Securing Transportation-Critical Infrastructures: Trends and Perspectives

Marianthi Theoharidou, Miltiadis Kandias, and Dimitris Gritzalis

Information Security and Critical Infrastructure Protection Research Laboratory
Dept. of Informatics, Athens University of Economics and Business
76 Patission Ave., Athens, GR-10434, Greece
{mtheohar,kandiasm,dgrit}@aueb.gr

Abstract. Critical infrastructure Protection (CIP) includes ensuring the resilience of transportation infrastructures. This sector is considered vital worldwide due to its economic importance and due to the various interdependencies with other infrastructures and sectors. This paper aims at examining the current state in national policies and in research regarding the protection of transport infrastructures. It examines methods to model interdependencies and to assess risk suitable for transport CIP. It recommends future steps for research in this sector.

Keywords: Critical Infrastructure, Transport, Interdependencies, Risk.

1 Introduction

Transportation is a key economic sector; it facilitates the movement of people, food, water, medicines, fuel, and other commodities. It faces multiple threats, ranging from accidents, failures or human errors to malevolent actions, namely sabotage, insider threats or terrorist attacks. Examples of the latter are the events in New York and Washington (2001), Madrid (2004), and London (2005). The common element of these incidents is the use of components of the transport infrastructure [1]. In several cases, transportation components were used as the main means for the attack; in other cases, they were used as the target, which included cyber attacks, too. Potential threats include the disruption of a mega-node in the transportation network, the use of a transport component as an attack method and the release of a biological agent at a major passenger facility (rail station, ferry terminal, hub airport) [2]. The increasing need of protecting transport infrastructures is recognized by most countries; all of them name the transportation sector among their critical sectors [1]. Assessing risk in critical infrastructures requires a different approach than in traditional information systems, mainly due to high complexity, multiple interdependencies, and the need for managing an heterogeneous infrastructure network [3].

Critical Infrastructures (CI) refer to an ‘asset, system or part, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact as a result of the failure to maintain

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 171–178, 2012.

those functions' [4]. Transport CIs fall into six main categories [2]: *Aviation*, *Maritime*, *Mass Transit*, *Highway*, *Freight Rail*, and *Pipeline*. Each type has its own characteristics, operates independently within both regulated and non-regulated environments, and yet is highly interdependent to other CIs.

In this paper, we examine the current state, regarding transport Critical Infrastructure Protection (CIP). In Section 2, we first review national initiatives and policies, regarding the assessment of transport risk. In Section 3, we identify interdependency types, and we review the literature regarding modeling and assessing interdependencies between transport infrastructures. Finally, we present conclusions and indicate future research steps.

2 National Initiatives and Policies

In order to examine the state of CIP in the Transportation sector, we first have to look into national and international strategic plans and guidelines. The US Transportation Security Administration is responsible for the sector-specific protection plan regarding transportation security [2]. It describes a generic systems-based risk management approach. The main goal of the method is to counter terrorism, enhance resilience, and facilitate the cost-effective security for transportation. It offers explicit guidelines on identification of assets, systems, networks and functions, risk assessment, development, and implementation of security programs, coupled with suggestions on security evaluation. The proposed method, under the prism of physical, human and cyber factors, defines six phases: (a) setting security goals, (b) identification of assets, systems, networks and functions, (c) risk assessment, (d) prioritization, (e) implementation of protective programs, and (f) measurement of effectiveness.

The US Government Accountability Office (GAO) conducted an assessment of transportation security [5],[6]. In general, GAO attempts to spot weak points in method and implementation and propose appropriate improvements. Their findings are quite interesting when compared to the actual plan of the DHS, especially to those who are interested in developing, implementing or evaluating a risk assessment method that deals with transportation. Regarding the security of the rail system, GAO has published an assessment of the actions taken by TSA to enhance mass transit and rail security [5].

Sandia National Laboratories also conduct research on transportation of hazardous material. The field of interest is safety of nuclear weapons stockpiling, energy and infrastructure assurance, nonproliferation of weapons of mass destruction, and enhancing the safety of CIs. They have developed RADTRAN [7],[8], an ad hoc international standard for transportation risk assessment for radioactive materials. RADTRAN combines parameters, such as user-determined demographic, routing, transportation, packaging, and other intelligence such as materials, meteorological, and health physics data, in order to calculate expected radiological consequences of incident-free radioactive materials transportation and associated accident risks. An implementation of the method is provided

(RADCAT[1]); it focuses on highway and rail transportation of radioactive material and on accident dose risk due to radiation exposure.

The Transportation Risk Assessment Working Group's handbook [9] aims to increase the efficiency and effectiveness of transportation risk assessments prepared pursuant to the National Environmental Policy Act (NEPA). Chronologically, it is the first attempt to propose a method to assess the risk of radioactive material transportation. The quantitative base of the method is RADTRAN [7],[8] and RISKIND [10], which contribute in computing cargo and vehicle related risk. The method specializes on accident risk and consequence risk.

In Europe, the Polish 'Management of Health and Environmental Hazards' (MANHAZ) Center focuses on the protection of human health, welfare and environment. It has published a quantitative transportation risk assessment method, which deals mainly with road and rail transportation of hazardous substances [11]. The proposed approach includes the assessment of transportation risk and environmental and land use safety factors, capability of the existing network and cumulative traffic implications, economic distribution considerations and operators' requirements for practical economics.

UK's Department of Transport has published guidance on how to implement a transportation assessment [12]. It includes general guidelines and useful tables to support the process of assessment, mainly in the urban environment. Although a specific method is not proposed therein, advice, suggestions, and guidelines over transportation assessment are provided. Similar guides on transportation assessment are also followed in Scotland [13] and in Northern Ireland [14].

Except for general directives on CIP [4], the European Commission is active in the area of transportation security and safety research. The Research and Innovation in Transportation Committee[2] funds research programs for aeronautics, rail, water, road, and multimodal transportation, though no official method or standard was found published. The STARTRANS[3] project aims to develop a comprehensive Transportation Security Risk Assessment Framework in interconnected, interdependent and heterogeneous transport networks. Also the Safety@Sea[4] project specializes in maritime transportation security. It deals mainly with risk assessment and management, coastal management and routing and safe seaways assurance in the North Sea, as well as with creating a maritime rescue coordination center in order to increase safety awareness.

Based on the above, it appears that only the US policy suggests a specific method on transportation CIs. The resulting method is system-based and calculates the risk as the function of threat, vulnerability, and impact. A lot of research focuses on material transportation [9],[11] and, in particular, radioactive [7],[8]. Most governments have adopted appropriate plans to strengthen both security and safety of transportation, with a strong emphasis on accidents, in particular when these affect people and the environment. It also appears that

[1] http://radtran.sandia.gov/

[2] http://ec.europa.eu/research/transport/

[3] http://www.startrans-project.eu/

[4] http://www.safetyatsea.se/

the regulations remain domain-based, even within the transport sector, and do not reflect the dependencies between transport CIs or to other sectors.

3 Interdependencies and Cascading Failures

One of the main characteristics of CIs in general is the multiplicity of interdependencies between them and their respective sectors. This is vital when one refers to transport CIs, as they are prerequisite for various other CIs [2]. For example, the Energy Sector relies on coal, crude oil, petroleum products, and natural gas to be transported by ship, barge, pipeline, rail, or truck. The Banking and Finance and the Government Sectors also rely on mass transit systems in large urban areas for employees to access the workplace. The ICT Sector co-locates much of its networking equipment (routers, fiber optic cable, etc.) along existing transportation routes (rail lines, highway tunnels, and bridges), the destruction of which may impact service availability in wide geographic areas. On the other hand, the Transport sector relies on the Energy Sector for fuel [15], or on the ICT Sector for the transmission of information necessary for the efficient operation of the transportation network. Beyond these obvious examples, cascading effects may also occur, due to changes in individual behavior during a crisis, like the work of [16], which studies the effect of a failure in Transportation sector and how it affects various wireless networks (ICT Sector).

3.1 Types of Dependencies and Disruptions

Dependencies [15],[17] can be: (1) *Physical* (a CI depends upon the output(s) of the other CI), (2) *Cyber/Informational* (a CI depends on information transmitted through the other CI), (3) *Geographic* (a CI depends on an environmental event on another CI), (4) *Logical* (a CI depends upon another CI via a non-physical, cyber, or geographic connection) and (5) *Social* (a CI is affected by the spreading of disorder to another CI related to human activities).

Interdependencies may fall into these non-mutually exclusive types, but one should not assume the complete availability or unavailability of a CI, as these may be available on different levels of quality [18]. Examples of quality degradation may include *quantity* (of power), *speed* (of transport or communication services), *reliability* (of information), *pressure* (of gas), *purity* (of water), etc. Also, multiple factors should be taken into consideration, such as state operations, social influence, political consequences and technological implications.

Rinaldi et al. classify interdependence-related disruptions or outages as *cascading*, *escalating*, or *common cause* [15]. A cascading failure occurs when a disruption in one CI causes the failure of a component and a subsequent disruption on a second CI. An escalating failure occurs when an existing disruption in one CI exacerbates an independent disruption of a second CI, generally 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 CIs are disrupted at the same time: components within each CI fail because of a common cause.

3.2 Review of Dependency Risk Assessment

Generic risk assessment methods for CIs have been initially reviewed in [3]. The main observation is that such approaches assess risk in terms of threat, vulnerability and impact, with a high emphasis on the societal impact of a CI failure or disruption. However, they fail to model and assess the risk caused by interdependencies, which have been proven crucial in transport CIP in the past [1]. Any modeling and simulation attempt faces several challenges, namely data accessibility, model development, and model validation. In the case of CI interdependency, such a task is further complicated by the detailed and disparate cross sector analysis which is required [19]. The lack of reliable real-time data makes the identification of interdependency related failures even worse [20].

Related work in identifying and modeling dependencies includes the use of sector-specific methods, e.g. gas lines, electric grid or ICT, or more general methods that are applicable in various types of CIs. Interdependency models fall into six broad categories: (a) Aggregate Supply and Demand Tools, (b) Dynamic Simulations, (c) Agent-Based Models, (d) Physics-Based Models, (e) Population Mobility Models and (f) Leontief Input-Output Models [21].

Dependencies also vary according to the level of analysis selected. Different aproaches have been used to examine dependencies under a microscopic or macroscopic view. One approach [22] 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 unbuffered and buffered types of resources. Another approach [23] 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 [18], within the same or different sectors of a country [24]. 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 [25]. 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 [24],[26],[27],[28]. The same model is also applied by [29], so as to include elements of business continuity and the cost to recover from an event.

Theoharidou et al. assess risk in three layers: (a) infrastructure level, (b) sector level, and (c) national/intra-sector level [3],[30],[31]. They identify first-order dependencies and provide a method for evaluating societal risk between CIs and sectors. These interdependencies can form risk graphs in order to identify multiple order interdependencies and assess risk on chained events. A similar approach is adopted on [32]. 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).

Approaches for assessing dependencies and risk in transport CIs can be also found; they follow similar approaches as the above. For example, [33] uses a Petri Net analysis procedure to estimate indirect losses in networks of critical transport infrastructures. The rest of the literature focuses on the risk assessment of hazardous materials (i.e. [7],[8],[9],[11],[34]).

4 Conclusions

In this paper we reviewed the current state-of-the-art in transportation CIP. One of the main characteristics of this sector is the multiple types of infrastructures within itself. These types vary both technologically and in terms of regulation, standards, and best practices. They also face different kinds of threats and vulnerabilities. Applying a universal method for these infrastructures should take into account multiple characteristics and should be combined with existing specific methods, which mainly focus on accidents and environmental security. Cross-sectoral regulation and standardization is particularly difficult, as it can only be initiated by international or national organizations and bodies.

Current approaches usually focus on a specific subsector and fail to assess the risk introduced by interdependencies. There are several recent approaches focusing on assessing risk of interdependencies, but they only focus on specific and isolated parts of the problem. Identifying and mapping societal interdependencies or identifying potential cascading effects is a really challenging aspect in terms of discovery, mapping, and validation of dependencies [19]. This requires cross-sector and cross-border collaboration.

The static nature of risk assessment models is another issue; models serve as a snapshot of a transport CI. Transport CIs are dynamic systems, a parameter which is reflected on risk as well. Most approaches also fail to connect the risk assessement process to spatial information [34]. Novel approaches for dynamic, real-time risk assessment could contribute significantly towards such a direction.

Since transport CIs are vast networks, they also share a significant -in number and variable- user-base. In highly critical systems, this factor introduces threats, thus assessing risk on a per-user basis could contribute significantly in mitigating the really important insider threat. Such a variable and vast user-base can be also used during the risk assessment process. Using collaborative technologies, in order to ensure more accurate and detailed data collection, could also be a promising future research step.

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. Brunner, E., Suter, M.: International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies. Center for Security Studies, ETH Zurich, Switzerland (2008)
2. Transportation Security Administration: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan. Dept. of Homeland Security, USA (2007)
3. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk-based criticality analysis. In: Palmer, C., Shenoi, S. (eds.) 3rd IFIP Int. Conf. on Critical Infrastructure Protection (CIP 2009), pp. 35–49. Springer, USA (2009)
4. European Council: Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal L345, pp. 75–82 (2008)
5. Government Accountability Office: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs. Committee on Homeland Security, USA (2009)
6. Government Accountability Office: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation. Committee on Homeland Security, USA (2009)
7. Neuhauser, K., Kanipe, F.: RADTRAN 5, User Guide. SAND2000-1257, Sandia National Laboratories, USA (2000)
8. Neuhauser, K., Kanipe, F.: RADTRAN 5, Technical Manual. SAND2000-1256, Sandia National Laboratories, USA (2000)
9. U.S. Department of Energy, Resource Handbook on DOE Transportation Risk Assessment. Report DOE/EM/NTP/HB-01, National Transportation Program, Office of Environmental Management, USA (2002)
10. Yuan, Y., Chen, S., LePoire, D., Rothman, R.: RISKIND-A Computer Program for Calculating Radiological Consequences and Health Risks from Transportation of Spent Nuclear Fuel. Energy Science and Technology Software Center, USA (1993)
11. Borysiewicz, M.: Transportation Risk Assessment. Report IAE B-54/2006, Institute of Atomic Energy, Poland (2006)
12. Department of Transport: Guidance on Transport Assessment, UK (2007)
13. Scottish Executive: Transport Assessment and Implementation: A Guide, UK (2005)
14. Department for Regional Development: Transport Assessment: Guidelines for Development Proposals in Northern Ireland, UK (2006)
15. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine 21(6), 11–25 (2001)
16. 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)
17. De Porcellinis, S., Oliva, G., Panzieri, S., Setola, R.: A Holistic-Reductionistic Approach for Modeling Interdependencies. In: Palmer, C., Shenoi, S. (eds.) 3rd IFIP Int. Conf. on Critical Infrastructure Protection (CIP 2009), pp. 215–227. Springer, USA (2009)
18. Nieuwenhuijs, A., Luiijf, E., Klaver, M.: Modeling dependencies in critical infrastructures. In: Goetz, E., Shenoi, S. (eds.) Critical Infrastructure Protection. IFIP, vol. 253, pp. 205–214 (2008)

19. Pedersona, P., Dudenhoeffer, D., Hartley, S., Permann, M.: Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research. INL/EXT-06-11464, Idaho National Laboratory, USA (2006)
20. 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)
21. Rinaldi, S.: Modeling and simulating critical infrastructures and their interdependencies. In: 37th Hawaii Int. Conf. on System Sciences, vol. 2. IEEE, USA (2004)
22. Svedsen, N., Wolthunsen, S.: Connectivity models of interdependency in mixed-type critical infrastructure networks. Information Security Technical Report 1, 44–55 (2007)
23. 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)
24. Aung, Z., Watanabe, K.: A framework for modeling Interdependencies in Japan's Critical Infrastructures. In: Palmer, C., Shenoi, S. (eds.) 3rd IFIP Int. Conf. on Critical Infrastructure Protection (CIP 2009), pp. 243–257. Springer, USA (2009)
25. 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)
26. Santos, J., Haimes, Y.: Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures. Risk Analysis 24(6), 1437–1451 (2004)
27. Haimes, Y., Santos, J., Crowther, K., Henry, M., Lian, C., Yan, Z.: Risk Analysis in Interdependent Infrastructures. Critical Infrastructure Protection 253, 297–310 (2007)
28. 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)
29. 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)
30. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: A multi-layer criticality assessment methodology based on interdependencies. Computers & Security 29(6), 643–658 (2010)
31. Theoharidou, M., Kotzanikolaou, P., Gritzalis, D.: Risk Assessment Methodology for Interdependent Critical Infrastructures. International Journal of Risk Assessment and Management (Special Issue on Risk Analysis of Critical Infrastructures) 15(2/3), 159–177 (2011)
32. 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
33. Di Febbraro, A., Sacco, N.: A Petri Nets approach for the interdependence analysis of Critical Infrastructures in transportation networks. In: 12th World Conference on Transport Research, Portugal (2010)
34. Gheorghe, A., Birchmeier, J., Vamanub, D., Papazoglou, I., Kroge, W.: Comprehensive risk assessment for rail transportation of dangerous goods: a validated platform for decision support. Reliability Engineering & System Safety 88, 247–272 (2005)