Physica A 391 (2012) 3323–3335

Contents lists available at SciVerse ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Vulnerability analysis of interdependent infrastructure systems: A methodological framework

Shuliang Wang [a,b,1], Liu Hong [a,*], Xueguang Chen [a]

[a] Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, PR China

[b] Department of Computer Science, Panzhihua University, Panzhihua, 617000, PR China

ARTICLE INFO

Article history:
Received 16 October 2011
Received in revised form 12 December 2011
Available online 31 December 2011

Keywords:
Interdependent infrastructure systems
Network model
Vulnerability analysis

ABSTRACT

Infrastructure systems such as power and water supplies make up the cornerstone of modern society which is essential for the functioning of a society and its economy. They become more and more interconnected and interdependent with the development of scientific technology and social economy. Risk and vulnerability analysis of interdependent infrastructures for security considerations has become an important subject, and some achievements have been made in this area. Since different infrastructure systems have different structural and functional properties, there is no universal all-encompassing 'silver bullet solution' to the problem of analyzing the vulnerability associated with interdependent infrastructure systems. So a framework of analysis is required. This paper takes the power and water systems of a major city in China as an example and develops a framework for the analysis of the vulnerability of interdependent infrastructure systems. Four interface design strategies based on distance, betweenness, degree, and clustering coefficient are constructed. Then two types of vulnerability (long-term vulnerability and focused vulnerability) are illustrated and analyzed. Finally, a method for ranking critical components in interdependent infrastructures is given for protection purposes. It is concluded that the framework proposed here is useful for vulnerability analysis of interdependent systems and it will be helpful for the system owners to make better decisions on infrastructure design and protection.

1. Introduction

Critical infrastructure systems, which are often called lifeline systems, refer to the framework of systems comprising identifiable industries, institutions, and distribution capabilities [1]. They provide a reliable flow of products and services essential to the defense and economic security of society. They include but are not limited to electric power systems, telecommunications, water supply systems, natural gas supply systems, and transportation systems, and they make up the cornerstone of modern society. Infrastructures do not exist in isolation, but are interconnected with other infrastructures. With the development of scientific technology and social economy, these infrastructure systems become increasingly complicated and mutually dependent. Also more and more resources and information are needed to maintain their day-to-day normal operation. Therefore the functions of one infrastructure and other infrastructures are mutually related. Once the systems are disturbed by external or internal perturbations, disruptions of components from one system may cause components in the other systems to fail, too. When some initial failures of components arise, they may trigger a

* Corresponding author. Tel.: +86 027-87540084; fax: +86 027-87540084.
E-mail addresses: shuliang0820@sina.com (S. Wang), hongliu1978@mail.hust.edu.cn (L. Hong).
1 Tel.: +86 13971494183.

0378-4371/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2011.12.043

recursive process of cascading failures that can damage the systems seriously [2]. Increasing interconnectivities among critical infrastructure systems have made them more vulnerable than before [3–6].

Widespread loss of these systems can be very disruptive. They can cause great economic, social, and physical disruption, amplifying negative consequences and affecting unforeseeable and haphazard sets of users. An example of infrastructure disruption is the 2003 North America power grid blackouts. The event led to 50 million people being affected in at least ten northeastern states and one Canadian province and caused about US$10 billion losses. Because of interdependences, most of the physical and organizational infrastructures were affected such as national security, health and welfare, communications, finance, transportation, food and water supplies, heating and cooling, computers and electronics, commercial enterprises, and even entertainment and leisure. Another example is the 2008 South China snowstorms. The snowstorm disaster in South China caused many infrastructure disruptions. Road, rail, aviation, electricity, water, transport, and other infrastructure systems in this area lost most of their functions and some even collapsed. More seriously, due to the interdependence between different infrastructures, what happened in one infrastructure affected the other systems directly and indirectly. For example, the traffic which was influenced by the snowstorm further threatened the electric power infrastructure which required coal fuel for its generators. Subsequently, rescue was delayed due to lack of adequate power resources and bad traffic conditions. This then worsened key segments of the vital human services. The disaster led to billions of dollars of losses, causing far-reaching security and reliability concerns. These examples illustrate that disruptions may exceed the boundaries of a single infrastructure due to coupling, and may cause significant damage. So these lifeline systems must be sufficiently reliable and governable to ensure that people living and working in these areas have access to most utility services, further, to "protect the well-being of the population, functioning of government, and economic capabilities". However, because of different coupling modes and unique failure propagation patterns, they respond differently to disruptions. In view of the importance of infrastructure systems on social development, the influence of infrastructure disruptions on social production, and economics, risk and vulnerability analyses of interdependent infrastructure systems have become increasingly important.

2. Related studies

Research in this area has attracted much attention, and some achievements have been made. For a single infrastructure, many researchers studied the reliability and vulnerability of such an infrastructure and the impact of random disturbance, deliberate attack, and natural disasters on it. When there is little information about the operation of the infrastructure, probabilistic risk analysis (PRA) methods have been developed for estimating and managing the infrastructure risk [7–9]. Then historical data combined with statistical learning theory has been developed by scholars to analyze and predict the impact of natural disasters on infrastructure performance [10–12]. However, neither PRA nor statistical learning theory has taken into account the infrastructure topology. Meanwhile, the impact of infrastructure layout on network performance is not considered. When the system topology is available, network-based approaches can readily contain various scenario disruptions, multiple hazards, component-level interventions, and reconfiguration.

Complex network approaches based on graph and network theory have subsequently been developed for modeling infrastructures. Complex network theory has been developed in the last two decades and, given in-depth research, a lot of valuable conclusions have been made. The theory has been applied to many research areas such as equipment systems, environmental protection, industrial production, communications, control science systems, computer engineering, artificial intelligence and infrastructure systems, amongst others. For infrastructure systems, graph and network theory has been widely used to characterize their topology and layout features by taking advantage of closed-form expressions and numerical simulations. Some researchers assess structural vulnerability against earthquakes and quantify uncertainty in seismic risk assessment [13,14]. Wang and Rong [15] investigate cascadingfailures induced by the intentional edge attacks in the power grid of the western United States. Water distribution systems are regarded as large sparse planar graphs with complex network characteristics; Yazdan [16] studies the robustness of a water distribution network and proposes indicators to quantify redundancy. Winkler et al. combine power network topology and a component fragility model to study how the network topology affects the reliability of a power system under natural disasters [17]. Booker estimates cellular network performance under hurricane events [18]. Other pertinent topological properties of electrical and other infrastructure networks are also illustrated [19–25]. In all these studies, only a single non-interacting infrastructure is chosen for risk and vulnerability analysis. However, as technology has advanced, infrastructure systems have become interconnected with each other. With this increasing interdependence, failures may propagate between different infrastructure systems, exceeding the boundaries of a single infrastructure. Therefore a risk and vulnerability analysis should not be undertaken in isolation. Interdependent features of the infrastructure systems must be considered from a perspective of global analysis.

Risk and vulnerability analysis of interdependent infrastructure systems is a relatively new area. Although the United States proposed the concept of infrastructure as early as 1997, it did not appear in the literature on the description of interdependent infrastructure until 2001. Achievements prominently in this research area include those of three US National Laboratories (Sandia, Argonne, Los Alamos) and a research center (National Infrastructure Simulation and Analysis Center, NISAC). Using network theory and system reliability, risk and vulnerability analyses of interdependent infrastructures are then carried out. Recently, a breakthrough work about the performance of interdependent coupled networks has been presented by Buldyrev et al. [2]. They demonstrate a cascade of failures using real-world data from a power network and an Internet network, and develop a framework for understanding the robustness of interacting networks subject to

cascading failures. Meanwhile, the critical threshold, which leads to a failure cascade and to a complete fragmentation of the interdependent networks, is analysed. Dueñas-Osorio et al. [26,27] present a novel approach to model the interdependent response of infrastructure networks under natural hazards and deliberate attacks. They make use of spatial proximity and logical interactions to establish the density and degree of coupling between power and water systems in their model. Svendsen and Wolthusen [28–31] develop a similar graph-theoreticapproach for modeling interdependent infrastructure systems by enduing network nodes and arcs their functional attributes. Other aspects such as vulnerability and flow analysis, failure propagation, and crisis evolution have also been studied [32–37]. Complex network theory is a classical and widely implemented method, able to represent complex topology structures and provide both qualitative and quantitative results. It provides an alternative to other modeling methods by being more physical component detailed. However, the approach alone lacks the ability to capture complicated time-stepped behaviors of infrastructures and is unable to model event-driven interaction [38]. So other modeling techniques have also been applied for interdependent infrastructures vulnerability analysis.

The agent-based modeling (ABM) method [38–43] is another methodology that emerged in the early phase of modeling infrastructure interdependence. It was employed to analyze the behavior of an infrastructure network and its associated economic entity. In agent-based simulations, infrastructures are modeled as complex adaptive systems composed of agents. An agent is a singular piece of code with a specific physical location, function, and memory of past interactions and behaviors. Different agents can be modeled at varying degrees of granularity based on the intended level of resolution modeling.

The object-oriented modeling (OOM) approach is an approach characterizing and analyzing the dynamic behavior of infrastructure systems. It is a modification and evolution of ABM. Using OOM, behaviors at an individual level are defined and the behavior at a global level emerges as a result of individuals, following their own behavior rules, each living together and communicating with each other [44–46]. This model has been widely used in infrastructure interdependence studies. However, it needs a better computer configuration to ensure a faster simulation speed and then to increase the complexity of the simulation platform due to the large number of parameters.

Another methodology for modeling infrastructure interdependences is the input–output model [47–54]. It was proposed by Leontief in 1973. Later, this model was used to establish the relationships between economic sectors and to quantify the correlation between various infrastructure networks. However, the interconnectedness is modeled among infrastructure sectors without dealing with elements of each infrastructure. Interdependence is captured in a macro-perspective rather than at a micro level. Although it is useful for vulnerability assessment, it would be difficult to extend this approach to restoration activities.

High Level Architecture (HLA) [44,55] is a general architecture for modeling and simulating complex distributed systems.

Combining HLA and various modeling/simulation techniques in a distributed simulation environment leads to a hybrid approach for interdependent infrastructure risk and vulnerability analysis. Such an approach was developed originally by the US Department of National Defense, aiming at incorporating interoperability and modularity into long-term simulation objectives. And it was approved as an open standard by the Institute of Electrical and Electronic Engineers in 2000. Since then it has been widely implemented for the purpose of conducting research in the area of critical infrastructure interdependence. However, implementing the hybrid approach for interdependence studies by adopting the HLA standard remains a challenge for many scholars. Whether the HLA standard is able to fulfill the requirements of the desired model/simulation remains unanswered.

Due to the complexity of interdependent infrastructure systems, vulnerability analysis is becoming more interdisciplinary and cross-institutional. Each of the modeling techniques above can be used for interdependence studies while all of them have their own limitations and shortcomings. They are suitable for solving specific problems. In practice, there is no ‘silver bullet solution’ in this area. So a framework of methodology is necessary and needed to solve the problem of analyzing the vulnerability of interdependent infrastructure systems.

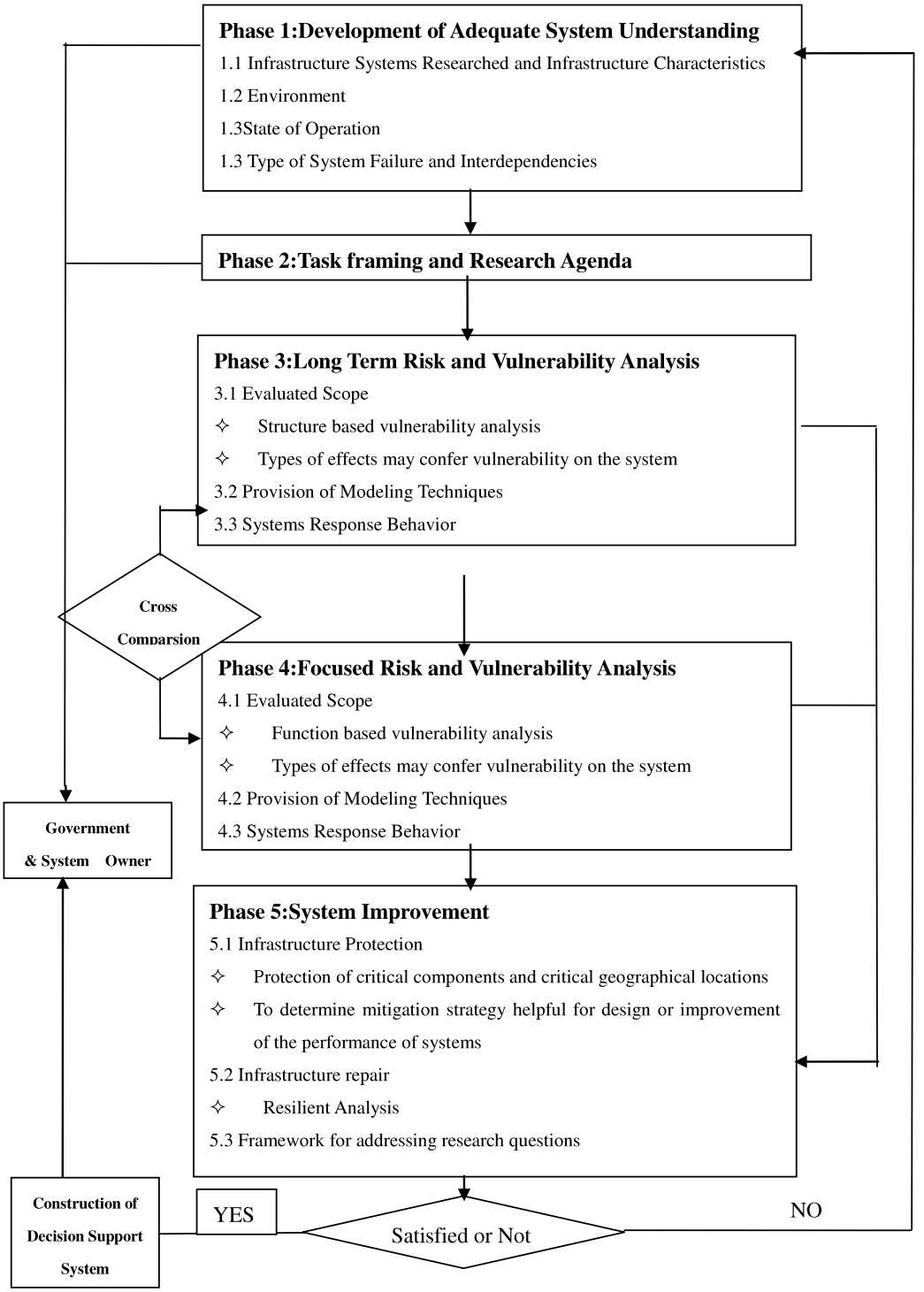
3. A framework for the vulnerability analysis of interdependent infrastructure systems

A methodical framework (Table 1) for the vulnerability analysis of interdependent infrastructure systems is described as follows.

Phase 1 aims at reaching a clear definition of the terms and a mutual understanding of the system being studied. The environment and the state of operation in which the infrastructures operate should be described. The infrastructure environment is the framework in which the owners establish goals and objectives [56]. These factors are influenced by the operating state and condition of each infrastructure. Meanwhile, the environment in turn exerts pressures on infrastructures. Threats and types of system failure should also be studied. Critical infrastructures such as power and water systems often suffer constant threat from various disasters. These threats include failures induced by natural disasters (e.g. earthquakes, hurricanes, storms, ice), random failure (e.g. operation errors, aging, animals) and those induced by intentional disruption (e.g. terrorist attacks). Due to interdependence between different infrastructures, the functions of infrastructure systems are mutually affected. Failure in one infrastructure often propagates to other systems and sometimes even back to the original infrastructure, making it more fragile to various kinds of disturbance. So we need to have a good understanding of interdependences and interdependent system responses under different type of threat.

Task framing and the research agenda are identified in Phase 2. The most common objectives are risk and vulnerability analyses. Meanwhile, risk mitigation measures, infrastructure protection, failure propagation, and interdependence

Table 1
A framework for the vulnerability analysis of interdependent infrastructure systems.



modeling are considered. Terms such as risk, performance, and operating mechanisms should be understood for further analysis. There are several methods for vulnerability analysis of infrastructures such as complex network approaches, agent-based modeling techniques, the input–output model, statistical methods, and so on. When selecting the appropriate approach, several factors should be considered, such as research goals, complexity of the model/simulation, and evaluated scope.

Then both long-term and focused vulnerability analyses are executed. In other words, vulnerabilities at a functional and structural level are comprehensively analyzed and cross compared. The analyses capture different aspects of infrastructures. To carry out an adequate performance analysis, discussion at a structural level will be helpful to design or improve the infrastructures in the long run while analysis at a functional level will be useful in the short term. With respect to system improvement, depending on the results obtained and related feedback, we need to identify critical components and critical locations, and protect them primarily. Then options that would best improve the infrastructure performance should be selected. Meanwhile, infrastructure mitigation strategies that ensure continuous functionality of systems, especially when resources are limited, need to be determined. A protection agenda needs to be established for addressing additional questions. Note that the work done in this paper only provides decision support for decision-making departments. The final decision about actually implementing the proposals of improvement is left to the system owner and operator.

4. Case study

In this paper, the power and water systems of a major city in China are taken as example to analyze the vulnerability of interdependent infrastructures. Power and water systems are selected because they share the same geopolitical boundaries and can help to demonstrate the significance of interdependent effects. Meanwhile, infrastructures such as water and power are single-commodity systems, where resources move from supply points, through a set of arcs and nodes, subject to capacity constraints, and reach the demand points, in an optimal fashion [57]. While the main purpose of this paper is to give a methodological framework for interdependent infrastructure vulnerability analysis, slight modifications of the systems are made for security considerations (Fig. 1).

4.1. Development of adequate system understanding

First, we need to have an in-depth understanding of the systems to be researched. To better understand the structural features of infrastructures, complex network and graph theory is adopted to extract the network topology. Each of the infrastructure systems is defined as a collection of nodes and edges with commodities flowing from node to node along paths in the system. Functional features and operational mechanisms of each infrastructure are considered. Then terms such as vulnerability and interdependence are identified and studied, and different disturbance modes that the infrastructure systems may encounter are analyzed.

4.1.1. Definition of interdependent infrastructure systems

The reference systems for study in our paper are power and water systems. Taking into account the data acquisition, the power grid considered in our paper is mainly composed of generators, 220 kV, 110 kV substation, the main distribution stations as well as edges linking them. Water plants, compressor stations, distribution nodes, and pipelines are mainly considered in the water systems. The power and water systems can be described as networks. For the power system, generators, substations, and load points are represented by nodes, while electrical wires are represented by edges. As for the water supply system, water plants, compressor stations, and distribution points are defined as nodes. Pipelines linking them are considered to be edges. Let $G = \langle V, E, A\rangle$ represents an annotated, simple, and undirected graph, where $V = \{1, 2, \ldots, N\}$ is the set of nodes and $E = \{e_{ij}\}$ is the set of edges. $A = (a_{ij})_{N\times N}$ represents the adjacent matrix of the graph, with a_{ij} equal to 1 if there is an edge joining node i to node j and to 0 otherwise. The basic composition and topological properties of the power and water networks are listed in Table 2.

In this section, we introduce the basic properties of the power and water networks, and several parameters are introduced to help us to understand the basic characteristics of the networks. As node degree is a good indicator of its topological importance, we first determine the degree distribution of the systems. Fig. 2 displays the degree distribution of the power and water networks to 'classify' the topology characteristic. The degree of a node is the number of edges the node is connected to, which has further influence on the connectivity properties of the network. For the power network, most of the nodes have fairly low degree: 67% of the node have degree less than or equal to 2. However, there are some high-degree nodes. The water network has higher average node degree than the power network, but without high-degree nodes.

Several other topological properties have been analyzed for the systems. The characteristic path lengths of the power and water network are 8.247 and 6.338. Characteristic path length is the average length of the shortest path between any two nodes which can be suggested as a measure of the interconnectedness of the network. Another metric measured on the network is the average clustering coefficient. It describes the connectivity of the network at a local level. The value turns out to be as small as 0.047 for the power network. It is bigger for the water network, with a value 0.1291, suggesting a better connection of its neighborhood. As the main function of a power system is to transport power from generators to consumers, a useful measure for the importance of a node is its betweenness. Suppose that power is routed through the shortest path: the betweenness of a node is a substitution for how much power it is transmitting. Average betweenness 797 gives the average frequency of shortest path passing a node.

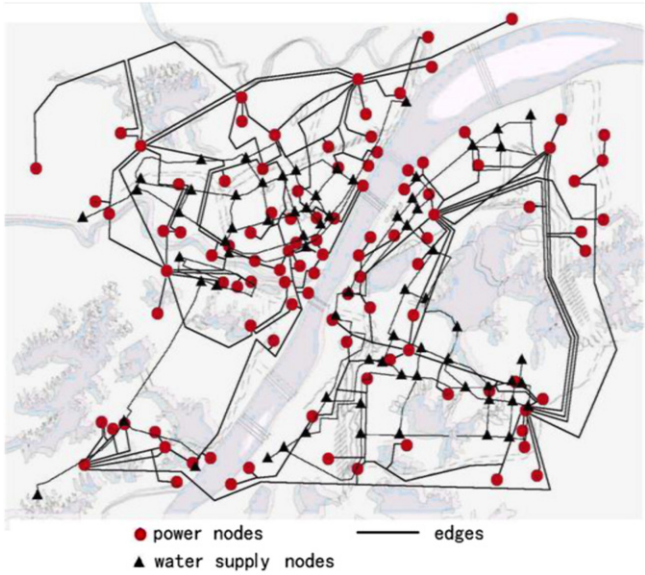


Fig. 1. Geographical representation of the power grid and water systems of a major city in China.

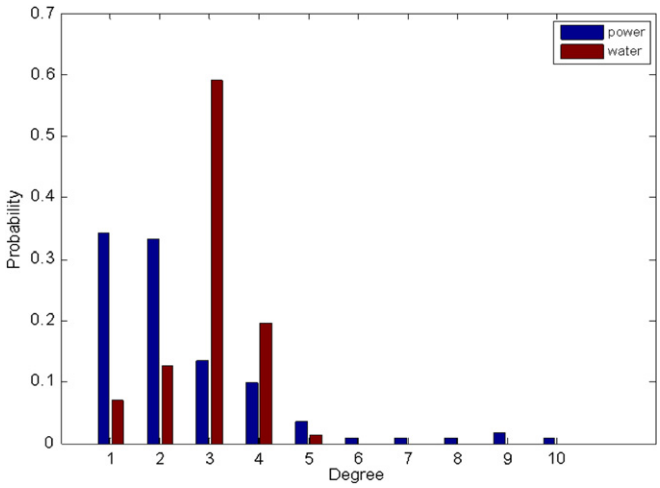


Fig. 2. Degree distribution of the power and water networks.

4.1.2. Perspectives on vulnerability

Vulnerability analysis is one of the basic tools for interdependent infrastructure protection and risk management. The analysis is related to attacks and disruptions. The meaning of the concept varies considerably between different disciplines and even within a particular discipline [58]. Johansson et al. illustrate two interpretations of the concept of vulnerability [59]. In the first interpretation, vulnerability is seen as a global system property that expresses the extent of adverse effects caused by the occurrence of a specific hazardous event. In the second interpretation, vulnerability is used to describe a system component or an aspect of the system. Three aspects of vulnerability (global vulnerability, critical components, and critical geographical locations) are analyzed. In this paper, the reciprocal characteristic path lengths of the network are used to measure network efficiency. When infrastructures are subjected to disturbance, the efficiencies decrease and their vulnerability can be analyzed. Two aspects of infrastructure vulnerability are analyzed: long-term vulnerability and focused vulnerability. Network topologies are taken into account for long-term vulnerability analysis while function and operational mechanisms are considered for the focused vulnerability study. They capture the structural and functional characteristics of infrastructures. Discussion at a structural level will be helpful to design or improve the infrastructures in the long run while analysis at a functional level will be useful in the short term. Meanwhile, we propose a method to find the critical components of the power network, i.e. nodes that are really crucial for the functioning and efficient connectedness of the network. The critical components for both interdependent and independent cases are illustrated and compared.

Table 2
General properties of the power and water networks.

Network	N	E	G	$\langle k\rangle$	C	$\langle l\rangle$	B
Power	111	135	11	2.432	0.047	8.247	797
Water	71	105	7	2.845	0.1291	6.338	249

(N: Number of nodes, E: Number of edges, G: Number of generators, $\langle k\rangle$: The average degree, C: The average clustering coefficient, $\langle l\rangle$: Characteristic path length, B: Nodes average betweenness).

4.1.3. Perspectives on interdependence

For the concept of infrastructure interdependence, we know that infrastructures do not exist in isolation. Especially with the development of scientific technology and social economy, many infrastructure systems in our life are becoming increasingly interconnected and interdependent. First, the issue of interdependence characterization for modeling interdependent infrastructure systems will be addressed. There are different explanations of interdependence in the literature, using different standards. Rinaldi et al. [56] consider the concept of interdependence as a bidirectional relationship between two infrastructures and categorize four general types of interdependence: physical interdependence, cyber interdependence, geographic interdependence, and logic interdependence. Six dimensions of interdependence are analyzed. Meanwhile, Buldyrev et al. [2] also demonstrate a bidirectional dependence such that power stations depend on communication elements for control and communication elements depend on power stations for electricity supply. However, McDaniels et al. consider a unidirectional relationship between systems [60]. Earl et al. [57] have concluded that there are five types of interrelationship between infrastructure systems, namely, input dependence, mutual dependence, shared dependence, exclusive-or dependence, and co-located dependence. For Hausken [61], the relations between infrastructures can be in parallel, in series, combined series–parallel, complex, k-out-of-n redundancy, independent, interdependent, and dependent. Vespignani indicates that infrastructures show a large number of interdependences of differing types [62]. In this paper, we consider infrastructure interdependence as a bidirectional relationship, and co-located and mutual interdependences are considered here. The physical components of the power and water systems are situated within a prescribed geographical region. The activities of one of the systems is dependent upon the activities of the other infrastructure system, and vice versa.

To give the mathematical representation of interdependence between the power and water systems, some nomenclature is first defined.

M: Collection of all infrastructure systems.

W: The water infrastructure system.

P: The power infrastructure system.

$I(P, W)$: Set of nodes in P upon which infrastructure W depends.

$I(W, P)$: Set of nodes in W upon which infrastructure P depends.

$O(P, W)$: Set of all nodes in P upon which infrastructure W depends.

$O(W, P)$: Set of all nodes in W upon which infrastructure P depends.

In this paper, we suppose that water compressor stations depend on a power supply to ensure their normal operation while some water-based generators are driven by sufficient water supplies. Mathematically, $|I(W, P)| = |O(P, W)| = 16 \cdot |I(P, W)| = |O(W, P)| = 3$. Let $i \in I(W, P)$ denote a node in the water system which accepts the power input and let $j \in O(P, W)$ denote a power node which provides supply to the water system. A simple mathematical representation of interdependence $d_1(i, j)$ for the dependence of the water node load on the power node load is given as

$$b_i^w = \begin{cases} b_i^w & b_j^p \neq 0 \\ 0 & b_j^p = 0, \end{cases} \tag{1}$$

where b_i^w is the load of node i in W while b_j^p is the load of node j in P, $e_{ij} = 1$ represent a link between the power node and water node. Let $s \in I(P, W)$ denote a node in the power system which depends on the water system, and let $t \in O(W, P)$ denote a node in the water system upon which the power system depends. A simple interdependent function $d_2(s, t)$ for the dependence of the power node on the water node is given as

$$b_s^p = \begin{cases} b_s^p & 0.75 \leq b_t^w / b_{t.o}^w \leq 1 \\ 0 & 0 \leq b_t^w / b_{t.o}^w < 0.75, \end{cases} \tag{2}$$

where b_s^p is the load of node s in P while b_t^w is the load of node t in W, $b_{t.o}^w$ is the initial load of node t in W, and $e_{st} = 1$. We can see from above that the two infrastructure systems affect each other sequentially and each eventually acts as a supply and a demand infrastructure system as observed in practice.

4.1.4. Perspectives on disturbances and attack strategies

Infrastructure systems operate in an environment subject to disruptions. These disruptions could be caused by hazards such as equipment failure, vegetation (trees), animals, aging, fire, human errors, natural hazards, terrorism, and so on. These types of hazard are divided into three categories here: random failure, deliberate hazards, and natural disasters. Random hazard captures common failures resulting from operation errors, aging, animals, fire, weather, poor maintenance, incorrect design, operating settings, or unintelligent attack. Intelligent attack such as terrorism belongs to the category deliberate hazards. Deliberate attacks on key components of infrastructure systems may cause severe damage and great economic loss. Sometimes they even cause the entire infrastructure system to go into a paralyzed state. Natural hazards such as earthquakes, hurricanes, and debris are "infrequent and high-consequences hazards" [63]. They have very small occurrence frequency but the economic loss and social impact that they can trigger are unimaginable. Usually they also need a long recovery period.

In order to measure infrastructure network vulnerability, we test the impact of power failures on the whole interdependent system. The responses of the system under different disturbance vectors are considered. The first vector is random failure, in which nodes are removed by random selection, with an equal failure probability for each node. The second vector is deliberate attacks. Here, we consider two types of deliberate attack: degree-based attack and load-based (i.e. betweenness) attack. For degree-based attack, disruption scenarios deliberately target the most connected nodes, i.e. the nodes are removed in descending order of degree in the network. If some nodes happen to have the same degree, we randomly choose one of them. Note that we periodically recalculate the degree after each removal, and select the nodes with highest degree next. The degree of a node is a good indicator of its topological importance. This strategy represents a deliberate and intelligent attack in which the attacker chooses to disable nodes with a large number of neighboring components. For load-based attack, disruption scenarios deliberately target the most loaded nodes. This vector is used to approximate an attack on high-load nodes, and it has been reported to result in disproportionately large failures. Meanwhile, after each selection the load will be recalculated and the nodes with the highest load will be deleted next.

4.2. Task framing and research agenda

The power and water systems of a major city in China are taken as an example to analyze the vulnerability of interdependent infrastructures. Both long-term and focused vulnerability analyses are considered. For the long-term vulnerability analysis, infrastructure topologies are mainly discussed; for the focused vulnerability analysis, distinct operating mechanisms of different infrastructure systems are utilized. They capture different aspects of infrastructures. Long-term vulnerability will be helpful to design or improve the infrastructures in the long run while focused analysis will be useful in the short term. At the same time, different interface coupling design strategies based on features such as maximum degree, maximum betweenness, maximum clustering coefficient, and minimum Euclidean distance are constructed. We test the infrastructure response under different coupling modes to find the optimal strategy, and finally we give a method, based on global efficiency variation, to find the key elements of the systems. These key components should be protected primarily for safety considerations.

4.3. Long-term vulnerability analysis

To characterize long-term vulnerability we choose to investigate the network representation from a topological perspective. Infrastructure topologies are the only information for long-term vulnerability analysis. We use this type of vulnerability to give a methodological approach to comprehensively analyze the vulnerability of the networks, and it can help us design infrastructure in the long run. The normalized network efficiency is utilized here relative to the intact efficiency values, enabling relative comparisons across different disturbances. Meanwhile, for simplicity, we only consider coupling modes based on Euclidean distances, i.e. linking water nodes to power nodes that are closest in terms of geographical proximity. Fig. 3 illustrates the dependence of the normalized efficiencies of the power grid on the fraction of nodes removed under three attack strategies. Network responses for both independent and interdependent cases are illustrated for comparison purposes. The normalized network efficiency shown in Fig. 3 reveals that random removal will cause less damage to the network than a high-betweenness-based attack and a high-degree-based attack. This is mainly because the selection of high-degree connection nodes may cause larger system structural destruction. However, there are no significant differences between the degree and betweenness strategies as functional characteristics and operating mechanisms are not taken into account. In addition, we also find that in the case of interdependent situations the decline in efficiency is greater than for independent ones, although they have the same efficiency drop orders for different attack strategies. This is because damage in the power network affects the water systems because of interdependences and they reach back to the originating network, making the power grid more fragile.

4.4. Focused vulnerability analysis

4.4.1. Interface topology design strategies

This section introduces a focused vulnerability analysis methodology for interdependent infrastructures that links the functional modeling technique with different interface coupling modes. The interface design strategies introduced by

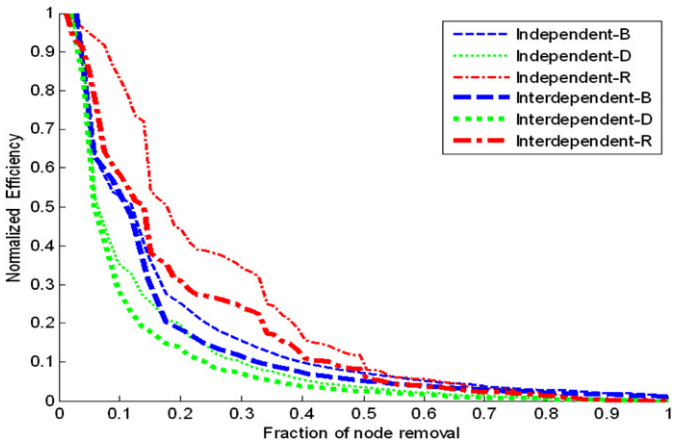


Fig. 3. Dependence of the structural efficiency of the power grid on the fraction of nodes removed under three attack strategies for both independent and interdependent cases.

Table 3
Interface coupling design strategies connecting water and electrical nodes.

Strategy	Connection criterion	Explanation
Betweenness	$\max_i \left[\frac{B(p_i)}{\text{dist}(w_j,p_i)}\right]$ $\forall j$	Link each water compressor node w_j to electrical substation p_i that is highly centralized
Clustering coefficient	$\max_i \left[\frac{C(p_i)}{\text{dist}(w_j,p_i)}\right]$ $\forall j$	Link each water compressor node w_j to electrical substation p_i that is locally well connected
Degree	$\max_i \left[\frac{d(p_i)}{\text{dist}(w_j,p_i)}\right]$ $\forall j$	Link each water compressor node w_j to electrical substation p_i with high degree

Winkler [64] are modified and adopted in this paper. Different interface construction criteria based on features such as betweenness, clustering, vertex degree, and Euclidean distance are illustrated regarding their role in connecting utility systems and propagating failures. One of the simplest and practical approaches is to link each water compressor node to the electrical substation that is closest in terms of geographical proximity via squared Euclidean distance. In addition to this Euclidean distance design strategy, betweenness, clustering, and vertex degree coupling strategies that simultaneously maximize each topological indicator and minimize the distance between the power and water nodes are illustrated below. Meanwhile, for economic feasibility, we link the power generators to the water load nodes in terms of geographical proximity (Table 3).

4.4.2. Provision of modeling techniques for power and water systems

For a power network, the load of a node is the power it sustains, and a lot of models have been given for blackout and cascading failure studies [65–68]. In this paper, a power model based on that of Motter [65] is used to describe the transport of electrical flow in the network. In this model, suppose that the flow is exchanged between every pair of nodes and transmitted along the shortest path connecting them. The load of a node is then defined as the betweenness of the node. Each node has a capacity, which is the maximum flow that the node can handle. Failures in one node create a transient, and cause the power flow in the network to be redistributed according to load laws. We assume that the capacity C_j of node j is proportional to its initial load L_j. $C_j = (1+\alpha)L_j$, where the constant α is the tolerance parameter, chosen as 0.5 in our study. Failures in the nodes, in general, change the distribution of shortest paths. Then, the load at a particular node will change. If it increases and exceeds the capacity limits, the corresponding node fails. Any failure leads to a new redistribution of loads and, as a result, opens the door to the occurrence of cascading failure. This model considers the functional regimes of the power systems and represents cascading blackouts caused by overloads and outages, and is used to produce blackout statistics. Also it captures loads redistribution by means of node betweenness. As for the water supply system, it is composed of water plants, compressor stations, distribution nodes, and water pipelines linking them. The water pipelines are all considered to be the same in our study, namely we ignore the differences of edge capacities and physical construction characteristics of transmission pipelines. A generalized betweenness centrality model is utilized here for modeling water supply systems. Consider the water supply network $G_W = (V_W, E_W)$ with node set V_W and link set E_W. Let $T_{K,L}$ be the flow from source subgraph (V_K, E_K) to sink subgraph (V_L, E_L). The generalized betweenness centrality of $e_{ij} \in E_W$ is defined as

$$G_{ij} = \sum_{\substack{s\in V_K \\ t\in V_L}} \frac{T_{K,L}}{|V_K|\,|V_L|} \frac{\sigma_{s,t}(e_{ij})}{\sigma_{s,t}}, \tag{3}$$

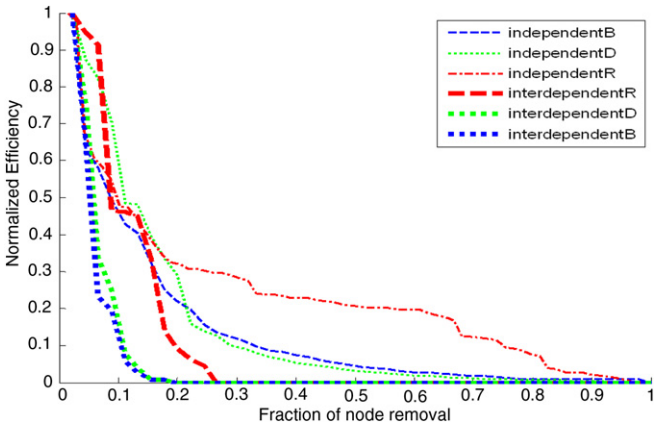


Fig. 4. Dependence of the functional efficiency of the power grid on the fraction of nodes removed under the distance-based construction strategy.

where $e_{ij} \in E_W$, $\sigma_{s,t}$ is the number of shortest paths from node s to node t, and $\sigma_{s,t}(e_{ij})$ is the number of these paths passing through link e_{ij}. Denote b_j^w to be the decision variable designating the flow of node j. The mathematical formulation of the flow in j is given as

$$b_j^w = \sum_i G_{ij} - \sum_m G_{jm}. \tag{4}$$

The simulation process is conducted as follows. When the power node is attacked and removed, the power flows in the network will be redistributed according to the functional model. If the load of a power node exceeds its maximum capacity, the node fails operationally and will be removed. This will be carried out until the power network reaches the steady state. Then if the water nodes cannot get sufficient power supply to ensure their normal operation, due to the power nodes linking them being destroyed, they will be removed. Next, the flows in the water network will be redistributed according to the generalized betweenness centrality model. When the water node for power production cannot supply sufficient water, the corresponding water-based generator will be removed and the power flow will be redistributed again. When the network reaches equilibrium we continue to attack the component according to the attack strategies illustrated above until the whole network collapses.

4.4.3. Simulation analysis

Fig. 4 illustrates the dependence of the functional level efficiencies on the fraction of nodes removed under three attack strategies. The network responses for both independent and interdependent cases are considered for comparison. Here interface designs based on Euclidean distances are illustrated as examples. When the power nodes are selected and removed, the loads of the nodes are redistributed. The load at a node can then be changed. If it increases and exceeds the capacity threshold, the corresponding node fails. This may cause the water nodes to not receive enough power supply and to disrupt, leading to a redistribution of flows in the water system. Then if the water-based generator cannot receive enough water it will be closed, causing a new performance loss. It is illustrated that the power network suffers large normalized efficiency declines as the fraction of nodes removed increases. Meanwhile, it is obviously observed from the figure that the efficiency decline of the interdependent network is larger than the efficiency declines in the independent cases, and different attack strategies have different impact strengths on the network performance. The normalized network efficiency shown in Fig. 4 reveals that the random removal of nodes will cause less damage to the network than a betweenness-based attack and a degree-based attack. The betweenness-based attack causes the largest performance losses. This is mainly because the high-degree and high-betweenness nodes usually bear more loads. When these nodes with high loads are attacked and removed, other nodes are assigned more loads, which may exceed their maximum capacity and cause more performance loss.

Network responses under different interface construction strategies and attack strategies are illustrated in Fig. 5. Design strategies based on distance, clustering coefficient, degree, and betweenness are considered. The distance-based coupling strategy (i.e. link water demand nodes to power supply nodes that are closest in terms of geographical proximity) is the simplest and most practical method which mainly stems from economic considerations. It does not take system connection information into consideration due to its emphasis on geographical closeness and associated costs. We can see from the figure that the distance-based coupling modes have low efficiency change trends under deliberate attacks but are rather vulnerable to random attacks. The betweenness-based coupling strategy links water nodes to power substations that maximize the ratio of node betweenness and distance. It is constructed for the purpose of selecting power stations with high load. Meanwhile, the clustering coupling strategy maximizes the topological criteria clustering coefficient and minimizes the distance between the power and water nodes. This strategy ensures local power supply redundancy. These two strategies both have relatively good performance, and the betweenness-based strategies have better tolerance to random events. This is because the strategy based on betweenness contains both topological and functional information of the power load nodes;

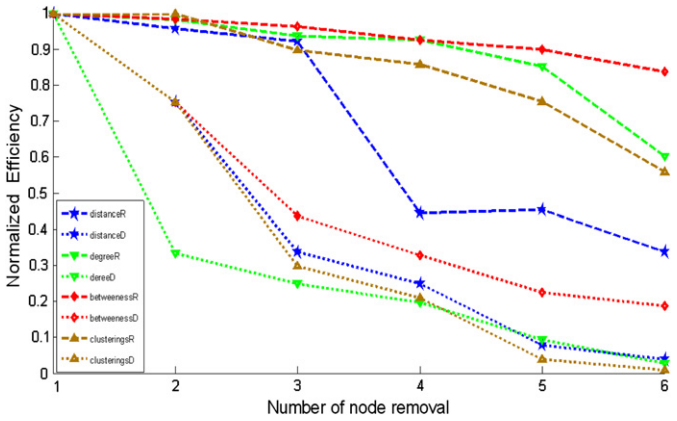


Fig. 5. Comparison of the dependence of the functional efficiency of the power grid on the fraction of nodes removed for different coupling strategies.

Table 4
The five most vulnerable nodes for both interdependent and independent cases.

Node index with independent networks	Node index with interdependent networks
4, 12, 21, 85, 99	4, 21, 31, 85, 99

it is highly efficient to minimize the cascading failure effects yielding highly effective topologies that are easy to operate in practice, but they may not be feasible given economic considerations. The degree-based strategy selects substations that are highly connected, reflecting the engineering practice of linking water demand nodes to available high distribution capacity substations. They have intermediate efficiency drops for random disturbance.

4.5. Identification of critical infrastructure components

In this section, we propose a method to find the critical components of the power network, i.e. nodes that are really crucial for the functioning and efficient connectedness of the network; key elements of both interdependent and independent cases are illustrated and compared. When some nodes lose their function due to failures, there will be a variation in the network performance. We evaluate the importance of an element by considering the drop in the network's performance. Here, a vulnerability indicator for the analysis of the most vulnerable components is defined in terms of the degradation in the global safety efficiency of the network due to the disconnection.

$$V^* = \frac{S_{\text{glob}}(G) - S_{\text{glob}}(G^*)}{S_{\text{glob}}(G)} \tag{5}$$

$$S_{\text{glob}}(G) = \frac{\sum_{i \neq j \in G} \varepsilon_{ij}}{N(N-1)} = \frac{\sum_{i \neq j \in G} 1/d_{ij}}{N(N-1)}, \tag{6}$$

where G^* is the new graph resulting from G. We utilize the method above to evaluate the importance of an element in the network. By considering variations in the network's performance, critical components of the infrastructure networks are found and extracted. Such elements are the ones for primary protection. The method, used as an improvement analysis, will be not only helpful to protect the key elements but also useful to better shape a planned expansion of networks.

By considering the variation in the network's performance we can get the critical components of the networks. The five most critical nodes for both interdependent and independent cases are displayed in Table 4. Note that, for the purpose of simplicity, we just consider the interdependent networks constructed based on distance criteria for identification of the critical infrastructure components. We find that the key nodes for independent cases are those with high loads and high numbers of connections. This is mainly due to the functional characteristic of the network. There is a slight difference for interdependent cases: node 31 appears instead of node 12. These nodes are the targets to protect for normal operation. Although the method illustrated above just considers a global efficiency decline, these nodes can help to better protect the network. To ensure the reliability, these nodes should be conceived with more safety considerations.

5. Conclusion

This research attempts to present a framework to analyze the vulnerability of interdependent infrastructure systems. The power and water systems of a major city in China are chosen as an example for vulnerability analysis. The framework illustrated in our paper can help to better shape a planned expansion of the network. A number of actions should be taken to

reduce the impact of the network's weaknesses on its vulnerability, and these actions might be useful for helping the design of critical infrastructure systems.

Of course, due to the complexity of the operation mechanism of actual systems, the models shown here are just a simplification of what happens in real interdependent systems. Several model refinements need to be further developed if sufficient data and related information are acquired.

1. The restoration process is not taken into account in this study. If some additional data, such as mean time to repair and the recovery process, becomes available, then a better model can be used as the objective function. Also there is still a need for instruments for the analysis of the network's dynamic functionality.
2. When backup support (redundancy) is considered during the interface topology design, a mitigation model can be combined into the proposed design approach; the results in this study do not take redundancy or mitigation into account. The interdependences between two infrastructures are more complicated in reality. There are many types of interdependence among infrastructure systems in practical cases. The cases considered in our study serve merely as an example of all types of interdependence.
3. In this study, the power and water systems of a major city in China are taken as a example to analyze the vulnerability of interdependent infrastructures. They are selected because they share the same geopolitical boundaries and are single-commodity systems. Meanwhile, multi-level infrastructure systems with different operating mechanisms should be illustrated for further analysis. All these will be studied in detail in our future research.

Summing up, this paper illustrates a framework to analyze the vulnerability of interdependent infrastructure systems. Although the work is methodological in nature, it shows the practical relevance of that approach in the analysis of interdependent infrastructure systems. With this method we are able to understand the performance of infrastructures under different attack strategies for various coupling modes, and to identify the key elements of infrastructure systems. The method can help to better shape an expansion of the network. Using the results of the research, critical infrastructure owners and emergency response officials could model different event scenarios and assess their impact on the services provided. Preparedness strategies could be formulated and evaluated to prevent disasters.

Acknowledgments

This work is jointly supported by the National Natural Science Foundation of China (No. 60903174), the Fundamental Research Funds for the Central Universities, HUST: 2010QN016, 2010MS017 and the Fund of Key Lab for Image Processing and Intelligent Control (20093).

References

[1] Presidential decision directive 63. [Online] Available: http://www.ciao.gov.
[2] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[3] T.D. O'Rourke, Critical infrastructure, interdependencies, and resilience, Bridge (2007) 22–29.
[4] T. Adachi, B. Ellingwood, Serviceability of earthquake-damaged systems: effects of electrical power availability and back-up systems on system vulnerability, Reliab. Eng. Syst. Saf. 93 (1) (2008) 78–88.
[5] L. Dueñas-Osorio, J.I. Craig, B.J. Goodno, Seismic response of critical interdependent networks, Earthq. Eng. Struct. Dyn. 36 (2) (2007) 285–306.
[6] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, Critical infrastructure interdependency modeling: a survey of US and international research, ReportINL/EXT-06-11464, Idaho Falls: Idaho National Laboratory, 2006.
[7] H.W. Lewis, R.J. Budnitz, W.D. Rowe, H.J.C. Kouts, F. von Hippel, W.B. Loewenstien, et al., Risk assessment review group report to the US nuclear regulatory commission, IEEE Trans. Nucl. Sci. NS-26 (1979) 4686–4690.
[8] G.E. Apostolakis, How useful is quantitative risk assessment? Risk Anal. 24 (2004) 515–520.
[9] M.E. Pate-Cornell, R. Dillon, Probabilistic risk analysis for the NASA space shuttle: a brief history and current work, Reliab. Eng. Syst. Saf. 74 (2001) 345–352.
[10] R.A. Davidson, H. Liu, I. Sarpong, P. Sparks, D.V. Rosowsky, Electric power distribution system performance in Carolina hurricanes, Nat. Hazard. Rev. 4 (1) (2003) 36–45.
[11] H. Liu, R.A. Davidson, D.V. Rosowsky, J.R. Stedinger, Negative binomial regression of electric power outages in hurricanes, J. Infrastruct. Syst. 11 (4) (2005) 258–267.
[12] H. Liu, R.A. Davidson, V.A. Tatiyana, Spatial generalized linear mixed models of electric power outages due to hurricanes and ice storms, Reliab. Eng. Syst. Saf. 93 (2009) 875–890.
[13] P.S. Koutsourelakis, Assessing structural vulnerability against earthquakes using multi-dimensional fragility surfaces: a Bayesian framework, Probab. Eng. Mech. 25 (2010) 49–60.
[14] Bruce R. Ellingwood, Kursat Kinali, Quantifying and communicating uncertainty in seismic risk assessment, Struct. Saf. 31 (2009) 179–187.
[15] Jian-Wei Wang, Li-Li Rong, Robustness of the western United States power grid under edge attack strategies due to cascading failures, Saf. Sci. 49 (2011) 807–812.
[16] Alireza Yazdan, Paul Jerey, A complex network approach to robustness and vulnerability of spatially organized water distribution networks, Physics (2010) 1–18.
[17] James Winkler, Leonardo Dueñas-Osorio, Robert Stein, Devika Subramanian, Performance assessment of topologically diverse power systems subjected to hurricane events, Reliab. Eng. Syst. Saf. 95 (2010) 323–336.
[18] Graham Booker, Jacob Torres, Seth Guikema, Alex Sprintson, Kelly Brumbelow, Estimating cellular network performance during hurricanes, Reliab. Eng. Syst. Saf. 95 (2010) 337–344.
[19] A. Cardillo, S. Scellato, V. Latora, S. Porta, Structural properties of planar graphs of urban street patterns, Phys. Rev. E 73 (6) (2006) 066107(1-8).
[20] S. Lammer, B. Gehlsen, D. Helbing, Scaling laws in the spatial structure of urban road networks, Physica A 363 (1) (2006) 89–95.
[21] L. Buzna, L. Issacharoff, D. Helbing, The evolution of the topology of high-voltage electricity networks, Int. J. Crit. Infrastruct. 5 (1) (2009) 72–85.
[22] L.C. Freeman, A set of measures of centrality based on betweenness, Sociometry 40 (1) (1977) 35–41.
[23] U. Brandes, A faster algorithm for betweenness centrality, J. Math. Sociol. 25 (2) (2001) 163–177.

[24] L. Dueñas-Osorio, S.M. Vemuru, Cascading failures in complex infrastructure systems, Struct. Saf. 31 (2009) 157–167.
[25] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, D. Helbing, Transient dynamics increasing network vulnerability to cascading failures, Phys. Rev. Lett. 100 (21) (2008) 218701(1-4).
[26] Dueñas-Osorio Leonardo, James I. Craig, Barry J. Goodno, Seismic response of critical interdependent networks, Earthq. Eng. Struct. Dyn. 36 (2007) 285–306.
[27] Dueñas-Osorio Leonardo, James I. Craig, Barry J. Goodno, et al., Interdependent response of networked systems, J. Infrastruct. Syst. 13 (3) (2007) 185–194.
[28] N.K. Svendsen, S.D. Wolthusen, Connectivity models of interdependency in mixed-type critical infrastructure networks, Inf. Secur. Tech. Rep. 12 (2007) 44–55.
[29] N.K. Svendsen, S.D. Wolthusen, Multigraph dependency models for heterogeneous critical infrastructures, in: Proceedings of the First Annual IFIP TC 11.10 International Conference on Critical Infrastructure Protection, Springer-Verlag, Hanover, NH, USA, 2007, pp. 337–350.
[30] N.K. Svendsen, S.D. Wolthusen, Analysis and statistical properties of critical infrastructure interdependency multiflow models, in: Proceedings from the Eighth Annual IEEE SMC Information Assurance Workshop, United States Military Academy, IEEE Press, West Point, NY, USA, 2007, pp. 247–254.
[31] N.K. Svendsen, S.D. Wolthusen, Graph models of critical infrastructure interdependencies, in: A.K. Bandara, M. Burgess (Eds.), Inter-Domain Management, Proceedings of the First International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2007, in: Lecture Notes in Computer Science, vol. 4543, Springer-Verlag, Oslo, Norway, 2007, pp. 208–211.
[32] M. Ouyang, L. Hong, Z. Mao, M. Yu, F. Qi, Simul. Modell. Pract. Theory 17 (2009) 817–828.
[33] I.B. Utne, P. Hokstad, J. Vatn, A method for risk modeling of interdependencies in critical infrastructures, Reliab. Eng. Syst. Saf. 98 (6) (2011) 671–678.
[34] I.B. Utne, P. Hokstad, J. Vatn, A method to modeling interdependencies in risk analysis of critical infrastructures, in: Reliability, Risk and Safety: Theory and Applications, CRC Press, 2009.
[35] Pengcheng Zhang, Srinivas Peeta, A generalized modeling framework to analyze interdependencies among infrastructure systems, Transp. Res. Part B 45 (2011) 553–579.
[36] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. De Porcellinis, R. Setola, Modelling interdependent infrastructures using interacting dynamical models, Int. J. Crit. Infrastruct. 4 (2008) 63–79.
[37] S. De Porcellinis, R. Setola, S. Panzieri, G. Ulivi, Simulation of heterogeneous and interdependent critical infrastructures, Int. J. Crit. Infrastruct. 4 (2008) 110–128.
[38] A. Tolk, A.M. Uhrmacher, Agents: agenthood, agent architecture, and agent taxonomies. Agent-directed simulation and systems engineering, WILEYVCH, 2009.
[39] Y. Tomita, C. Fukui, H. Kudo, Cooperative protection system with an agent model, IEEE Trans. Power Deliv. 13 (4) (1998) 1060–1066.
[40] A. Wildberger, Modeling with independent intelligent agents for distributed control of the electric power grid, in: Proceedings of the American Power Conference, 1997.
[41] A. Wildberger, Modeling the infrastructure industries as complex adaptive systems, in: Proceedings of Simulation International, San Diego, CA, 1998, pp. 168–173.
[42] M. Amin, Toward secure and resilient interdependent infrastructures, J. Infrastruct. Syst. 8 (3) (2002) 67–75.
[43] N. Basu, R. Pryor, T. Quint, Aspen: a microsimulation model of the economy, SAND96-2459, Albuquerque, Sandia National Laboratories, NM, 1996.
[44] Cen Nan, Irene Eusgeld, Adopting HLA standard for interdependency study, Reliab. Eng. Syst. Saf. 96 (2011) 149–159.
[45] I. Eusgeld, W. Kroger, G. Sansavini, M. Schlapfer, E. Zio, The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures, Reliab. Eng. Syst. Saf. 94 (2009) 954–963.
[46] A. Borshchev, A. Filippov, From system dynamics and discrete event to practical agent based modeling: reasons, techniques, tools, in: Proceedings of the 22nd International Conference of the System Dynamics Society, 2004.
[47] M. Leung, Y. Haimes, J. Santos, Supply- and output-side extensions to the inoperability input–output model for interdependent infrastructures, J. Infrastruct. Syst. 13 (4) (2007) 299–310.
[48] Y. Haimes, B. Horowitz, J. Lambert, Inoperability input–output model _IIM_ for interdependent infrastructure sectors. II: case study, J. Infrastruct. Syst. 11 (2) (2005) 80–92.
[49] Y. Haimes, B. Horowitz, J. Lambert, Inoperability input–output model for interdependent infrastructure sectors. I: theory and methodology, J. Infrastruct. Syst. 11 (2) (2005) 67–79.
[50] P. Jiang, Y. Haimes, Risk management for Leontief-based interdependent systems, Risk Anal. 24 (5) (2004) 1215–1229.
[51] P. JJiang, Input–output inoperability risk model and beyond: a holistic approach, Ph.D. Dissertation, Systems and Information Engineering Dept., Univ. of Virginia, Charlottesville, 2003.
[52] J. Santos, Interdependency analysis: Extensions to demand reduction inoperability input–output modeling and portfolio selection. Ph.D. Dissertation, Dept. of Systems and Information Engineering, Univ. of Virginia, Charlottesville, 2003.
[53] J. Santos, Y. Haimes, Modeling the demand reduction input–output (I–O) inoperability due to terrorism of interconnected infrastructures, Risk Anal. 24 (6) (2004) 1437–1451.
[54] J. Santos, Inoperability input–output modeling of disruptions to interdependent economic systems, J. Syst. Eng. 9 (1) (2006) 20–34.
[55] Irene Eusgeld, Cen Nan, Dietz Sven, System-of-systems approach for interdependent critical infrastructures, Reliab. Eng. Syst. Saf. 96 (2011) 1–8.
[56] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelley, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Syst. Mag. 21 (6) (2001) 11–25.
[57] Earl E. Lee II, John E. Mitchell, William A. Wallace, Restoration of services in interdependent infrastructure systems: a network flows approach, IEEE Trans. Syst. Man Cybern. Part C Appl. Rev. 37 (6) (2007) 1303–1317.
[58] Y.Y. Haimes, On the definition of vulnerabilities in measuring risks to infrastructures, Risk Anal. 26 (2) (2006) 293–296.
[59] Jonas Johansson, Henrik Hassel, An approach for modelling interdependent infrastructures in the context of vulnerability analysis, Reliab. Eng. Syst. Saf. 95 (2010) 1335–1344.
[60] T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, D. Reed, Empirical framework for characterizing infrastructure failure interdependencies, J. Infrastruct. Syst. 13 (3) (2007) 175–184.
[61] Kjell Hausken, Defense and attack of complex and dependent systems, Reliab. Eng. Syst. Saf. 95 (2010) 29–42.
[62] Alessandro Vespignani, The fragility of interdependency, Nature 464 (2010) 984–985.
[63] Ming Ouyang, Leonardo Dueñas-Osorio, An approach to design interface topologies across interdependent urban infrastructure systems, Reliab. Eng. Syst. Saf. 96 (2011) 1462–1473.
[64] J. Winkler, L. Dueñas-Osorio, R. Stein, D. Subramanian, Interface network models for complex urban infrastructure systems, J. Infrastruct. Syst. 17 (4) (2011) 138–150.
[65] A. Motter, T. Nishikawa, Y. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (2002) 065102(1–4).
[66] A. Motter, Cascade control and defense in complex networks, Phys. Rev. Lett. 93 (2004) 098701(1–4).
[67] I. Dobson, B.A. Carreras, V. Lynch, D.E. Newman, Complex systems analysis of series of critical points, and self-organization, Chaos 17 (2) (2007) 026103(1-33).
[68] I. Dobson, B.A. Carreras, D.E. Newman, An initial model for complex dynamics in electric power system blackouts, in: Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001.