Chapter 21

RISK ANALYSIS IN INTERDEPENDENT INFRASTRUCTURES

Yacov Haimes, Joost Santos, Kenneth Crowther, Matthew Henry,
Chenyang Lian and Zhenyu Yan

Abstract Human activities are defined and influenced by interdependent engineered and socioeconomic systems. In particular, the global economy is increasingly dependent on an interconnected web of infrastructures that permit hitherto unfathomable rates of information exchange, commodity flow and personal mobility. The interconnectedness and interdependencies exhibited by these infrastructures enable them to provide the quality of life to which we have become accustomed and, at the same time, expose seemingly robust and secure systems to risk to which they would otherwise not be subjected. This paper examines several analytical methodologies for risk assessment and management of interdependent macroeconomic and infrastructure systems. They include models for estimating the economic impact of disruptive events, describing complex systems from multiple perspectives, combining sparse data to enhance estimation, and assessing the risk of cyber attack on process control systems.

Keywords: Risk analysis, systems engineering, interdependent systems

1. Introduction

Critical infrastructure and industry sectors in the United States and abroad are becoming more interdependent, due largely to the increasing integration and application of information technology in business operations such as manufacturing, marketing and throughout the supply chain. New sources of risk to critical infrastructures and national security emerge from the dynamics of large-scale, complex systems that are highly interconnected and interdependent.

Over several years, researchers at the Center for Risk Management of Engineering Systems at the University of Virginia have addressed these emergent risks and their association with interdependent infrastructures by developing new analytical and methodological frameworks for gaining insight into complex systems, their interdependencies, and the means by which risk can be effectively managed by public policy makers and corporate decision makers. The portfolio of analytical and methodological tools spans several operational domains at the macroeconomic, industry and facility levels. The work is founded in the broad conception that interdependent infrastructures are themselves characterized by interdependent facilities that produce, transport and consume commodities that are distributed over physical and cyber networks. Furthermore, at a more abstract level, the commodity production and consumption patterns of industries can be modeled at the macroeconomic level to gain insight into the dynamics of commodity disruptions at the regional or national levels.

This paper highlights several methodologies for modeling, assessing and managing risk in complex, interdependent systems. Also, it discusses the contexts in which the methodologies are useful from a systems perspective. For reasons of space, we focus on analytical methods developed at our center at the University of Virginia. Our purpose is not to discount the contributions of other research groups. Instead, we advocate the use of our models in combination with other approaches to arrive at more robust analyses of system interdependencies.

2. Risk Assessment

Risk assessment is a process for understanding the result of destructive forces acting on systems of interest in terms of the potential adverse consequences and their associated likelihoods. By understanding how fundamental characteristics of a system contribute to its vulnerability to different sources of risk, a risk assessment methodology provides insight into how to manage risk by changing the state of the system to reduce vulnerability, improve resilience and mitigate potential consequences. Kaplan and Garrick [13] posed the risk assessment triplet of questions:

- What can go wrong?
- What is the likelihood?
- What are the consequences?

Ideally, the process of risk assessment fully develops answers to these questions and, thus, holistically captures all the sources of risk and assesses their associated likelihoods and consequences. Current assessment methodologies decompose systems into isolated subsystems for analysis and recombination to create system-level measures [14]. This approach, however, is inadequate for analyzing complex, interdependent systems of systems. Rinaldi and coworkers [18] underscore the need to enhance interdependency analysis. In their words, "it is clearly impossible to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures; rather, we must consider multiple interconnected infrastructures and their interdependencies in a holistic manner." Current work seeks to address this gap and improve methods for interdependency assessment.

3. Modes of Coupling

Risk assessment and management in large-scale systems requires an understanding of how and to what degree composing subsystems are interdependent. For any given analysis, a subset of particularly relevant interdependencies will tend to dominate the modeling activity, depending on the modeling objectives and the decision maker who will ultimately use the analytical results for developing risk management policies. The role of the modeler is to isolate the relevant interdependencies and build analytical tools to answer the questions posed by decision makers. This section reviews several fundamental modes of coupling, each of which is characterized by different functional and structural relationships. In addition, each mode of coupling is subject to risk in different ways. This is due to the variety of vulnerabilities that can be exploited by potential adversaries; the differing degrees of robustness, resilience and redundancy that provide risk-mitigating mechanisms; and the diverse types and levels of associated consequences.

Physical Coupling Physical coupling between components exists when energy, information or matter is physically transferred from one component to another. In the case of interdependent infrastructures, physical couplings are manifested in the transmission of (i) electricity from distribution networks to electromechanical loads via transformers and transmission lines, (ii) water and gas from distribution infrastructures to points of consumption via plumbing, (iii) materials from one process to another or from one facility to another via plumbing, pipeline or other transport, and (iv) information from one network component to another via the transmission and reception of electromagnetic signals. As such, physical couplings have the capacity to render multiple systems inoperable if critical nodes are disrupted. For example, refineries cannot ship their products to consumers by way of a pipeline if the valves that enable flow from holding tanks to the pipeline are immovably shut. Due to their high degree of criticality, physical couplings tend to be highly robust and are often redundant. However, they are typically neither adaptable nor resilient due to structural and mechanical constraints. Therefore, the risks associated with physical couplings tend to be characterized by significant consequences, yet with relatively low degrees of likelihood. Moreover, risk analysis of physical couplings is typically performed by comparing a set of disruptive scenarios against design or operational specifications.

Logical and Information Coupling Logical couplings provide mechanisms by which coupled systems will conditionally behave based on shared measurements and functional relationships. Information couplings involve mechanisms by which information is physically transferred from one device to another by way of signal transmission. Many infrastructure sectors have become extremely dependent on networked information systems for efficient operations and timely delivery of products and services. The ubiquity of networked information systems in the various infrastructure sectors introduces risks associated with the three main security goals: confidentiality, integrity and availability [1].

As a case in point, the June 1999 rupture of the Olympic Pipeline in Washington State resulted in the leakage of 277,000 gallons of gasoline and the shutdown of the pipeline for more than a year. Tanker trucks and barges were used for gasoline transport during this time, which led to higher retail prices. The National Transportation Safety Board [17] report indicated that the incident was caused by the "slow response" or "non response" of a supervisory control and data acquisition (SCADA) system. From a homeland security perspective, the fact that such an event could have been triggered by a malicious agent is a grave concern, especially since a well-placed attack could cause widespread disruption due to infrastructure interdependencies. Therefore, in order to ensure the security of critical infrastructure sectors, it is imperative not only to understand their inherent physical and economic linkages, but also the information and logical interdependencies associated with networked information systems.

In distributed control systems, logical couplings are implemented in the payloads of data packets; information coupling, on the other hand, is implemented in the routing headers of data packets. In other words, logical coupling is embedded in the messages being communicated, and information coupling is associated with the sequence of relay points in carrying messages from their origins to their destinations. Locally, logical coupling is characterized by the rules embedded in automation software that govern the functionality of controlled processes in response to other processes with which they are interdependent.

Logically coupled systems are by nature prone to risk associated with the propagation of erroneous data or control signals. Using knowledge about the logical coupling in a system, an attacker could potentially disrupt its operation by manipulating measurements or other data used to make control decisions. A well-executed attack of this type would be difficult to detect if the manipulated data is within the normal ranges. For this reason, risk analysis of logically interdependent systems must also take into account the propagation of apparently innocuous manipulations of data and erroneous data.

Inter-Regional Economic Couplings These couplings exist when the production, distribution and consumption of commodities are dictated in part by regional interdependencies defined by physical infrastructures, import and export flows, and relative geographic distances. These couplings are often evident in the aftermath of massively disruptive events such as natural disasters, major plant closures and adversarial geopolitical activity. Typically, inter-regional couplings act to dampen the propagation of disruptions by way of locational redundancies and consumption patterns provided by competitive markets, excess capacities and consumer adaptation in the form of substitution and income effects. In the case of oil and gas infrastructures, geographic couplings were evident in the wake of hurricanes Katrina and Rita, where, immediately following the storms, the supply of crude oil to refineries increased with distance from the epicenter of the storm damage (this observation is based on an analysis of numerous EIA Hurricane Rita situation reports). In other words, supplies of crude from other regions were more available to refineries that were less geographically dependent on Gulf sources.

Risk associated with inter-regional interdependencies is often manifested in economic effects; however, other relationships can create and propagate risk. For example, the water distribution infrastructure poses risk by way of geographic coupling due to the fixed nature of water assets. Hazardous chemical releases in one region threaten consumers in neighboring regions by way of natural hydrology and engineered water distribution infrastructures. Similarly, through geographic coupling, ecological risks associated with oil and gas infrastructures are propagated to regions not directly associated with the infrastructures. Therefore, any analysis of the degree to which communities in the vicinity of accident-prone systems are at risk must take into account geographic interdependencies.

Inter-Sector Economic Couplings These couplings yield insight into how disruptions in one sector will affect dependent sectors. Interdependencies are characterized by the production functions used by the manufacturers of a commodity and the commodities upon which they are dependent for production. Furthermore, as production is driven by demand, disruptions in the marketplace, where commodities are consumed by households, will propagate back to the producers that supply the end products as well as constituent ingredients and other support commodities. A thorough understanding of these interdependencies enables regional and national preparedness planners to better pre-position materials for rapid rehabilitation of critical sectors in the aftermath of a major disaster.

4. Modeling Interdependent Systems

In order to provide answers to the triplet of risk assessment questions, it is necessary to construct models of the systems being considered, potential sources of risk and the couplings to other systems that might provide insights into the dynamics of risk propagation. The models provide descriptions of the state of the system and how changing the system state can reduce the likelihood of adverse consequences, thereby providing a means for evaluating the efficacy of different risk management options. This section describes several methodologies for analyzing interdependent systems: (i) the Input-output Inoperability Model (IIM) [9, 19] and its derivatives, the Multi-Regional IIM (MR-IIM) developed by Crowther [2], and the Dynamic IIM (DIIM) developed by Lian and Haimes [16]; (ii) the Hierarchical Holographic Model (HHM) developed by Haimes [4] and its derivatives, the Adaptive Multi-Player HHM (AMP-HHM) developed by Haimes and Horowitz [7], and the Risk Filtering and Ranking Method (RFRM) developed by Haimes, Kaplan and Lambert [10]; (iii) the Hierarchical Coordinated Bayesian Model (HCBM) being developed by Yan, Haimes and Waller [20]; and (iv) the Network Security Risk Model (NSRM) being developed by Henry and Haimes [11, 12].

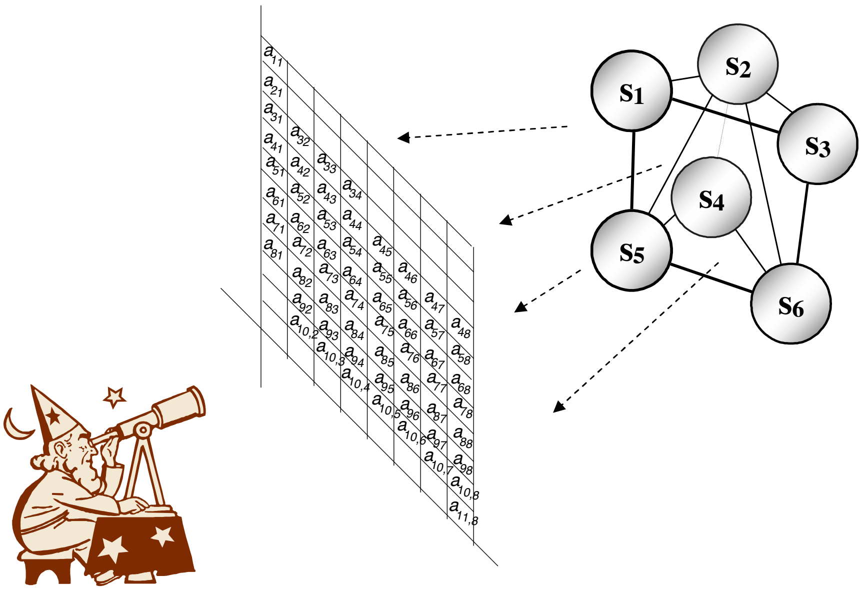

Figure 1. IIM modeling principle as a snapshot of interdependencies.

4.1 Inoperability Input-Output Model

Several models have been proposed to study economic couplings. Input-output analysis, based on the Nobel Prize winning work by Wassily Leontief, is a useful tool for determining the economic ripple effects associated with a disruption in a particular sector of an economy. The Inoperability Input-output Model (IIM) [6, 8, 9, 19] extends the input-output analysis methodology to model the interconnectedness and interactions of different sectors of an economy. Given a perturbation from one or more sectors, IIM estimates the ripple effects measured in terms of industry inoperability and economic loss. For example, a disruption in the oil and gas sector will impact dependent sectors: petroleum and coal products, manufacturing, pipeline transportation, utilities, air transportation, chemical manufacturing and mining. Figure 1 presents IIM as a mapping of sector interdependencies, where s_i, $i = 1, 2, \ldots, 6$ notionally represents a sector with financial, physical and commercial linkages to other sectors (depicted by dotted lines). These linkages are mapped to a series of linear equations whose parameters a_{ij} that populate the matrix quantify the linkages between sectors i and j based on inter-sector transaction data collected and processed by the U.S. Bureau of Economic Analysis.

IIM is an inexpensive, holistic method for estimating economic impacts and sector interdependencies. It can model a nation or regions of contiguous states or counties as an interdependent set of linear causal relationships with perfect communication between all economic sectors. Thus, the resulting effects of a perturbation are estimated uniformly across the entire region without temporal recovery details. The lack of spatial and temporal explicitness in IIM risk analysis produces average estimates across geography and time. These estimates may overlook geographically-concentrated risks and significant cross-regional interdependencies and dynamic effects associated with post-event recovery.

Several extensions to IIM have been developed to address these problems. The Dynamic IIM (DIIM) [16] describes the temporal recovery of sectors after an attack or natural disaster. The concept of resilience is incorporated so that sector improvements can be quantified and managed over time. Like IIM, DIIM shows economic loss and the number of sectors affected when considering different policy options, which directly or indirectly change the recovery dynamics of different sectors as quantified by resilience coefficients in the dynamic model. The Multi-Regional IIM (MR-IIM) [2] estimates higher-order impact propagations across multiple regions and industry sectors by integrating regional models with cross-regional flows gleaned from geospatial databases.

4.2 Hierarchical Holographic Model

The Hierarchical Holographic Model (HHM) [4, 6] provides a construct for capturing the multifarious nature of a complex system to drive subsequent detailed analysis. For example, the HHM in Figure 2 presents a simplified taxonomy of interdependency analysis. The major topics, displayed in the second row of double-lined blocks, describe considerations for interdependency models. The corresponding subtopics cover ranges that may be included in the modeling effort. The value in approaching complex modeling in this way is that questions and analytical activities can be more narrowly and appropriately defined by way of careful system decomposition. Moreover, the reconstruction of the model and analysis follow the reverse process and yield a more comprehensive and useful product for policy analysis and formulation.

The Adaptive Multi-Player HHM (AMP-HHM) [7] and the Risk Filtering and Ranking Method (RFRM) [10], which are derived from HHM, provide more extensive frameworks for collaborative and resource allocation analyses, respectively. In particular, AMP-HHM is a framework for making more structured use of experts with different points of view when analyzing risk in specific assets or classes of systems. In conducting an AMP-HHM exercise, each of several teams of experts is charged with constructing an HHM from its point of view, after which the HHMs are combined to build a richer model of the system of interest. For example, two teams, one representing asset owners and the other representing potential adversaries, might build separate HHMs to capture, from their perspective, the possible paths of attack, methods of defense, etc. The combined HHM serves as a seed for future HHM adaptation on the part of each team. RFRM makes use of HHM development to construct risk scenarios, which are then filtered and prioritized according to their likelihood and consequence assessments to make reasoned judgments for risk management.

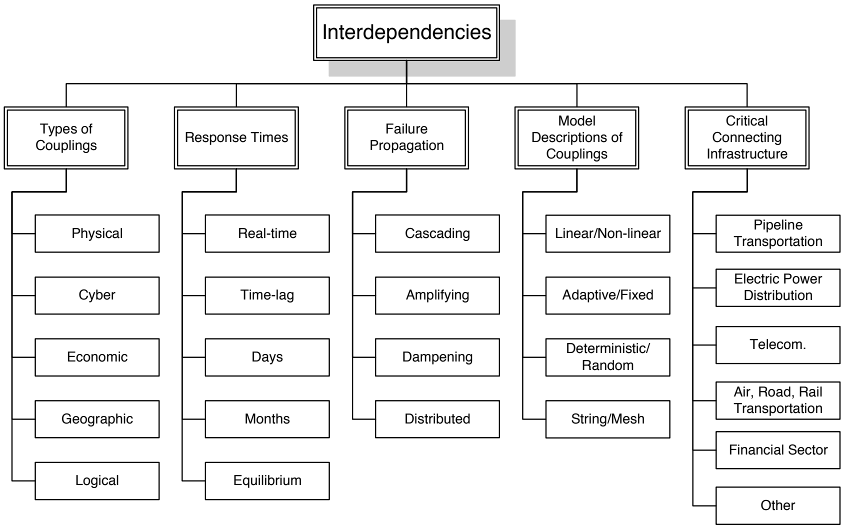

Figure 2. Introductory taxonomy for interdependency analysis.

4.3 Hierarchical Coordinated Bayesian Model

It is well known that when estimating the distributions of parameters with traditional statistical methods (e.g., maximum likelihood estimation), larger data sets give more accurate estimates with smaller confidence intervals and standard errors. However, when statistical methods are applied to small data sets, they produce confidence intervals and errors so large that they are described as unstable. Because problems in risk analysis often involve extreme events, which rarely occur or have never occurred, direct empirical data for these problems are almost always lacking. Therefore, a methodology for analyzing sparse data would be a great asset in risk analysis.

The Hierarchical Coordinated Bayesian Model (HCBM) [20] is a statistical data analysis tool for analyzing sparse data related to extreme events. By decomposing data into multiple perspectives, HCBM can integrate direct data and indirect data from multiple sources and make inferences about extreme event likelihoods and consequences using hierarchical coordination. HCBM reduces the estimation variance and enhances estimation accuracy compared with direct estimation methods.

4.4 Network Security Risk Model

At the facility level, interdependencies exist between system components within the facility, between system components and facility objectives, and between system components and adversary objectives. The Network Security Risk Model (NSRM) [11, 12] was developed to assess the risk of cyber attacks on process control networks in facilities that produce or distribute commodities over large infrastructures. The models are scenario-based to reflect the different attack progressions and consequences arising from different entry points and different attacker objectives. Furthermore, the models are formulated so that risk management policies map directly to the model parameter space, permitting an evaluation of the efficacy of risk management policies as each policy implementation induces a new measure of risk. Dynamic risk assessment results from the sequential implementation of policies. The efficacy of long-term strategies can be evaluated by measuring the average risk due to the state trajectory induced by each risk management strategy.

Several modeling paradigms have been employed, including scenario development, stochastic shortest path models and dynamic risk management. Stochastic shortest path modeling provides a state machine analysis that yields insight into how an attack on an asset might proceed because of the interdependencies between adversary objectives and facility system response. These interactions also provide insight into how attacks might disrupt or disable facility operability as a result of the interdependencies between facility objectives and system components, some or all of which may be disabled by an attack on the facility.

5. Managing Risks in Interdependent Systems

Risk management is a process for developing a set of decisions that place decision makers in a position where they understand and recognize the range of possible consequences and trade-offs for actions in an uncertain environment. The intertwined processes of risk assessment and risk management provide an analysis and decision structure for policy formulation in interdependent systems that accounts for uncertainty and extreme events. The development of risk management policies is guided by the risk management triplet of questions posed by Haimes [5, 6]:

- What can be done and what options are available?
- What are the trade-offs in terms of costs, benefits and risks?
- What are the impacts of current decisions on future options?

The previous section reviewed several methodologies that provide answers to the first two questions. Specifically, the identification of candidate risk management policies can be accomplished through HHM and AMP-HHM, where measures are elicited to mitigate either the likelihood or consequences of disruptive events. Furthermore, RFRM can assist in setting priorities for addressing specific risk scenarios.

Evaluating tradeoffs requires the quantitative assessment of risk for comparison with the costs of risk management. For large-scale economic systems, IIM and its extensions DIIM and MR-IIM provide quantitative estimates of the economic impact stemming from disruptions in commodity production and distribution. NSRM and HCBM provide tools for assessing the risk of cyber attacks on process control networks at a facility level. These risk models provide a means for evaluating the efficacy of candidate risk management policies

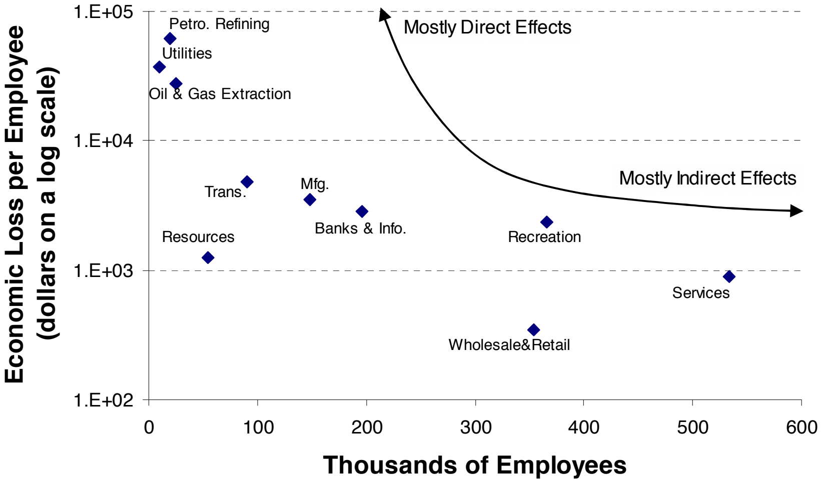

Figure 3. Distribution of direct and indirect impacts across Louisiana economic sectors during the month after Hurricane Katrina.

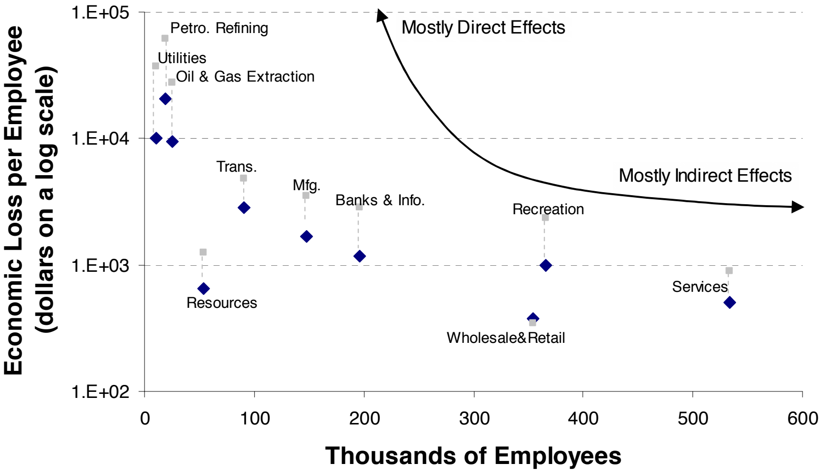

Figure 4. Hypothetical redistribution of impacts from specific preparedness activity.

by producing a measure of risk with and without the policy in place. These assessments, when compared against the estimated cost of risk management policies, permit an evaluation of cost-benefit-risk tradeoffs.

For example, Figures 3 and 4 illustrate the results of an MR-IIM assessment of the benefits of proactive risk management to Gulf Coast residents prior to Hurricane Katrina in 2005 [3]. The analysis also clarifies how cost and benefit could be distributed amongst different interest groups.

Addressing the third question requires a new approach for employing risk models in a dynamic decision framework that evaluates the cost-benefit-risk tradeoffs in the context of constrained future options due to past and present

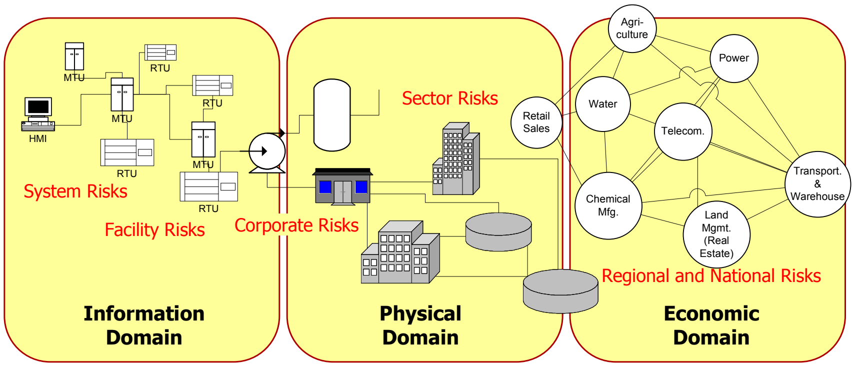

Figure 5. Types and layers of interdependencies.

decisions. A minimax methodology [11, 12], based on the envelope approach to multiobjective optimization [15], has been developed to evaluate the efficacy of risk management policies under scenario uncertainty. For facility-level analysis, NSRM is used as a risk assessment engine to provide measures of risk for evaluation of candidate policies over the course of several decision periods that correspond to corporate resource allocation cycles. Analyses based on minimax envelopes are robust in the face of the uncertainty associated with cyber attack scenarios. At a macroeconomic level, MR-IIM is embedded in the minimax envelope framework to evaluate preparedness and emergency response policies at a regional level.

6. Layers of Interdependencies

Interdependencies may be characterized by different modes of coupling to facilitate modeling and analysis. Similarly, systems can be modeled from different perspectives and abstraction levels to provide analytical support to decision makers at various levels within an organization or system of organizations.

Consider the interdependent systems illustrated in Figure 5. At the lowest level, a process control system manages petrochemical plant operations. This information level connects organizations, protocols, operators and machines based on defined operations, and it allows the vulnerabilities present in any aspect of the system to affect other parts of the system. The middle layer of the diagram illustrates the larger physical and business interconnections. Plants and buildings are physically connected, and products flow between plants and are shared by the plants. At the highest level, plant units interoperate with other businesses, economic sectors and infrastructure sectors.

Risk is experienced and analyzed at each level of this hierarchy according to the objectives and requirements of the respective decision makers. Correspondingly, analyses require hierarchies of models and simulations to understand how micro-level activities affect the behavior of macro-level systems. These interactions are bi-directional in the sense that events in one micro-level system will influence the events and decisions made in other micro-level systems by way of interdependencies, which are observed and experienced at an abstracted level. Therefore, the risk analyst must determine the appropriate hierarchy of questions to ask, the systems to model, and the information to collect when assessing risk in interdependent systems and providing insights for risk management.

7. Conclusions

The United States is a hierarchy of interdependent systems comprising multiple classes of decision makers and stakeholders ranging from national policy makers to operators of specific critical infrastructure components. The risk assessment and risk management methodologies presented in this paper support analyses of the interdependencies surrounding macroeconomic and infrastructure systems. The analyses may be conducted at multiple levels of system resolution and can be integrated to develop hierarchies of insights and recommendations. IIM and its dynamic and multi-regional extensions support analyses of the ripple effects of disruptive events across interdependent macroeconomic sectors and regions. In contrast, NSRM models cyber and logical interconnections among components of a process control network and its infrastructure for the purpose of assessing the risk of cyber attacks on specific facilities.

The many dimensions of interdependencies coupled with the data-sparse nature of extreme risk scenarios make model parameterization a challenge. HHM identifies critical sources of risk; its collaborative extension enables the pooling of parameter estimates from multiple experts along with the associated uncertainties. To complement the parameter estimation and risk quantification processes, HCBM is being developed to integrate multiple databases to improve confidence in statistical inference when data scarcity is a significant factor.

Acknowledgements

This work was partially supported by the Institute for Information Infrastructure Protection (I3P) under Award 2003-TK-TX-0003 from the Science and Technology Directorate of the U.S. Department of Homeland Security. Additionally, we wish to acknowledge the contributions of Bayard Gennert, Grace Zisk and Joanne Foster, who edited versions of this manuscript, and Professors Barry Horowitz and James Lambert, who provided their expertise and insight through discussions and critical reviews.

References

[1] R. Bace, *Intrusion Detection*, MacMillan Technical Publishing, Indianapolis, Indiana, 2000.

[2] K. Crowther, Development and Deployment of the Multiregional Inoperability Input-Output Model for Strategic Preparedness of Interdependent Regions, Ph.D. Dissertation, Department of Systems and Information Engineering, University of Virginia, Charlottesville, Virginia, 2006.

[3] K. Crowther, Y. Haimes and G. Taub, Systemic valuation of strategic preparedness through application of the inoperability input-output model with lessons learned from Hurricane Katrina, to appear in *Journal of Risk Analysis*, 2007.

[4] Y. Haimes, Hierarchical holographic modeling, *IEEE Transactions on Systems, Man and Cybernetics*, vol. 11(9), pp. 606–617, 1981.

[5] Y. Haimes, Total risk management, *Risk Analysis*, vol. 11(2), pp. 169–171, 1991.

[6] Y. Haimes, *Risk Modeling, Assessment and Management*, Wiley, New York, 2004.

[7] Y. Haimes and B. Horowitz, Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis, *Journal of Homeland Security and Emergency Management*, vol. 1(3) (www.bepress .com/jhsem/vol1/iss3/302), 2004.

[8] Y. Haimes, B. Horowitz, J. Lambert, J. Santos, C. Lian and K. Crowther, Inoperability input-output model for interdependent infrastructure sectors, *ASCE Journal of Infrastructure Systems*, vol. 11(2), pp. 67–92, 2005.

[9] Y. Haimes and P. Jiang, Leontief-based model of risk in complex interconnected infrastructures, *Journal of Infrastructure Systems*, vol. 7(1), pp. 1–12, 2001.

[10] Y. Haimes, S. Kaplan and J. Lambert, Risk filtering, ranking and management framework using hierarchical holographic modeling, *Risk Analysis*, vol. 22(2), pp. 383–398, 2002.

[11] M. Henry, Mimimax Envelopes for Total Cyber Risk Management in Process Control Networks, Ph.D. Dissertation, Department of Systems and Information Engineering, University of Virginia, Charlottesville, Virginia, 2007.

[12] M. Henry and Y. Haimes, A new dynamic risk assessment and management model for supervisory control and data acquisition networks, presented at the *Society of Risk Analysis Annual Meeting*, 2006.

[13] S. Kaplan and B. Garrick, On the quantitative definition of risk, *Risk Analysis*, vol. 1(1), pp. 11–27, 1981.

[14] S. Kaplan, Y. Haimes and B. Garrick, Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk, *Risk Analysis*, vol. 21(5), pp. 807–819, 2001.

[15] D. Li and Y. Haimes, The envelope approach for multiobjective optimization problems, *IEEE Transactions on Systems, Man and Cybernetics*, vol. 17(6), pp. 1026–1038, 1987.

[16] C. Lian and Y. Haimes, Managing the risk of terrorism to interdependent systems through the dynamic inoperability input-output model, *Systems Engineering*, vol. 9(3), pp. 241–258, 2006.

[17] National Transportation Safety Board, Pipeline Accident Report: Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999, Washington, DC, 2002.

[18] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems*, vol. 21(6), pp. 11–25, 2001.

[19] J. Santos and Y. Haimes, Modeling the demand reduction input-output inoperability due to terrorism of interconnected infrastructures, *Risk Analysis*, vol. 24(6), pp. 1437–1451, 2004.

[20] Z. Yan, Y. Haimes and M. Waller, Hierarchical coordinated Bayesian model for risk analysis with sparse data, presented at the *Society of Risk Analysis Annual Meeting*, 2006.