Columbia-Wharton/Penn Roundtable on
"Risk Management Strategies in an Uncertain World"
April 12-13, 2002
IBM Palisades Executive Conference Center
Palisades, New York

# Life-Cycle Infrastructure Risk Management : R&D Needs

(Thought Piece – Do Not Quote or Copy)

Miriam Heller, Ph.D.
Program Director, Civil Infrastructure and Information Systems
National Science Foundation, USA
Tel: +01.703.292.8360
Email: mheller@nsf.gov

**Summary:** Assessing and managing risk to our Civil Infrastructure Systems became a high profile matter as a result of the September 11, 2001 terrorist attacks. Mission-based, reactive agencies have had to focus a great deal of their efforts on recovery efforts and countering terrorism. Yet US Civil Infrastructure is equally and possibly more vulnerable to threats of natural, accidental and technological origin as well as to the slow but steady failures due to deterioration and neglect. This paper presents infrastructure risk management as a holistic framework defined by a range of intervention options from which an infrastructure asset portfolio could be envisioned. Some options aim to reduce the risks posed by these threats either through mitigation measures and improved design; others focus on correction, reactive risk management and response. A broad research question is how to allocate resources over this range of options, over various stages of development (R&D, development, implementation) and over time, especially accounting for the multi-objective, multi-stakeholder nature of the decisions. This will, among other things, entail quantifying the risks, both pre- and post-event, associated with the investment, which, given the low probability of some extreme events, i.e., overwhelming uncertainty, offers still more fertile areas for research.

## Background

Not too long after the Twin Towers of the World Trade Center (WTC) collapsed on September 11, 2001, the value—and the vulnerability—of US critical infrastructure skyrocketed in the public eye. *All eight infrastructures defined by Presidential Decision Directive #63 as critical were disrupted*. Live on TV, Americans watched the air transportation infrastructure itself destroyed and subverted to destroy another structure, which housed the single most concentrated seat of banking and finance infrastructure in the world, the state Department of Transportation offices, and myriad


Figure 1. Critical Infrastructures Defined in PDD 63.

telecommunications satellite dishes and relays perched on the Towers. Strewn plane debris and the progressive collapse of Twin Towers cascaded into disruption of the densest power grid system in the world while setting aflame fuel stored in Tower 7, the destruction of the Office of Emergency Management and the geographical data it house for responding to the city's emergency needs, the curtailment of telecommunications services headquartered in the adjacent Verizon building, flooding and crumbling of the Chamber Street subway station, broken water mains, and blockages of wastewater conveyance systems.

The urban disaster of September 11th, like natural, accidental, and technological disasters before, qualifies as an extreme event: an occurrence deemed rare in terms of frequency, impact, or both. The extremeness of these events tempts us to surrender control, abdicate our responsibility and acquiesce to "Acts of God and War." The reality of our scant experience, though, hints that there may be an underlying science to extreme events: patterns from which to learn to predict the event, respond more efficiently, or mitigate the impacts. If this were true, then not trying to learn from the events would render us irresponsible.

To exploit perishable data and maximize "Learning from Urban Disasters," the National Science Foundation's Civil and Mechanical Systems Division funded 10 quick response grants and 17 small travel awards through the Natural Hazards Research and Application Information Center, housed at the University of Colorado, Boulder. Four research areas capture the main questions of these researchers: 1) structural forensics and fire protection; 2) data acquisition and management; 3) critical infrastructure system services; and 4) emergency response. These areas and the more specific areas under investigation by the researchers define a full life-cycle of integrated risk management options that beg for resource allocation optimization both in terms of research and implementation.

Estimated costs for September 11th lie between $85-$100 billion. The magnitude of this figure and mass psychological impact of the event has refocused infrastructure policy toward short-term counter-terrorism measures. The single-minded diversion of effort and funds away from everyday, unintentional risks to infrastructure systems, which are of comparable staggering proportion, may prove to be another tragedy.

Natural disasters test the robustness and reliability of infrastructure design. Galaxy 4 satellite's failed attitude control system resulted in losses of $5.8 million over two days due to lost credit card sales, missed market trades, inability to contact doctors and emergency medical services, etc. Earthquakes take a much larger toll, averaging $4.4 billion per year[1]. Current traffic management systems lead to congestion of US roadways,

[1] Federal Emergency Management Agency. (1999). HAZUS®: Estimated Annualized Earthquake Losses for the United States, FEMA:Washington, DC.

estimated to cost $78 billion in idled away fuel and wasted time[2]. Power blackouts in the western US during July and August 1996 cost $1.5 billion[3], while power quality disturbances, such voltage sags and surges, cost primarily discrete manufacturing and electricity-dependent utilities over $119 billion annually[4]. Finally, neglecting infrastructure maintenance, already estimated to cost $1.3 trillion over the next 5 years, will likely only increase the risks[5].

**A Holistic Life-Cycle Framework for Infrastructure Risk Managment**

This suggests that terrorist risks must be addressed within the context of other extreme as well as everyday risks to infrastructure. Moreover, as recent investigations of the World Trade Center suggest, the condition of the infrastructure, i.e., how well it has been maintained, may contribute to the degree of damage resulting from an actualized threat as well as the probability of endogenous failures. For instance, the level and maintenance of fire protection appears to have contributed, if not caused, the progressive collapse of the World Trade Center[6]. In fact, other major changes imposed on our infrastructure systems, such as regulation, deregulation, globalization, devolution, deterioration or innovation, have the potential to exert stress on the system and thereby pose potential risk.

The range of risks suggests managing risk to infrastructure should be viewed from a full life-cycle perspective. This is consistent with the long-term, global perspective espoused by Mileti (1999)[7]. Investment in technologies associated with design, construction, operations, maintenance and retirement of physical infrastructure must be optimized over all threats, natural, technological, accidental, deliberate, as well as the slow creeping menace of deterioration. Mapped on to each of these life-cycle phases are risk reduction, analysis, and management methods from the social,

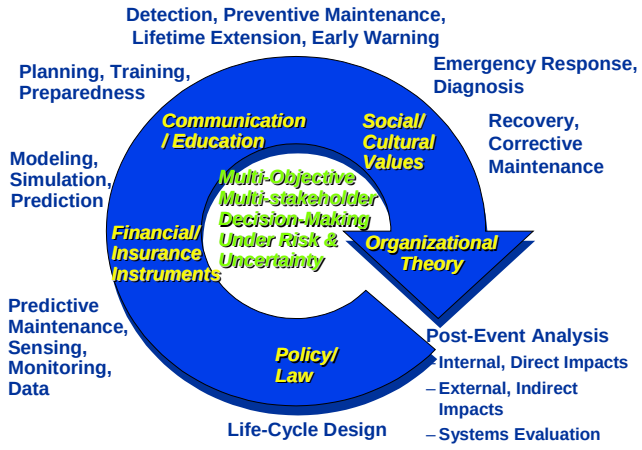


Figure 2. Holistic Risk-based Life-Cycle Infrastructure Engineering and Management

[2] Texas Transportation Institute. (2001). The 2001 Urban Mobility Study. Report for Texas Transportation Institute.
[3]Amin, M. (2001). Toward Self-Healing Energy Infrastructure Systems. IEEE Computer Applications in Power, January 2001, pg. 20-28.
[4]Lineweber.D. and S. McNulty. (2001). The Cost of Power Disturbances to Industrial and Digital Economy Companies, http://ceids.epri.com/ceids/Docs/outage_study.pdf
[5]American Society of Civil Engineers. (2001). The 2001 Report Card for America's Infrastructure, http://www.asce.org/reportcard.
[6] Glanz, J. and E. Lipton. (2002). Towers Withstood Impact, but Fell to Fire, Report Says. New York Times, March 29, 2002.
[7] Mileti, D. (1999). Disaster by Design, National Academy of Sciences: Washington, DC.

economic, human, and political domains. Figure 2 depicts this two level cycle, which is not intended to imply independent and linear decision points but rather the range of risk intervention options.

**Modeling, Simulating and Predicting Interdependent Infrastructure Systems**

Quite to the contrary, interdependencies abound among these risk intervention options. Budgetary constraints determine which interventions to invest in over different stages of development and over time. Investment in corrective actions likely depends on the level of deterioration and previous investments in maintenance. The effectiveness of an early warning system likely depends on the investment in sensing, monitoring, modeling, and prediction. Moreover, as the tragedy of 9/11 demonstrated, individual infrastructure systems are interconnected as well so that failures cascade from one subsystem to another and from one system system to next. Electricity outages curtail compressor stations in natural gas pipelines, which supply the very fuel they need and stop pumps at water and wastewater treatment plants. They disrupt traffic signals and transportation infrastructure. Water can neither be delivered by pipeline for irrigation and fire suppression nor by truck in bottles. Emergency crews cannot get to the sites where their services are needed. The telecommunications sector is halted without the electricity: no phones, jammed cell phone switches, no internet and no computing, no SCADA (supervisory control and data acquisition) nor control systems.

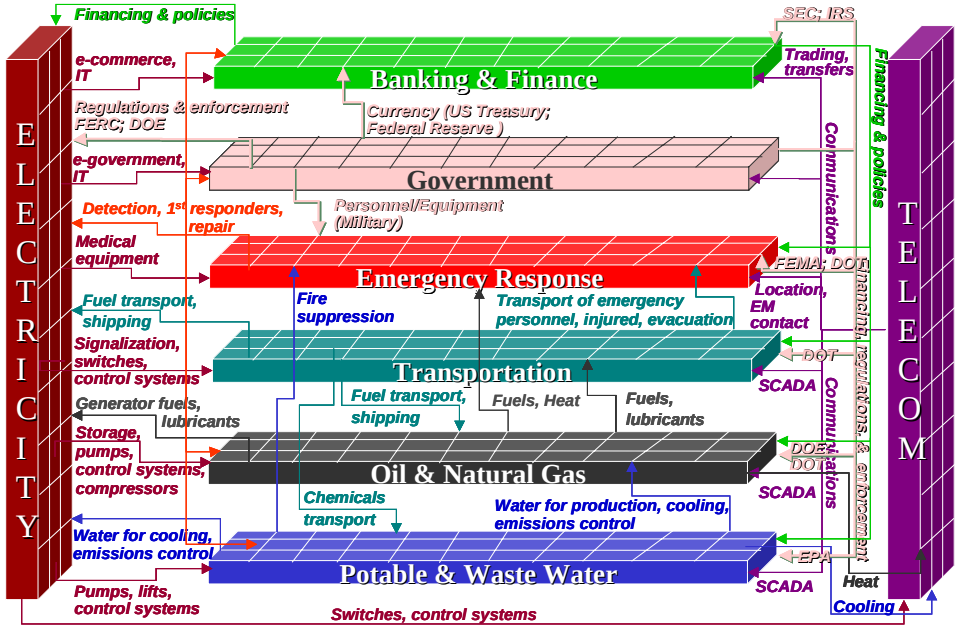


Figure 3. Interdependencies between the eight critical infrastructure

Infrastructure interdependencies add complexity to risk management that has yet to be addressed, primarily because the interdependencies have yet to be characterized and understood. Only a handful of researchers

have begun investigating infrastructure interdependences[8,9,10]. Understanding these interdependencies is crucial to assessing vulnerability, assuring preparedness, enabling recovery, and designing infrastructure to avoid negative interdependencies and exploit positive interdependencies.

Per Bak (1996) developed the theory of self-organizing criticality (SOC) and demonstrated its relationship with the power law relating the magnitude of the criticality and the frequency. Amin (1991)[11] reported that electricity disruptions exhibited similar behavior.

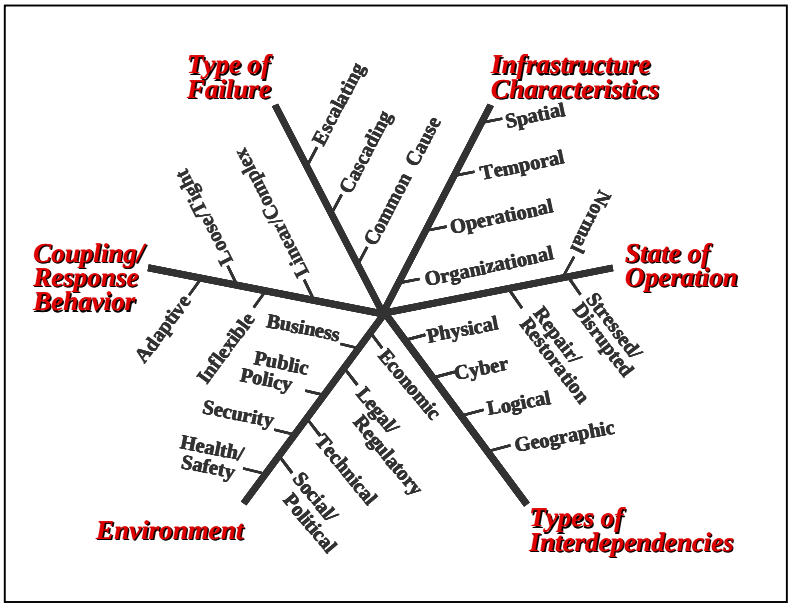


Figure 4. Framework of Infrastructure Interdependencies (Rinaldi et al., 2001)

SOC is exhibited in complex systems which exhibit system level emergent behavior not predictable by knowing lower level component behaviors. Many research opportunities exist to develop tools to model, simulate and predict complex systems, some of which are adaptive as well, i.e., the individual agents can adapt to the overall system. Theoretical frameworks for large-scale complex adaptive systems, CAS, must be defined to lay the theoretical underpinnings of this new area. Any model for CAS must take into account and enable modeling of non-linear coupled subsystems as well as system interdependencies, which are spatially distributed, and adaptive. Very real issues come into play in trying to define whether control is (or should be) centralized, decentralized, or distributed. The models had to account for multiple agents and multiple decision-makers. In this broad view of risk minimization, multiple system operational objectives: efficiency, reliability, security, resiliency, sustainability, must be accounted for as must the multiple agencies with different missions, resources, timetables, and agendas. Advanced computing paradigms, such as neural networks, genetic algorithmss, complex (adaptive) systems, knowledge discovery and datamining, can be explored for their modeling fidelity. Models are not in themselves solutions and the

[8] Haimes, Y.Y, and P. Jiang. 2001. Leontief-based model of risk in complex interconnected infrastructures. ASCE Journal of Infrastructure Systems 7(1):1-12.
[9] Friesz, T., S. Peeta, and D. Bernstein. 2001. Multi-layer Infrastructure Networks and Capital Budgeting. Working Paper TF0801A. Department of Systems Engineering and Operations Research, George Mason University, Fairfax, Virginia
[10] Rinaldi, S.M., J.P. Peerenboom, and T. Kelly. 2001. Complexities in identifying, understanding, and analyzing critical infrastructure interdependencies. Accepted for publication in IEEE Control Systems, December 2001.
[11] Amin, M. 2000. Toward self-healing infrastructure systems. IEEE Computer, 33(8):44-53.

translation of model into usable forms draws on a range of disciplines. Visualization, virtual reality, haptics, and other human computer interfaces must be explored in terms of their utility in interpreting model results.

The ability to predict from these models will depend on how well they can be used to estimate and model risk. Much work remains in this area where some risks are best dealt with using mean value and maximum likelihood estimation methods or order statistics, extreme value theory and simulation to deal with low probability, high consequence events. Issues that have yet to be resolved are risk associated with components versus system risk versus risks associated with interdependent systems. The multiple dimensions of risks require further research in multi-objective risk methods as well as methods for integrating current assessment methods for environmental, health, ecological, financial, and technological risks. In addition to discovering how to address the great amount of what is known on risk, there is an overwhelming need to develop methods to account for what is not yet known — uncertainty, e.g., Bayesian, sensitivity, and bounding methods. Other research directions for dealing with risk and prediction are vulnerability and consequence assessment, the latter of which focuses on outcomes separately from the probability of those outcomes.

Finally, successful infrastructure modeling will depend on certain non-technical issues: the ability to procure secure, reliable, and verifiable data. The models must be multi-resolutional to reflect the multiple scales over which decisions are made and over which the systems fail. These system models must be able to capture the wide array of failures, including organizational and human errors and failure. Non-technical issues must be resolved as well such as education and training to provide the workforce and inform R&D.

**Emergency Response and Diagnosis**

Given that extreme events are, by definition, unexpected and unpredictable, a reasonable strategy entails the reactive response. Reactive risk intervention strategies focus on efficient and effective emergency response and crisis management. Key research issues include the creation and curation of infrastructure databases, database on emergency responders and their role, information flows, risk management/communication, group dynamics, organization theory, psychological biases in decision making, and more.

**Life-Cycle Design**

The realization that disasters are designed suggests that design can also reduce risk. Research opportunities exist to better understand thermal stresses, impact loading, plasticity, and stability of structural systems as well as fire proofing and blast resistance. New (smart) materials and designs may prevent or postpone collapse of building structures. Concurrent design methods, such as those employed in manufacturing, can be adapted to build and civil infrastructure for improved safety, reduced costs, environmental, and aesthetic

considerations. After 9/11, building design, particularly for tall buildings, will have to consider and even model occupant behavior during crisis as well. Proper evaluation of these improvements require substantial advances in engineering economics, including life-cycle costing, environmental life-cycle and risk assessment, and decision theory (MADM) to deal with multiple metrics.

**Sensing Critical Infrastructure**

Data is needed for models of system operations and design, early warning, emergency response and recovery. Advances in sensing and communications technologies offer new, low cost capabilities to collect these data and monitor infrastructure systems as well as control them. The scale of this sensing effort will be enormous. Collection of vast quantities of sensed data will demand research in data storage, including multimedia/internet-based systems and domain-specific data architectures. Data quality research will remain an issue as it becomes necessary to track source, reliability, durability, accuracy, uncertainty, security, and privacy information about the data to guarantee its utility. Data transmission will continue to pose interesting research questions about how to use and integrate GIS, GPS, and wireless technologies. The inherent trade-offs between local processing and data transmission to remote control centers pose numerous research questions about both the hard technology and soft algorithms. Optimal control of complex systems that exhibit emergent behavior may require heterogeneous control schemes based on multiple scales, centralized, supervisory, and distributed. Concerns and costs of data storage, transmission, and use will provide the tension necessary to limit excessive data collection. Research must be directed toward optimal design and configuration of sensor systems. Given the lightning pace of sensor technology innovation, sensor and embedded system design must address serviceability and upgradability. Finally, the current teraflops of computational power and rich agent-based paradigms that more accurately capture dynamic gaming and infrastructure interdependencies will be exhausted. New data processing algorithms will be needed for large-scale, real-time and faster-than-real-time data and signal processing of sensed data for monitoring, controlling, and optimization. Such sophisticated software programs will likely generate new demands for newer, faster, and less expensive computing capabilities as well as new system architectures.

**Social, Behavioral, Political and Economic Systems**

Equally important are various social sciences that offer non-structural methods to manage risk and which govern the effectiveness of the technological alternatives in practice. A broad research question is how to allocate resources over this range of options, over various stages of development (research, development, implementation) and over time, especially accounting for the multi-objective, multi-stakeholder nature of the decision. This will entail quantifying the risks, both pre- and post-event, associated with the investment, which, given the low probability of extreme events, offers still more fertile areas for research.

**Conclusion**

Several overarching issues exist regarding the sufficiency of the current workforce to deal with these complicated infrastructure systems at risk, the role of R&D at the Office of Homeland Security, and finally the long-view of risk management, namely, its context in global sustainability.

*(Note:The opinions expressed in this paper are those of the author only, and do not necessarily represent those of the National Science Foundation or any other entity with which the author has been or is now affiliated.)*