DRAFT

Report #04-005

DECISION-MAKING AND THE VULNERABILITY OF INTERDEPENDENT CRITICAL INFRASTRUCTURE

Zimmerman, R.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

October 10, 2004

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California
Los Angeles, California

3710 McClintock Avenue, RTH 314 Los Angeles, CA 90089-2902 ~ (213) 740-5514 ~ www.usc.edu/create

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the U.S. Department of Homeland Security.

Decision-making and the Vulnerability of Interdependent Critical Infrastructure[1]

Rae Zimmerman
Professor of Planning and Public Administration
and Director, Institute for Civil Infrastructure Systems (ICIS) (www.nyu.edu/icis)
Robert F. Wagner Graduate School of Public Service
New York University
295 Lafayette Street
New York, NY 10012
USA
rae.zimmerman@nyu.edu

Abstract-*Interdependencies among critical infrastructure systems are well-recognized as key points of vulnerability that can compromise system performance especially during extreme events. At the heart of these vulnerabilities are decisions, often unnoticed and indirect, which occur anywhere from infrastructure planning, siting and design through operation and maintenance. The key contributions of the paper are (i) the presentation of a method for constructing a catalog of infrastructure interdependencies, (ii) the construction of a set of indicators transferable to other databases, and (iii) preliminary analytical results of the application of the indicators to a sample database of catalogued events with interdependencies. This paper addresses how case analysis findings can be used in decision making to promote non-adverse interdependency-related outcomes from extreme events. Critical infrastructure analyzed includes facilities and services for transportation, telecommunications, water supply, wastewater, electric power and other energy infrastructure. Event databases for this research include government, industry, academic and media reports.*

Keywords: Infrastructure interdependencies, extreme events, vulnerability assessment

1 Introduction

The provision of infrastructure services is dominated by infrastructure networks spanning long distances combined with increasingly centralized production nodes. This pattern of service delivery has largely arisen to support low-density development marked by two characteristics. The first is the increasing amounts of developed land per capita to the point where major metropolitan areas are consuming land at a rate that is several times the rate of population growth [1]. The second is the promotion of economies of scale based on direct costs of service provision.

Often accompanying this condition is a pattern of interconnected infrastructure systems regardless of the density of populations served. Two ways that different infrastructure sectors can be connected or interdependent are spatially or functionally [2]. Spatial dependency refers to the proximity of one infrastructure to another as the major relationship between the two systems. Functional dependency refers to a situation where one type of infrastructure is necessary for the operation of another, such as electricity being required to operate the pumps of a water treatment plant. Other typologies of interdependencies have been put forth; for example, Peerenboom, Fisher, and Whitfield suggested physical, cyber, geographic, and logical categories [3]. The two categories selected here (spatial and functional) encompass most of the elements of the Peerenboom, Fisher and Whitfield typology. Spatial is equivalent to the geographic category and functional combines physical, cyber and logical.

Infrastructure interdependencies are now recognized as both opportunities as well as points of vulnerability. A number of theoretical models exist to conceptualize characteristics of these interdependencies and their impacts [4]. Empirical work has been less common,

[1] This work is supported by National Science Foundation grants for the Institute for Civil Infrastructure Systems (ICIS) located at NYU (in partnership with Cornell University, Polytechnic University of NY and the University of Southern California) under Cooperative Agreement 9728805 the "Institute for Civil Infrastructure Systems" (PI: R. Zimmerman); Grant 0204660 "Urban Infrastructure in a Time of Crisis" (PI: R. Zimmerman); and Grant 0091482, "Bringing Information Technology to Infrastructure: A Workshop to Develop a Research Agenda from the National Science Foundation" (PI: R. Zimmerman). It was also supported in part by a grant from the U.S. Department of Homeland Security (through the U. of Southern California).

and anecdotal evidence tends to be used more commonly as the basis for describing and modeling the behavior of interdependent infrastructure. As a result of the absence of more empirically based data, highly valued theoretical approaches remain untested against real circumstances that reflect infrastructure condition, policies regarding interdependencies, and other factors.

To begin to provide such an empirical approach, a search was conducted for infrastructure failures in the United States drawn from published event accounts. These accounts were coded to form a database of event structures, then analyzed for infrastructure interdependencies.

The purpose was not only to begin to build a database of these events, but also to conduct some preliminary analyses of the data by developing and applying diagnostic tools to it and developing indicators in order to identify and portray the prevalence of certain combinations of failures. Knowledge of these patterns provides an important basis for evaluating and improving decisions to reduce and otherwise manage these vulnerabilities. Decision makers require a means of organizing information on failures, focusing on key points of vulnerability in order to prioritize decisions anywhere from planning, siting and design to operation and maintenance.

2 Prevalence and impact of interdependencies

2.1 Prevalence of interdependencies

Numerous examples exist of spatial and functional interdependencies that support and provide a foundation for a more rigorous analysis.

Spatial Interdependencies - Colocation: Utility lines are often co-located with transportation arteries, such as roads, bridges, and rail lines. In Paris, France, bridges are conveyances for water lines. In one of the drought years in the northeastern United States, the George Washington Bridge linking New York (NY) and New Jersey (NJ) was used for a water supply pipe to potentially provide water from NY to NJ. Unused water pipes were considered as potential routes for fiber-optic cable in New York City (NYC). In each of these cases, infrastructure facilities were located together, but did not otherwise depend upon one another mechanically or electronically to function.

Functional Interdependencies: Functional interdependencies, where one infrastructure relies on another to operate, are increasing in some areas. One area where this is occurring is in the use of information technologies for operational control of infrastructures. The fact that this is very common is not surprising given the rapid growth of information technologies in the economy. These interdependencies are likely to increase as information technologies become more sophisticated [5]. Transit systems, for example, are relying to a greater extent on information technologies for the operation of trains. Trains run by the Bay Area Rapid Transit (BART) system in California and the Washington DC Metro are operated by computer. The Air Train to JFK airport in the NY region has been planned to be computer operated [6], and the Metropolitan Transportation Authority (MTA) is also planning to computerize the operation of its subway trains [7]. Security needs of infrastructure are contributing to the expansion in the use of information technologies, since security technologies tend to rely heavily upon sensors and computer-based data analysis.

Functional interdependencies between electric power and other infrastructures are also increasing. For example, water and wastewater treatment systems rely heavily on electric power; the operation of chemical processes and mechanical equipment account for the greatest sources of power consumption within water systems. Water treatment systems are estimated to consume about 3% of U.S. energy resources, and these loads are expected to increase by 20% by about the year 2020 [8]. These trends are in part due to the increasing stringency of water treatment requirements.

2.2 Unanticipated impacts of interdependencies

Given the prevalence of such interdependencies, is there sufficient reason to believe that they create negative impacts? These interdependencies are raising important issues for urban areas regardless of urban size and density. Some examples are provided below that will be the basis for the analysis that follows.

The patterns that have been emerging with respect to functional interdependencies between electric power and other infrastructures can contribute to the vulnerability of other infrastructures. For example, according to Payne's account of the electric power substations of the NYC subway system, in 1959 the independent substations were sold to the local electric power utility; since that time the subways have been more vulnerable to power outages whenever the electric power system is disrupted [9].

Failures of information technologies, whether communications or computing that initiate failures of infrastructures dependent on cyber systems, are often catastrophic. In the case of the Intercity Express (ICE) high speed rail crash of June 2, 1998 in Germany, communication disruptions prevented a train engineer from knowing that the rest of the train had derailed. Without this information, he was probably unable to avoid additional damage. Failures of some software systems are now known to have been one of the contributors to the blackout of August 14, 2003 in the United States and Canada [10]. Computer and communication system failures have also been a source of outages at airports, ranging from disruptions of fiber optic cable to computer systems going down that support flight and ticketing information.

3 Deriving interdependency structures through case analysis

3.1 Approach

In order to address the question of whether certain combinations of infrastructure failures are more common than others, case histories of utility failures were used to create a database of the components that failed and the sequence of failures. These databases included the web sites of construction accidents, reports of the National Transportation Safety Board, and news media searches. Since there is generally no systematic reporting of coverage of cases across all infrastructure areas, the selection of data sources was opportunistic, which served the purposes of this work to develop analytical methods. Rather than producing definitive failure sequences, the database was used to illustrate a method to systematically identify and characterize failures, especially those that occur as a result of interdependencies among two or more different kinds of infrastructure. Interdependencies among components were the particular focus of the failure analysis, that is, where a failure of one type of infrastructure led to the failure of another. The type of failure could be a cascading failure or common cause failure [11].

Several simple indicators were used to characterize the data:

- The types of infrastructure that more frequently damaged other infrastructure
- The types of infrastructure more commonly affected by or damaged by failures in other infrastructure
- The ratio of being a cause of failure to being affected by failure
- Combinations of failures that were most frequent
- The number of people affected and how they are affected

3.2 Database characteristics

The database, only used to illustrate how one can conceptualize interdependencies, was not randomly selected, and thus, the findings are intended for use in developing analytical approaches to the problem rather than being generalizable in their own right.

The types of infrastructure encompassed by the data set are listed below. These were derived from traditional areas that define infrastructure and from those covered in the data set itself, though some categorizations of infrastructure, particularly critical infrastructure, include other categories, such as banking and finance and emergency services [12].

Airports
Cable
Cell Towers
Electric Lines
Fiber Optic/Telephone
Gas Lines
Oil Pipelines
Sewer/sewage treatment
Street Lights
Transit
Transportation-bridges
Transportation-rail
Transportation-roadways
Transportation-tankers
Wastewater
Water mains

In this particular database, events were drawn primarily from accidents that occurred in connection with failures during construction, maintenance or operation, or due to facility condition related to age of structures. The database includes events from 1990 through 2004. Such events also occur as a consequence of direct or indirect terrorist attacks [13, 14] or natural hazards; further development of the database will include these cases. The method of distributing events is illustrated below in connection with the discussion of the results in Table 1.

The events in the database were approximately equally divided between those involving one event per incident, that is, the failure of one component, and those involving two to six types of events per incident.

3.3 Results

The database was used to illustrate several ways of quantifying failures due to interdependence. Each failure was broken down into types of infrastructure involved or affected. Some of the results of applying the indicators listed above to the sample data are briefly described below:

1) *Infrastructure frequently the cause of failure to other infrastructure* (column 2 in Table 1). Water mains, roads, and gas line infrastructures (in that order) were most often the cause of damage to other infrastructure, accounting for approximately two thirds of the failures to other infrastructure in this database.

2) *Infrastructure frequently affected by other infrastructure failures* (column 3 in Table 1). Gas lines, roads, electric power and fiber optic cable (in that order) were most often affected by other infrastructure failure - about eighty percent of the affected infrastructure.

3) *Ratio of being a cause of failure relative to being affected by failure: Effect Ratio* (column 4 in Table 1). For the top six types of infrastructure involved in most of the failures, ratios were developed to reflect the extent to which a particular type of infrastructure initiated or caused a failure of another type of infrastructure vs. being affected by the failure of another type of infrastructure.

The results are shown in Table 1 for a subset of the data reflecting the six types of infrastructure that accounted for the highest number of failures of other infrastructure types.

Table 1. Effect Ratios

1 Type of Infrastructure	2 # of Times Infrastructure (Column 1) Caused Failure of Other Infrastructure	3 # of Times Infrastructure (Column 1) was Affected by Other Infrastructure Failures	4 Ratio of Causing vs. Affected by Failure (Col. 2 divided by Col.3)
Water mains	34	10	3.4
Roads	25	18	1.4
Gas lines	19	36	0.5
Electric Lines	12	14	0.9
Cyber/ Fiber Optic/ Telephone	8	15	0.5
Sewers/ sewage treatment	8	6	1.3

These illustrative results indicate that at least for this database, water mains are more frequent initiators of other infrastructure failures than the reverse. For roads and sewage facilities the direction is about equal. In contrast, gas lines and telecommunication lines are more likely to be damaged by other infrastructure than to initiate damage to other infrastructure. More important than these particular findings is the fact that a relatively simple indicator can portray the direction of vulnerabilities. Thus, decision-makers can use a framework such as this to identify where the major vulnerabilities in their systems are as a basis for prioritizing investments. The framework can obviously be refined to capture not only overall effects but details behind the effects, such as construction, design, operation or maintenance weaknesses.

4) *Common combinations of infrastructure interactions.* Certain types of infrastructure were frequently linked with one another, whether they caused or were affected by infrastructure failures. This database showed that the most likely combinations, in decreasing order of the number of events were: gas lines and roads (16), water and gas lines (12), electric and water lines (10), and electric and gas lines (7). This may simply be a function of how frequently these facilities are co-located, or alternatively, may reflect unintended interactions that occur when these facilities are subject to external stress.

5) *Most severe effects in terms of persons affected and how they are affected.* Perhaps the most significant indicator of infrastructure failures is how many people are affected and how. These attributes were also tabulated; however, conclusions are still pending since this information is not consistently reported. Data on population effects take the form of number of evacuations, number of people experiencing service interruptions, business closings, and property value effects. Other common indicators reflect severity also. One set of indicators based on epidemiology that is potentially valuable here is the mortality and morbidity rates or the percentage of people exposed who died or were sickened/injured respectively.

The case of the August 14, 2003 blackout in the United States and Canada [15] illustrates how infrastructure failure event components were coded from incidents, shown in Table 1, since the blackout reflects how a single incident can result in a large number of failure events. A key factor in the blackout was a cyber failure. The electric power failure was followed by shutdowns of water and wastewater treatment systems when pumps failed particularly in the mid-West and NYC, shutdown of transit lines dependent on electrified rail, and failure of street lights and other highway infrastructure. Many other kinds of impacts occurred as well that were unrelated or indirectly related to infrastructure failures, such as the inability of ATM machines, electronic hotel doors and electronically driven boat slips to function. The information from the blackout scenario would be coded in the following way. For causes, one entry would be made under the category cyber causing an electric power outage, one for electric power causing a sewage treatment outage, and another entry for electric power affecting transit and other transportation. To capture affected infrastructure, one entry would be made for sewers and sewage treatment being affected by electric power and another entry for transit and other transportation facilities being affected by electric power. Thus, if a given type of infrastructure caused a failure in another infrastructure system and was affected by a failure in another kind of infrastructure (in the case of electric power in the blackout incident) it would appear twice in Table 1 (once in column 2 and again in one or more rows in column 3).

Some caveats are in order. The database used to illustrate the use of these indicators may make the results very sensitive to other factors. Such factors include causes of the initial failure, the propensity for affected infrastructure to become seriously damaged, and the extent to which the database used is representative of the universe of combinations that actually exist. Thus, considerable attention needs to be paid to the set of events to which any indicator is applied to avoid drawing spurious conclusions.

4 Conclusions

It has been recognized for quite some time that interdependencies among diverse infrastructure systems have grown dramatically as a consequence of a highly networked society. Though these interdependencies create opportunities, they also create vulnerabilities. These vulnerabilities may produce adverse impacts that are becoming more frequent, longer-lasting, and more widespread, depending on the type of infrastructure, its condition, configuration, and many other characteristics.

In order to manage these systems, a systematic way of evaluating the prevalence of these interdependencies and the incidence of certain combinations that produce adverse effects is needed. Such approaches will support priority setting and inform ways of designing these systems relative to one another to avoid negative impacts. A number of indicators that reflect patterns in the set of interdependencies that have negative effects reveal some useful results with a preliminary, illustrative data set. One indicator, the ratio of the number of times a particular type

of infrastructure initiates damage to other infrastructure compared to the number of times it is affected by damages that other infrastructures impose, is a way to begin to provide such knowledge. This illustrative database shows that water main breaks are more frequently initiators of failure than the consequence of another infrastructure failure.

Tracing the sequence of actual failure events and using indicators of the frequency of combinations begins to provide a tool for decision-makers to combine such systems spatially or functionally in a manner that reduces vulnerability. To provide more useful knowledge to decision makers, this database needs to be expanded and made more representative of actual occurrences. In addition, important dimensions to be added as database characteristics include the attributes of certain infrastructures that initiated failures in other systems as well as what weaknesses in some infrastructure facilities made them more vulnerable to failures in other systems.

Acknowledgments

The author gratefully acknowledges the inputs of National Science Foundation scientists and the work of graduate research assistant, Nicole Dooskin, who assisted in the development of the database.

Disclaimer

Any opinions, findings, and conclusions or recommendations in this document are those of the author and do not necessarily reflect views of the National Science Foundation or the U.S. Department of Homeland Security which provided some of the funds for this research.

References

[1] U.S. EPA, *Development, Community and Environment - Our Built and Natural Environments*, Washington, DC: U.S. EPA, November 2000.

[2] R. Zimmerman, "Social Implications of Infrastructure Network Interactions," *Journal of Urban Technology*, Vol. 8, No. 3, pp. 97-119, 2001.

[3] J. Peerenboom, R. Fisher, and R. Whitfield, "Recovering from Disruptions of Interdependent Critical Infrastructures," prepared for CRIS/DRM/IIIT/NSF Workshop on "Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures" Lyceum, Alexandria, Virginia, September 10-11, 2001.

[4] S.M. Rinaldi, J.P. Peerenboom, and T.K.Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems* magazine, pp. 11-25, December 2001.

[5] R. Zimmerman and T.A. Horan, eds., *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, London, UK: Routledge, 2004.

[6] D. Diamond, "JFK AirTrain Tour of 7/13/02," *NYCRail.com*, 2002, Accessed 7 April 2004: http://www.nycrail.com/misc/airtrain.htm

[7] M. Luo, "The Next Stop for the Subway Is a Fully Automated Future," *New York Times*, p. B1, June 23, 2004.

[8] J. Joseph, "Energy Use in the Municipal Water/Wastewater Treatment Sector," Presentation at the New York Regional Energy Workshop, New York, NY: Columbia University, April 20, 2004.

[9] C. Payne, *New York's Forgotten Substations. The Power Behind the Subway*, New York, NY: Princeton Architectural Press, 2002.

[10] A. Jesdanun, "GE Energy acknowledges blackout bug," *The Associated Press*, Feb 12, 2004, http://www.securityfocus.com/news/8032. Accessed April 7, 2004.

[11] S.M. Rinaldi, J.P. Peerenboom, and T.K.Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems* magazine, pp. 11-25, December 2001.

[12] U.S. Executive Office of the President, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998.

[13] R. Zimmerman, "Public Infrastructure Service Flexibility for Response and Recovery in the September 11th, 2001 Attacks at the World Trade Center," in Natural Hazards Research & Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems, *Beyond September 11th: An Account of Post-Disaster Research*, Special Publication #39. Boulder, CO: University of Colorado, pp. 241-268, 2003.

[14] National Research Council, *Making the Nation Safer*, Washington, DC: National Academy Press, 2002.

[15] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14th 2003 Blackout in the United States and Canada: Causes and Recommendations*. The Task Force, April, 2004.