Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects

Panayiotis Kotzanikolaou[1], Marianthi Theoharidou[2], and Dimitris Gritzalis[2]

[1] Dept. of Informatics, University of Piraeus,
85 Karaoli & Dimitriou, GR-18534, Piraeus, Greece
pkotzani@unipi.gr

[2] Dept. of Informatics, Athens University of Economics & Business,
76 Patission Ave., GR-10434, Athens, Greece
{mtheohar,dgrit}@aueb.gr

Abstract. One of the most challenging problems, when protecting critical infrastructures, is the identification and assessment of interdependencies. In this paper we examine the possible cumulative effects of a single security incident on multiple infrastructures. Our method provides a way to identify threats that may appear insignificant when examining only first-order dependencies, but may have potentially significant impact if one adopts a more macroscopic view and assesses multi-order dependencies. Based on previous work, we utilize existing first-order dependency graphs, in order to assess the effect of a disruption to consequent infrastructures.

Keywords: Critical Infrastructure, Interdependencies, Risk, Cascading Effect.

1 Introduction

Protecting Critical Infrastructures (CI) poses challenges not only due to the significant social impact caused by disruption of their services, but also due to the high number of dependencies between them. The most important parameter that interdependencies may introduce is that they allow security incidents to escalate or cascade to different infrastructures, thus causing potentially significant impact to multiple types of sectors, individuals or countries. Motivating examples for this paper include the electric power disruptions in California (2001) [1], as well as the major blackouts in the US, Canada and Europe (2003) [2].

The electric power disruptions in California caused cross-sectoral cascading effects [1]. Electric power disruptions affected the natural gas production, the operation of petroleum product pipelines transporting gasoline and jet fuel within California and to Nevada and Arizona, and the operation of massive pumps used to move water for crop irrigation (first-order dependencies). Gas production curtailed by power losses directly impacted gas supplies for generating units, further exacerbating power problems (feedback loop). Tight natural gas supplies

S. Bologna et al. (Eds.): CRITIS 2011, LNCS 6983, pp. 104–115, 2013.

also had the potential to shut down gas-fired industrial co-generation units producing steam for injection into California's heavy oil fields (second-order dependencies), thus potentially reducing heavy oil recovery (third-order dependencies). Similarly, the disruption of product pipelines caused inventories to build up at refineries and draw down at the product terminals (second-order dependencies), including several major California airports. Declining jet fuel stocks at airports caused several major airline operators to consider contingency plans in the event of fuel shortages (third-order dependencies).

Similarly, the blackouts in the US-Canada (August 2003), Southern Sweden and Eastern Denmark (September 2003), and Italy (September 2003) highlight the possibility of international cascading effects. The common element in these cases is that a single event, which may have been assessed initially to pose relatively limited and isolated effect, is indeed causing problems to other infrastructures. In all three blackouts, we observe a chain of failures causing cross-border effects and significant impact to people, even without estimating the impact of their cross-sector effect like the California example.

The impact of a disruption, or failure, may spread both geographically and across multiple sectors. Identifying interdependencies may appear to be a useful task; however, there are specific dependencies, which are not easy to identify, e.g. social dependencies. Social dependencies may refer, for example, to the changes in individual behavior during a crisis, which may consequently affect various infrastructures or networks. For example, a disruption in the transportation sector may cascade in wireless communication networks [3]. Although the identification of first-order interdependencies may be sufficient, in order to assess the risks of a particular CI, they may fail to capture cascading risks in a macroscopic level. For example, one or more relatively minor, security incidents on one CI may cause cascading and escalating impacts to an interdependent CI of a second or third level. Identifying multi-order CI interdependencies leads to a more accurate assessment on the criticality level of an CI or a sector. It also enables the identification of chains between interdependent CIs. This way, it becomes possible to identify the "most" critical among the infrastructures and adopt more cost-efficient security controls, so as to reduce cumulative risks and avoid catastrophic cascading failures.

In this paper we will analyze the cascading effects of security incidents in CIs, so as to assess the possible cumulative effects of a single security incident on multiple CIs. Such effects are the result of interdependencies, which are hard to identify and - most of the times - are out of the scope of mainstream risk assessment methodologies. Our ultimate goal is to reduce the cumulative risks of security incidents and to avoid catastrophic cascading failures, by reducing threat, vulnerability, and/or impact levels, in the most appropriate and cost-efficient steps of a chain of interdependent CIs.

The paper is organized as follows. Section 2 provides definitions of interdependencies and disruptions on CIs. Section 3 summarizes the method on which the proposed approach is based on. Then, it describes the new steps required, in order to assess second-order dependencies. This is followed by a comprehensive example.

Section 4 describes other existing approaches in CI dependency assessment. The paper concludes with Section 5, where future research steps are referred to.

2 Interdependencies and Disruptions

Following [1, 4], dependencies may be:

– *Physical* (the state of a CI depends upon the material output(s) of the other CI),
– *Cyber/Informational*(the state of a CI depends on information transmitted through the other CI),
– *Geographic* (the state of a CI depends on an environmental event on another CI),
– *Logical* (the state of a CI depends upon the state of another CI via a non-physical, cyber, or geographic connection) or
– *Social* (the state of a CI is affected by the spreading of disorder to another CI related to human activities).

The interdependence-related disruptions or outages can be classified as cascading, escalating, or common-cause [1]. A *cascading* failure is defined as a failure in which a disruption in an infrastructure A affects one or more components in another infrastructure, say B, which in turn leads to the partial or total unavailability of B. An *escalating* failure is defined as a failure in which an existing disruption in one infrastructure exacerbates an independent disruption of another infrastructure, usually in the form of increasing the severity or the time for recovery or restoration of the second failure. A *common-cause* failure occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause. This occurs when two infrastructures are co-located (geographic interdependency) or because the root cause of the failure is widespread (e.g., a natural or a man-made disaster).

3 Assessing Hidden Interdependencies for Critical Infrastructures

Critical Infrastructure Protection (CIP) is usually based on risk assessment reviews [5]. With traditional risk assessment methodologies, a Critical Infrastructure Operator (CIO for short) will assess the information risks of all the assets within the organization, in order to identify the most critical assets. The criticality of the assets is related to the potential impact for the organization, which may result because of the unavailability, disclosure, or modification of an asset. In recent CIP research [1, 5–8], the criticality of an asset depends not only on the potential impact of a security incident on the organization itself, but also on the outgoing societal risk caused to other dependent organizations. For example, if a major energy provider is experiencing a disruption for a certain period (i.e. unavailability of the core service of this CIO), this will result in potential impact not only for the operator itself, but also for any other interconnected operators belonging to various sectors, and also for all the potential users of all the dependent operators. In order to identify and mitigate the security risks caused due to the interdependencies between CIOs, our approach will be based on a recently proposed, multi-layer risk assessment methodology for interdependent critical infrastructures [7, 8].

3.1 Pre-requisites: A Risk-Based Criticality Assessment Methodology

In [7, 8], a risk-based criticality assessment methodology is presented. The goal of the methodology is to identify which infrastructures are the most critical, and to assess the security risks related with these CIs. The rationale of the methodology relies on the fact that traditional risk assessment methodologies are organization-oriented (i.e. they assess the security risks of an infrastructure mainly by measuring the possible consequences for the operator organization, in case of a security event). For this reason, they cannot always capture the criticality of an infrastructure in a macroscopic level (i.e. what are the *societal impacts*, in case of a security event realized on an infrastructure). This is closely related with the interdependencies between CIs.

Based on the interdependencies between different infrastructures, in [7, 8] the *criticality level* of an infrastructure (or a complete sector) is assessed based on three risk factors: (a) the *societal risk* that may be caused to the society (or to a significant number of persons), due to a security incident realized to the particular infrastructure; (b) the outgoing risk on an infrastructure, which mainly consists of the potential risk caused to other infrastructures due to a security incident to this infrastructure; (c) the incoming risk on an infrastructure, which mainly consists of the potential risk suffered by the infrastructure in question, due to a security incident caused to another dependent infrastructure.

The methodology is organized in three phases or levels of analysis. In the Operator level, it is assumed that all the participating CIOs have already conducted an organization-wide risk assessment and have, thus, identified their first-order dependencies. Since these interdependencies are known, each CI is expected to assess its incoming risks, i.e. the potential risks caused to the CI due to a security event in another connected infrastructure. In the second phase (Sector level), the results of the previous phase (incoming risks[1] of CIs) are analyzed by experts of each infrastructure sector, in order to estimate the outgoing societal impact of an incident or threat on other infrastructures (dependent CIs) and the society. In the third phase, the sector coordinators will reexamine all the results of the previous layers, in order to identify and confirm the dependencies between CIs, and form a more macroscopic view for the criticality of each sector at a national level, e.g. ICT, transport or power sector.

[1] For a particular dependency $A \rightarrow B$, the incoming risk estimated by CI_B is essentially equivalent to the outgoing risk estimated by CI_A. By considering both views, sector-level experts may fine-tune the risks identified at the operator-level analysis.

This methodology [7, 8] identifies and assesses interdependencies between infrastructures, despite which sector each infrastructure is located or depends on. However, it only considers first-order dependencies, i.e. direct physical, logical, procedural, geographical or social dependencies between two CIs. Thus, the identification of second- or third-order dependencies is not captured and as described in Section 1 through real examples, such complex, chain dependencies are often the cause of major consequences.

3.2 The Proposed Method

Following the approach suggested in [8], by defining the first-order outgoing risks of various infrastructures in an Operator level and analyzing their societal risk in a Sector level, it is possible for the risk assessor to construct the *Dependency Risk Table*, as shown in Table 1 (based on an example of 8 infrastructures and 4 sectors).

The Dependency Risk Table summarizes the dependencies of each infrastructure to others. It also indicates for each dependency the source impact $SImp$ (i.e. the effect on the source of the dependency), the incoming impact $IImp$ (i.e. the potential effect on the dependent infrastructure), as well as the incoming impact scale and the likelihood of the source impact being realized. The product of the last two values is used for assessing the dependency risk. Method [8] assesses the societal risk of a disruption due to an (inter)dependency, and does not take into account the impact on the infrastructure operator at this stage (Sector level).

For example, as shown in Table 1, CI_A has two dependent CIs, mainly CI_G and CI_F. The infrastructure CI_F (the second raw of the table) has a Cyber (or Infromational) dependency from CI_A, since CI_F has outsourced its payment services to CI_A. A possible service unavailability of CI_A will produce an incoming dependency impact to CI_F (unavailability of its payment services), denoted as $I_{A,F}$. This would cause loss of public confidence to CI_F, of a relatively low impact ($I_{A,F} = (L)ow$). The likelihood of an event causing unavailability to CI_A (and consequently a cascading unavailability to CI_F) is considered low, i.e. $L_{A,F} = (L)ow$. Thus the outgoing risk of this dependency, denoted as $R_{A,F} = I_{A,F} \times L_{A,F}$ has a risk value equal to 4, based on a risk matrix as described in [8]. Although the example considers total loss of availability as source and incoming impact, modified risk matrices can also be formed in order to assess various levels of service loss.

Dependencies can be visualized through graphs, as shown in Figure 1. An infrastructure is denoted as a circle. An arrow from $X \rightarrow Y$ denotes a risk dependency, i.e. an outgoing risk from the infrastructure CI_X to the infrastructure CI_Y. A bi-directional arrow $X \leftrightarrow Y$ denotes an outgoing risk from CI_X to CI_Y and another outgoing risk from CI_Y to CI_X. The number in each arrow refers to the level of the incoming risk for the receiver due to the dependency, based on a risk scale $[0-9]$. For example, CI_G has an incoming dependency risk of 6 from the infrastructure CI_A. This risk value refers to the likelihood of a disruption from CI_A to cascade to CI_G, as well as the societal impact in the case of such an event.

Table 1. Dependency Risks

Dependent CIs	Dep. Type	Description	SImp	IImp	IImp Type	Scale $I_{j,i}$	LH $L_{j,i}$	Risk $R_{j,i}$
	CI_A (Finance Sector)							
CI_F	C	Provides payment services	UA	UA	Public Confidence	L	L	4
CI_G	C	Provides payment Services	UA	UA	Public Confidence	H	L	6
	CI_B (Energy Sector)							
CI_A	P	Depends for power	UA	UA	Economic Impact	VL	L	3
CI_C	P	Depends for power	UA	UA	Public Confidence	H	VL	5
CI_D	P	Depends for power	UA	UA	Economic Impact	VH	VL	6
CI_E	P	Depends for power	UA	UA	Economic Impact	H	VL	5
CI_F	P	Depends for power	UA	UA	Public Confidence	L	L	4
CI_G	P	Depends for power	UA	UA	Public Confidence	H	L	6
	CI_C (ICT Sector)							
CI_F	C	Network Services	UA	UA	Public Confidence	L	VL	3
CI_G	C	Network Services	UA	UA	Public Confidence	H	VL	5
	CI_D (ICT Sector)							
CI_C	P	Depends for network connectivity	UA	UA	Public Confidence	H	VL	5
CI_E	P	Depends for network connectivity	UA	UA	Economic Impact	H	VL	5
	CI_E (ICT Sector)							
CI_F	G	Hosts backup systems	UA	UA	Public Confidence	L	VL	3
CI_G	G	Hosted in its facilities	UA	UA	Public Confidence	VH	VL	6
	CI_F (Government Sector)							
CI_G	C	Receives insurance information	UA	UA	Public Confidence	L	L	4
CI_G	S	Industrial action	UA	UA	Economic Impact	L	M	5
	CI_G (Government Sector)							
CI_F	S	Industrial action	UA	UA	Economic Impact	M	M	6

Dependency. P: Physical, C: Cyber, G: Geographic, Log: Logical, S: Social
Source/Incoming Impact (SImp/IImp). UA: Unavailability, DS: Disclosure, MD: Modification
Scale/Likelihood. VH: Very High, H: High, M: Medium, L: Low, VL: Very Low

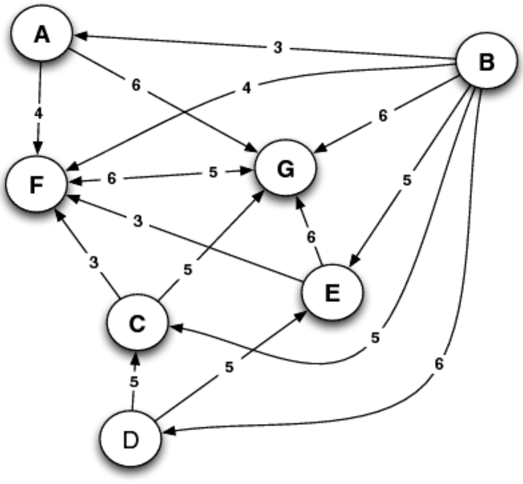

Fig. 1. Dependency Risk Graph of interdependent CIs

In order to estimate second-order dependency risks, the following steps are performed for each examined critical infrastructure CI_i:

1. **Identification of the 1^{st}-order dependencies of CI_i.** Identify all the incoming dependency risks of CI_i. For simplicity, and without loss of generality, we assume that the incoming risk $CI_j \to CI_i$ has risk value $R_{j,i} = L_{j,i} \times I_{j,i}$, where $I_{j,i}$ is the incoming impact and $L_{j,i}$ is the likelihood of this incoming impact, as computed in Table 1. For example, as shown in Figure 1, the infrastructure C has an incoming dependency from B and another one from D. We will examine the $D \to C$, 1^{st}-order dependency.
2. **Identification of the n-order dependencies of CI_i.** During this step, we identify the correlated 2^{nd} and more generally, n-order dependencies of CI_i. For each 1^{st}-order incoming $CI_j \to CI_i$ dependency of the examined infrastructure CI_i, examine the source infrastructure CI_j in order to identify its possible incoming dependencies $CI_k \to CI_j$. If the incoming impact of the dependency $CI_k \to CI_j$ is of the same type as the source impact of the $CI_j \to CI_i$ dependency, then mark this dependency and continue until all the possible threads of the n-order dependencies of CI_i have been examined. In the example of Figure 1, for the $C \to D$ dependency identified in step 1, we examine the 2^{nd}-order dependency $B \to D$ (the complete n-order dependency of this thread is $B \to D \to C$). By examining Table 1 the incoming impact of the $B \to D$ dependency is of type Unavailability ($IImp(B \to D) = UA$), which is of the same type as the source impact of the $D \to C$ dependency ($SImp(D \to C) = UA$). Thus this second order dependency is marked and we continue by examining possible 3^{rd}-order dependencies. Since B has no other incoming dependencies, all the possible n-order dependencies of this thread have been examined and marked according to the rule

of this step and we can continue with another thread of C's dependencies. By examining Figure 1 we see that the infrastructure C has another incoming dependency $B \rightarrow C$. Thus C has a 1^{st}-order and a 2^{nd}-order dependency from B.

3. **Evaluation of the n-order dependency risks.** Check if the $CI_k \rightarrow CI_j$ dependency has been marked in the previous step. In this case, the 2^{nd}-order dependency risk $Risk(CI_k \rightarrow CI_j \rightarrow CI_i) \equiv R_{k,j,i}$ for short, can be computed as:

$$R_{k,j,i} = R_{j,i} \times L_{k,j,i} = (I_{j,i} \times L_{j,i}) \times L_{k,j,i} = I_{j,i} \times (L_{j,i} \times L_{k,j,i}) \qquad (1)$$

where $L_{k,j,i}$ is the conditional probability of the likelihood $L_{j,i}$ being realized, given the fact that the likelihood $L_{k,j}$ has been realized, i.e.

$$L_{k,j,i} = P(L_{j,i}/L_{k,j}) = \frac{(L_{j,i} \cap L_{k,j})}{(L_{k,j})} \qquad (2)$$

If we consider a worst-case scenario, then $L_{k,j}$ and $L_{j,i}$ can be considered as likelihoods of independent events and thus the conditional probability of Equation 2 can become:

$$L_{k,j,i} = P(L_{j,i}/L_{k,j}) = \frac{(L_{j,i} \cdot L_{k,j})}{(L_{k,j})} = L_{j,i} \qquad (3)$$

Thus from Equations 1,3 we have:

$$R_{k,j,i} = R_{j,i} \times L_{j,i} = I_{j,i} \times {L_{j,i}}^2 \qquad (4)$$

Equation 4 can be trivially extended in order to compute the n-order dependency risk $Risk(CI_1 \rightarrow CI_2 \rightarrow ... \rightarrow CI_n) \equiv R_{CI_1,CI_2,...,CI_n}$ as:

$$R_{CI_1,CI_2,...,CI_n} = R_{CI_{n-1},CI_n} \times L_{CI_{n-1},CI_n} = I_{CI_{n-1},CI_n} \times (L_{CI_{n-1},CI_n})^n \qquad (5)$$

4. **Examine next infrastructure.** Repeat from step one until all the examined infrastructures are exhausted.
5. **Rank cascading risks.** Rank all the examined cascading risks and choose the most critical paths (according to a risk threshold set by the security experts).
6. **Mitigate cascading risks.** Consider risk mitigation controls throughout the path under a cost-benefit analysis, in order to reduce the dependency risks below the threshold, both on a sector and an infrastructure level. The examination of n-order dependencies allows the identification of the most critical infrastructures and their respective sectors in terms of chain effects. The examination of the risk path provides additional options for risk mitigation, in a 'cost-efficient' way. For example, the alternative risk mitigation approaches include:
   - Controls to reduce the likelihood of the possible events that may cause the source impact in the source of the examined dependency chain.

- Controls that reduce the likelihood of the possible events that cause the source impact in any intermediate node within the chain.
- Controls that reduce the impact of dependencies by creating alternative paths.
- Controls that increase the resilience of critical nodes in a dependency chain, thus reducing the impact on individual nodes.

When planning investments for critical infrastructures or sectors, the information provided by the dependency graphs and n-order dependencies can be significant. This is due to the fact that adopting such a macroscopic view permits a more efficient distribution of budget within or across sectors. It also reduces the cost of applying excessive countermeasures on all infrastructures, while it increases their effectiveness, not only in respect of the particular infrastructure, but of the dependent ones as well.

3.3 Example

If we consider an example of a second-order dependency, we would have three infrastructures: CI_A: Power Generator, CI_B: Train, CI_C: Mobile Network. These infrastructures face the following interdependencies:

$CI_A \rightarrow CI_B$: Physical Dependency (power supply)
$CI_A \rightarrow CI_C$: Physical Dependency (power supply)
$CI_B \rightarrow CI_C$: Social Dependency

Following the method described above, we perform the following steps:

1. We examine possible threats that will result in the Source Impact "disruption of CI_A", which causes blackout in a region (Societal Risk of CI_A).
2. Disruption in power supply causes several trains to be immobilized for several hours in this region (Incoming Impact in CI_B). This is a cascading disruption from A to B.
3. Disruption to communication network due to the blackout (Incoming Impact in CI_C). This is a cascading disruption from A to C, but it is also a common cause disruption between B and C.
4. Disruption to communication network follows due to heavy load (Incoming Impact in CI_C). This is a cascading disruption from B to C.

In order to calculate the cascading risk of the initial event from CI_A to CI_C, we will have to assess the conditional probability (likelihood) $L_{C,A}$ and take into account all the potential societal impacts due to the following paths:

(a) $CI_A \rightarrow CI_B \rightarrow CI_C$: $R_{C,B,A} = f(R_{B,A}, R_{C,B})$ (second-order dependency risk) and

(b) $CI_A \rightarrow CI_C$: $R_{C,A}$ (first-order dependency risk)

The next step will be to evaluate these risks and examine which is the most cost-efficient way to mitigate them. Both paths of dependency need to be examined. Countermeasures options would be (a). the use of alternative power supply for CI_C (reduce the probability $L_{C,A}$), (b). countermeasures for load management during crisis (reduce the probability $L_{C,B}$ or increase the resilience of infrastructure CI_C).

4 Related Work

Interdependency models and approaches found in the literature vary according to the level of analysis selected. Some adopt a microscopic and some a macroscopic view of dependencies. One approach [10] focuses on CI components (microscopic view), and demonstrates several types of multi-dependency structures for both linear and particularly cyclical dependencies among multiple infrastructure types. It also considers un-buffered and buffered types of resources. Another approach [11] focuses on the component level, as well, and models/simulates two types of vulnerability: (a). structural and (b). functional. It calculates the interdependent effect and the effect of interdependence strength. It includes examples on power grid and gas pipeline models. Other models examine dependencies between different CIs [12] or within the same or different sectors of a country [13]. A method to map interdependencies, with a workflow enabling the characterization of coupled networks and the emerging effects related to their level of interdependency, is presented by [14]. This work aims at mapping the interdependency between electrical and related communication nodes.

Several methods that are proposed for evaluating risk in interdependent CIs apply Leontief's Inoperability Input-Output model (IIM), which calculates economic loss due to unavailability on different CI sectors based on their interdependencies [6, 13, 15–17].

Theoharidou et al. assess risk in three layers: (a). infrastructure level, (b). sector level, and (c). national/intra-sector level [5, 7, 8]. The authors identify first-order dependencies and provide a method for evaluating societal risk between CIs and sectors. A similar approach is adopted on [18]. It follows six steps: (1). Identify the initiating event, (2). Identify interdependencies and Perform qualitative analysis, (3). Perform semi-quantitative assessment of the scenario, (4). Perform detailed quantitative analysis of interdependencies (optional), (5). Evaluate risk and measures to reduce interdependencies, and (6). Perform Cost/benefit analysis (optional).

5 Conclusions

In this paper we examine the possible cumulative effects of a single security incident on multiple CIs. Such paths of dependent CIs add complexity and are usually out of the scope of typical risk assessment methodologies. Our method provides a way to identify threats that may appear insignificant when examining only first-order dependencies, but may have potentially significant impact if one adopts a more macroscopic view and assesses multi-order dependencies.

Based on previous work, we utilize existing first-order dependency graphs, in order to assess the effect of a disruption to consequent infrastructures. This approach utilizes existing risk assessments that refer to the societal risk of first-order interdependencies (performed at a sector level). Also, the assessment of impact is not expressed only on economic terms, like most IIM approaches. Finally, it is scalable to n-order dependency assessments.

The current approach does not analyze the graphs fully, so it does not evaluate possible cycles or reverse interdependencies. Also, it does not consider parallel paths in an automated way, as well as their potential effect to minimize risk. Future steps will include the adoption of graph analysis algorithms, in order to identify the most critical paths of dependencies, and to provide ways to reduce risks by adopting alternative paths in a graph. In order to validate our method, we also plan to apply the model in a real scenario which will analyze interdependencies between transport, ICT and energy infrastructures.

Acknowledgments. This work was supported in part by the S-Port (09SYN-72-650) project, which is funded by the Hellenic General Secretariat for Research & Technology, under the *Synergasia* Programme.

References

1. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine 21(6), 11–25 (2001)
2. Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., Martins, N., Paserba, J., Pourbeik, P., Sanchez-Gasca, J., Schulz, R., Stankovic, A., Taylor, C., Vittal, V.: Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance. IEEE Trans. on Power Systems 20(4), 1922–1928 (2005)
3. Barrett, C., Beckman, R., Channakeshava, K., Huang, F., Kumar, V., Marathe, A., Marathe, M., Pei, G.: Cascading failures in multiple infrastructures: From transportation to communication network. In: 5th Int. Conf. on Critical Infrastructure (CRIS), pp. 1–8 (2010)
4. De Porcellinis, S., Oliva, G., Panzieri, S., Setola, R.: A Holistic-Reductionistic Approach for Modeling Interdependencies. In: Palmer, C., Shenoi, S. (eds.) Critical Infrastructure Protection III. IFIP AICT, vol. 311, pp. 215–227. Springer, Heidelberg (2009)
5. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk-based criticality analysis. In: Palmer, C., Shenoi, S. (eds.) Critical Infrastructure Protection III. IFIP AICT, vol. 311, pp. 35–49. Springer, Heidelberg (2009)
6. Setola, R., De Porcellinis, S., Sforna, M.: Critical infrastructure dependency assessment using the input-output inoperability model. Int. J. Critical Infrastructure Protection 2(4), 170–178 (2009)
7. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: A multi-layer criticality assessment methodology based on interdependencies. Computers & Security 29(6), 643–658 (2010)
8. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk Assessment Methodology for Interdependent Critical Infrastructures. Int. J. Risk Assessment & Management (2011) (to appear)
9. Rinaldi, S.: Modeling and simulating critical infrastructures and their interdependencies. In: 37th Hawaii Int. Conf. on System Sciences, USA, vol. 2. IEEE (2004)
10. Svedsen, N., Wolthunsen, S.: Connectivity models of interdependency in mixed-type critical infrastructure networks. Information Security Technical Report, vol. 1, pp. 44–55 (2007)

11. Min, O., Liu, H., Zi-Jun, M., Ming-Hui, Y., Fei, Q.: A methodological approach to analyze vulnerability of interdependent infrastructures. Simulation Modeling Practice and Theory 17, 817–828 (2009)
12. Nieuwenhuijs, A., Luiijf, E., Klaver, M.: Modeling dependencies in critical infrastructures. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection II. IFIP, vol. 290, pp. 205–214. Springer, Boston (2008)
13. Aung, Z.Z., Watanabe, K.: A framework for modeling Interdependencies in Japan's Critical Infrastructures. In: Palmer, C., Shenoi, S. (eds.) Critical Infrastructure Protection III. IFIP AICT, vol. 311, pp. 243–257. Springer, Heidelberg (2009)
14. Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., De Porcellinis, S., Setola, S.: Modeling interdependent infrastructures using interacting dynamical models. Int. J. Critical Infrastructures 4(1/2), 63–79 (2008)
15. Santos, J., Haimes, Y.: Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures. Risk Analysis 24(6), 1437–1451 (2004)
16. Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian, C., Yan, Z.: Risk Analysis in Interdependent Infrastructures. Critical Infrastructure Protection 253, 297–310 (2007)
17. Crowther, K.: Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model. Int. J. Critical Infrastructure Protection 1, 53–67 (2008)
18. Utne, I.B., Hokstad, P., Vatn, J.: A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety 96(6), 671–678 (2011); ESREL 2009 Special Issue