268.

22. McNally, R. K., Lee, S.-W., Yavagal, D., & Xiang, W.-N. (2007). Learning the critical infrastructure interdependencies through an ontology-based information system. *Environment and Planning B: Planning and Design*, 34, 1103 -1124.

23. Mendonca, D., & Wallace, W. A. (2006). Impacts of the 2001 world trade center attack on New York city critical infrastructure. *Journal of infrastructure systems*, 12(4), 260-270.

24. Michaud, D., & Apostolakis, G. E. (2006). Methodology for ranking the elements of water-supply networks. *Journal of infrastructure systems*, 12(4), 230-242.

25. Mili, L., Krimgold, F., Alwang, J., & Bigger, J. E. (2004). Integrating Engineering, Economic, and Social Modeling in Risks of Cascading Failures Across Interdependent Complex Networks. *Proceeding of the 8'th International Conference on Probabilistic Methods Applied to Power System*, Ames, Iowa, USA, Iowa State University.

26. Min, H.-S. J., Beyeler, W., Brown, T., Son, Y. J., & Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions*, 39, 57-71.

27. Moselhi, O., Hammad, A., Alkass, S., Assi, C., Debbabi, M., & Haider, M. (2005). Vulnerability assessment of civil infrastructure systems: a network approach. *Proceeding of the 1st CSCE Specialty Conference on Infrastructure Technologies, Management and Policy*, June 2-4, Toronto, Ontario, CA.

28. Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E., & Gradney, P. (2005). Risk Assessment in Complex Interacting Infrastructure Systems. Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii, USA.

29. Nozick, L. K., Turnquist, M. A., Jones, D. A., Davis, J. R., & Lawton, C. R. (2005). Assessing the performance of interdependent infrastructures and optimising investments. *International journal of critical infrastructure*, 1(2), 144-154.

30. Panzieri, S., Setola,R. ,and Ulivi,G. (2004). An agented based simulator for critical interdependent infrastructures. *Securing Critical Infrastructures*, October.

31. Peerenboom, J., Fisher, R., & Whitfield, R. (2001). Recovering from disruptions of interdependent critical infrastructures. *Paper presented at the CRIS/DRM/IIIT/NSF Workshop on "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures"*, September 10-11, Alexandria, Virginia, USA

32. Peerenboom, J. P., & Fisher, R. E. (2007). Analyzing cross-sector interdependencies. *Proceeding of 40th Hawaii international conference on system sciences*, Hawaii, USA.

33. Rinaldi, S. M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies. *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, US.

34. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11-25.

35. Simpson, D. M., Rockaway, T. D., Weigel, T. A., Coomes, P. A., & Holloman, C. O. (2005). Framing a new approach to critical infrastructure modeling and extreme events. *International journal of critical infrastructure*, 1(2), 125-143.

36. Staudinger, T. J., England, E. C., & Bleckmann, C. (2006). Comparative analysis of water vulnerability assessment methodologies. *Journal of infrastructure systems*, 12(2), 96-106.

37. Zimmerman, R. (2004). Decision-making and the Vulnerability of Interdependent Critical infrastructure. *Proceeding of 2004 IEEE International Conference on Systems, Man and Cybernetic*, Hague, Netherlands.