Chapter 19

AN INTEGRATED METHODOLOGY FOR CRITICAL INFRASTRUCTURE MODELING AND SIMULATION

William Tolone, Seok-Won Lee, Wei-Ning Xiang, Joshua Blackwell, Cody Yeager, Andrew Schumpert and Wray Johnson

Abstract Integral to effective critical infrastructure analysis is the assessment of infrastructure vulnerabilities, which provides insights into potential disruptions that can enhance protection plans and response and recovery operations. Effective critical infrastructures analysis, however, must account for the complex, multi-dimensional characteristics of infrastructures and the dependencies between infrastructures. This paper presents a new methodology for integrated modeling and simulation that supports such analysis. An integrated analysis environment that embodies this new methodology is presented as a proof of concept.

Keywords: Modeling, simulation, geospatial analysis, ontological analysis

1. Introduction

Critical infrastructures are infrastructures that, if disrupted, can undermine a nation's security, economy, public health and way of life [15]. Recent incidents such as the 2003 blackout in the Northeastern United States and Southeastern Canada and the 2005 hurricanes in Louisiana and Texas demonstrate the catastrophic impacts of critical infrastructure disruptions. While it is unlikely that disruptions can be prevented, effective critical infrastructure analysis can – at the very least – minimize their impact by improving vulnerability assessments, protection planning and strategies for response and recovery.

Critical infrastructure analysis seeks to provide insights into infrastructure behavior and potential disruptions that can increase the efficacy of protection plans and response and recovery operations. The U.S. Government has identified thirteen critical infrastructure sectors (e.g., energy, communications, and banking and finance) [15]. Each sector is a mission-critical, socio-technical system involving complex, multi-dimensional collections of technologies, infor-

Please use the following format when citing this chapter:

Tolone, W., Lee, S.-W., Xiang, W.-N., Blackwell, J., Yeager, C., Schumpert, A. and Johnson, W., 2008, in IFIP International Federation for Information Processing, Volume 290; *Critical Infrastructure Protection II*, eds. Papa, M., Shenoi, S., (Boston: Springer), pp. 257–268.

mation, processes and people. All the sectors are highly interdependent – disruptions in one sector cascade and escalate across the other sectors [12].

In order to account for these characteristics, critical infrastructure analysis must satisfy two important requirements. First, it should emphasize the engineering properties and the behavioral properties of each infrastructure. Engineering properties describe the technical characteristics of an infrastructure in terms of the underlying physics-based properties of the inanimate objects that constrain infrastructure operation. Behavioral properties describe the relational properties that emerge from business processes, decision points, human interventions, information availability, reliability and consistency, in addition to the engineering properties of the infrastructure.

Second, critical infrastructure analysis must be conducted *in situ*, i.e., in context. Suchman [13] argues that context gives meaning to action – separating actions from the context in which they are performed causes the meanings or implications of the actions to be lost. Examining infrastructures in isolation ignores the complex dependencies that exist between infrastructures and the contextual factors that constrain infrastructure behavior. This results in vulnerability assessments that are at best incomplete and at worst invalid.

These two requirements must constitute the foundation for any comprehensive, holistic and systemic analysis of critical infrastructures, especially modeling and simulation activities that support infrastructure protection. This paper presents a new methodology for infrastructure modeling and simulation that addresses the two requirements. The methodology is realized within an integrated environment that supports effective critical infrastructure analysis.

2. Related Work

Modeling and simulation are important activities that facilitate the exploration and analysis of complex phenomena, especially those encountered in critical infrastructure systems. In fact, for many phenomena, modeling and simulation may be the only viable means for exploration and analysis. This is particularly true for phenomena that are characterized by organic collections of events involving open systems — systems that may include social, economic, technical, civic, environmental, informational and geographic contexts. Effective modeling and simulation of these phenomena often require a system-of-systems approach that recognizes the various dimensions of the phenomena and the relationships between the dimensions.

A comprehensive survey of critical infrastructure modeling and simulation solutions can be found in [10]. Several solutions decompose analysis to the exploration of individual infrastructures. Many useful single infrastructure solutions exist (see, e.g., [4, 11]). However, decomposition methods fail to recognize the importance of the behavioral properties of infrastructures and the complex dependencies existing between infrastructures. Furthermore, these solutions are difficult to generalize due to the unique characteristics of each infrastructure.

Other solutions focus on infrastructure interdependencies (see, e.g., [3, 6]). These solutions attempt to recognize the *in situ* requirement and model the

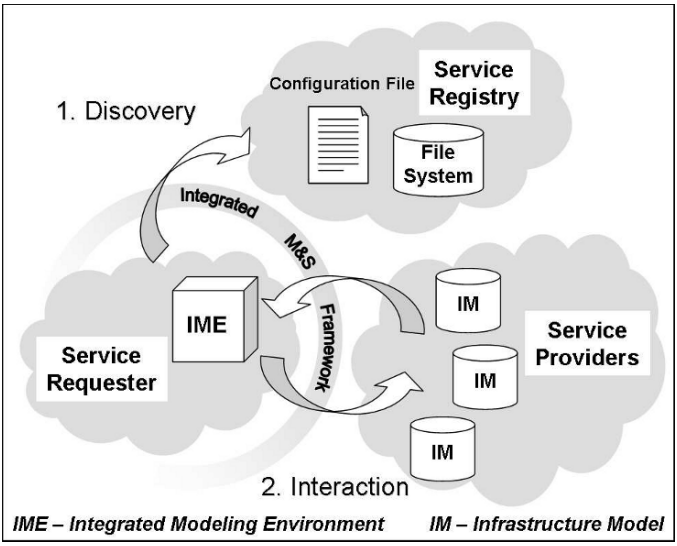

Figure 1. Integrated modeling and simulation framework.

complex behavior that emerges from the interdependencies. However, these solutions do not adequately incorporate the unique behaviors of the underlying infrastructures. While interdependencies can lead to cascading and escalating effects [12], these effects arise specifically from the interplay of the interdependencies and the individual behavior of infrastructures. When the behavior of individual infrastructure is ignored, the fidelity of the model is greatly reduced.

Still other solutions attempt to construct comprehensive models of critical infrastructures (see, e.g., [2, 5, 9, 12, 14]). However, detailed comprehensive models are difficult to construct due to the unique characteristics of each infrastructure. As a result, these models emphasize higher levels of analysis at the cost of detailed analysis.

Recently, there have been efforts to develop hybrid solutions for critical infrastructure modeling and simulation (see, e.g., [1, 16]). Pederson and colleagues [10] describe these efforts as adopting a "coupled modeling" approach. Under this approach, individual infrastructure models are integrated in a generalized manner with models of infrastructure dependencies to enable system-of-systems analysis, which couples the fidelity of individual infrastructure models with the requirement for *in situ* analysis. Our modeling and simulation solution leverages this coupled approach.

3. Modeling and Simulation Methodology

This section describes the modeling and simulation methodology, which builds on our previous work in the area [16]. The methodology leverages existing infrastructure models and a representation of context and behavior.

3.1 Integration Framework

The methodology for modeling and simulation is based, in part, on the ability to integrate separate infrastructure models within a single framework. The framework is designed around a service-oriented architecture supported by a common service provider API (Figure 1). Under this framework, each infrastructure model is integrated by implementing a framework connector, which realizes the common service provider API, and registering the connector with the framework's service registry. The infrastructure models are leveraged during analysis via the connectors by the Integrated Modeling Environment (described below), which functions as a service requester. Interaction between the service requester and service providers is event-driven. Thus, the methodology enables discrete simulations in support of analysis activities. Individual infrastructure models, however, may or may not be event-based. To integrate continuous simulation models, it is necessary to implement a framework connector that adapts continuous simulations to discrete simulations.

3.2 Representing Context and Behavior

Because context gives meaning to action [13], examining the behavior of critical infrastructures in isolation and outside of space and time leads to a loss in the meaning or implication of infrastructure behavior. John Locke's definition of "knowledge" inspires our representation of context and the meaning it embodies. Locke [8] describes knowledge as the ability to distinguish concepts or ideas. In other words, knowledge emerges from relationships among concepts. Our representation leverages this definition and draws on ontology principles and the notion of a relation to provide a representation of context and behavior. Our methodology uses relations to support the specification of contextual and behavioral properties along three dimensions: function, time and space. These dimensions situate infrastructure features and their collective behavior by answering how, when and where features are related. In this context, an infrastructure feature is any modeled component of an infrastructure.

Functional Relations Under our methodology, each infrastructure feature may be associated functionally with other infrastructure features. We define functional relations according to a specified commodity and relational rule, and by leveraging a provider/subscriber paradigm. Commodities are tangible or intangible goods or services that may be generated, transported or consumed by infrastructure features. Relational rules further restrict the relation by constraining the set of origin features that may provide a commodity to a destination feature. Most relational rules constrain this behavior according to provider/subscriber proximity.

A functional relation is represented by the tuple, $(origin \times commodity \times destination \times relational\_rule)$, which states that the infrastructure feature *origin* provides the *commodity* to infrastructure feature *destination* according to the *relational_rule*. Given that the collective critical infrastructure of a

region may contain tens of thousands of features, it is not feasible to specify every functional relation. Therefore, we allow functional relations to be specified at a type/subtype level and an instance level using selection sets. A selection set is a specification that resolves to a set of features according to a specified criterion. For example, functional relations can be specified that state that infrastructure features of type *origin_type* provide a *commodity* to infrastructure features of type *destination_type* according to the *relational_rule*.

Temporal Relations Under our methodology, each infrastructure feature may be associated with temporal latencies for enabling or disabling the feature. A temporal relation is represented by the tuple, ($feature \times commodity \times effect \times duration$), which states that when an infrastructure $feature$ loses or gains access to a *commodity*, the *effect* (i.e., disable or enable) is delayed by a *duration*. For example, if an infrastructure feature losses access to the essential commodity electricity, the disabling effect of losing the commodity is delayed until the specified latency has passed; this latency may model a limited alternative commodity source (e.g., battery backup). Similarly, once an infrastructure feature gains access to its essential commodities, the enabling effect is delayed until the specified latency has passed; this latency can model the startup time required to enable the feature. If access to an essential commodity is restored before the disablement latency has expired, then the disable event is discarded. Similar to functional relations, temporal relations for infrastructure features may be specified at the type/subtype or instance levels.

Spatial Relations Finally, our methodology recognizes that infrastructure features, as physical objects, are spatially tangible. Therefore, each infrastructure feature may be associated with a location in space. Its location and spatial relationships with other infrastructure features are represented by geographic coordinates and also, as in many geographic information systems, by topological relationships [7]. A spatial relation is represented by the tuple, ($feature \times location$), which states that infrastructure $feature$ is located at *location* in geographic space. Spatial relations of infrastructure features are used in numerous ways, including for proximity analysis according to relational rules (e.g., nearest provider in a given radius), spatial correlations (e.g., map overlays) and geo-visualizations.

Infrastructure Context and Behavior Ontology Integrating functional, temporal and spatial relations leads to an ontology for modeling infrastructure context and behavior (Figure 2). An ontology models the well-defined dimensions of a domain in terms of objects, attributes and relations. It also enables the construction of a common understanding through a common language and representation for analytical discourse. In our ontology, functional and temporal relations are represented by the objects in grey. Spatial relations are modeled by the "Space" association between the "Feature" object and the "Location" object.

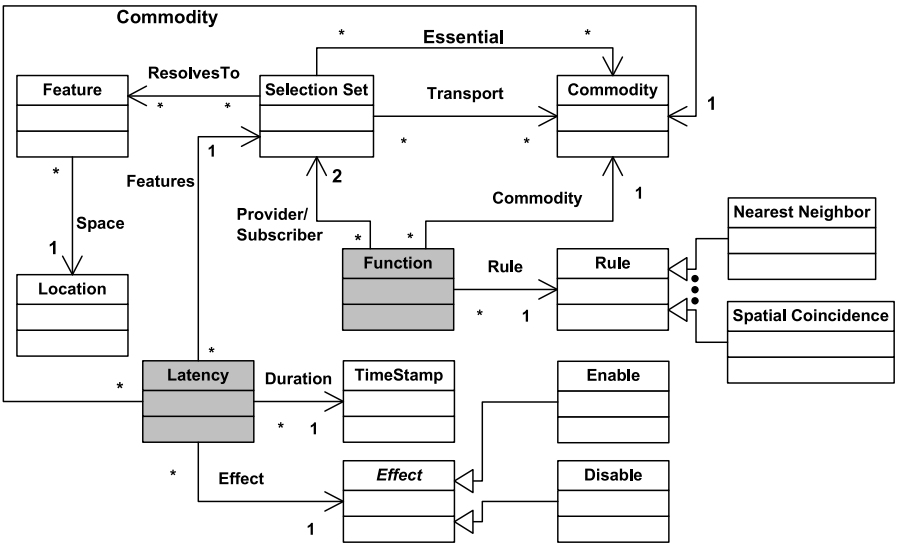

Figure 2. Infrastructure context and behavior ontology.

4. Integrated Methodology

Our new methodology leverages the integration framework and the context and behavior ontology. It involves five steps.

1. **Infrastructure Model Identification and Development:** Infrastructure models are realized by using third party products (e.g., [4, 11]) or by instantiating generic infrastructure models that are built into the integration framework (e.g., utility, transport and channel networks).
2. **Connector Development:** Each infrastructure model must instantiate a connector for the model to participate in the integration framework. The framework provides a simple connector API for connector development.
3. **Infrastructure Model Importation:** The modeling environment, as a service requester, requires from each infrastructure model a representation of the infrastructure features for the model for the features to participate in the context and behavior ontology.
4. **Integrated Model Development:** Functional, temporal and spatial relations are specified (ontology instantiation); relationships are instantiated based on these specifications.
5. **Integrated Modeling and Simulation:** Models are explored, simulations are executed and analyzed, models are validated and analysis products are constructed.

These five steps are not necessarily performed in a sequential manner. Each step remains ongoing as analysis questions change, infrastructure models evolve (due to data acquisition, verification and validation), and the integrated model

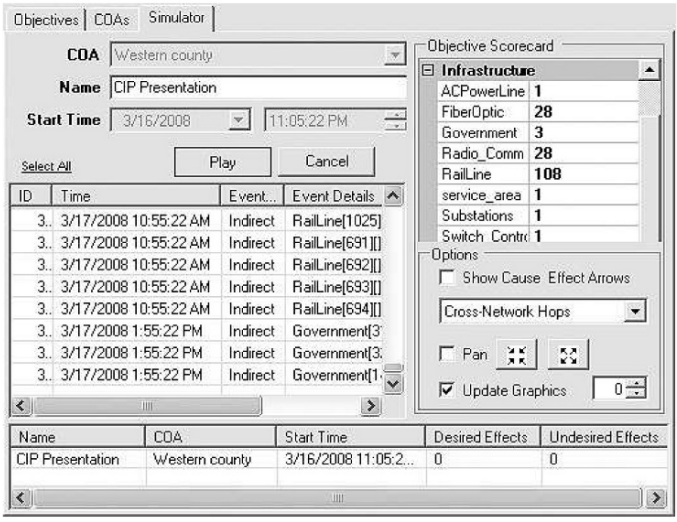

Figure 3. Analyst interface (Simulator tab).

evolves (due to model evolution, verification and validation). Thus, analysis is an organic activity that is seamlessly integrated with infrastructure model development, integrated model development, and verification and validation.

5. Integrated Modeling Environment

The Integrated Modeling Environment (IME) facilitates system-of-systems analysis by enabling the horizontal fusion of infrastructure models. System-of-systems analysis seeks to explore and understand the collective behaviors of integrated systems. In the context of critical infrastructure protection, system-of-systems analysis may require the integration of separate models of, for example, the electric power, telecommunications, natural gas distribution and transportation infrastructures in a geographic region. Analysts may use the IME to conduct integrated, multi-model analyses using simulations to explore and understand the collective behaviors of the integrated models.

The primary interface for the analyst includes a multi-tab palette and a geo-visualization of a given region. The Analyst interface palette is presented in Figure 3. Included in this palette are three tabs. The first tab, "Objectives," enables analysts to specify desired and undesired effects aggregated under a named objective. An effect represents the disabling of a domain model element (infrastructure feature). Objectives may be specified from a red-team or blue-team perspective.

The second tab allows analysts to specify sequences of scheduled events (courses of action), where each event represents the enabling or disabling of an infrastructure feature at a specific time during the simulation.

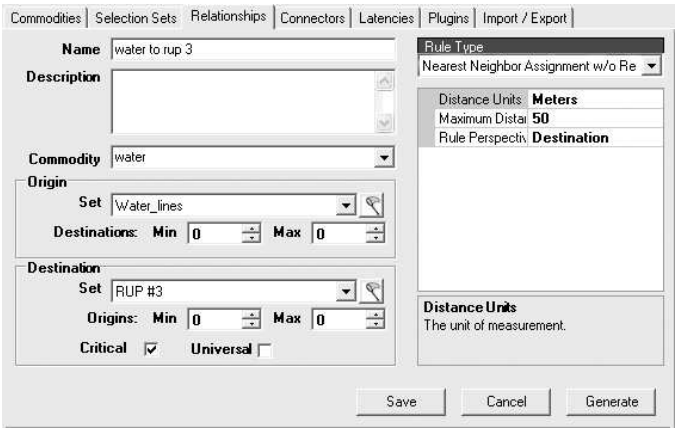

Figure 4. Model Builder interface (Relationships tab).

The third tab, "Simulator," is visible in Figure 3. This tab allows analysts to select a course of action, specify a start time and initiate a simulation. As the simulation executes, the analyst sees on the left-hand side of this tab an event stream capturing infrastructure feature enable and disable events. Features are enabled/disabled as a function of individual infrastructure model behavior and as a function of the relations specified in the infrastructure context and behavior ontology. Each simulation event includes a timestamp. The right-hand side of the simulator tab contains a scorecard that aggregates simulation event stream data along various dimensions (e.g., time, infrastructure and feature type). Saved simulations are listed at the bottom of the tab. As the simulation executes, analysts can observe the effects in the geo-visualization. Dynamic changes in feature symbology reflect domain model state changes (i.e., enabling and disabling of features).

To conduct meaningful analysis, however, the context and behavior ontology must be specified. This activity is supported by a separate Model Builder interface palette. The palette includes, among other tabs, interfaces for specifying commodities, relationships, latencies and connectors. The "Relationships" tab (Figure 4) enables model builders to specify and manage the functional relations for domain models. The "Latencies" tab provides model builders with a means to manage the temporal relations that specify infrastructure feature enabling and disabling latencies. Finally, the "Connectors" tab provides model builders with a means to manage the participating infrastructure models. Several infrastructure models have been integrated into the IME via the connector framework (e.g., [4, 11]). In addition, the IME, by default, provides the aforementioned built-in models (utility, transport and channel networks).

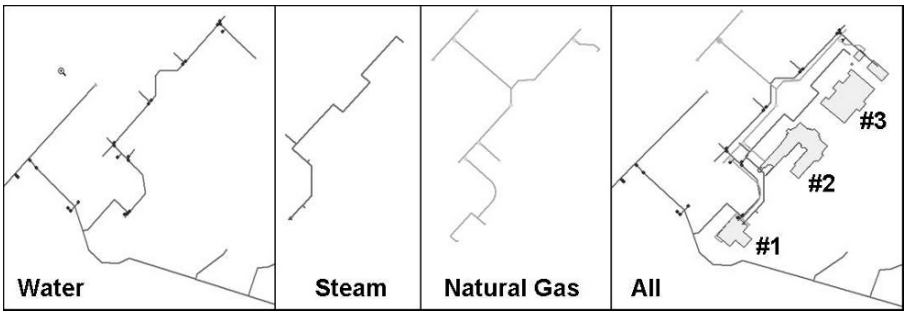

Figure 5. Example infrastructure models.

6. Critical Infrastructure Analysis

This section presents an example application of our integration methodology. The example involves a small geographic region with several buildings and three critical infrastructures (natural gas, steam and water). Figure 5 presents each infrastructure and a layered view of all three infrastructures.

Table 1. Temporal relations.

Selection Set	Commodity	Effect	Duration
Steam Source	Steam	Disable	1.00:00:00 (d.h:m:s)

To support integrated modeling and simulation across the infrastructures, it is necessary to geo-code relevant infrastructure features to establish spatial context. Next, the commodities that are essential to operating the infrastructures are identified (steam, gas and water). The temporal latencies for infrastructure features are then specified to establish the temporal context. Table 1 lists the single temporal latency specification used in the example.

Table 2. Functional relations.

Origin	Commodity	Destination	Rule
Water Line	Water	Building #1	Nearest Neighbor
Building #1	Steam	Steam Source	Nearest Neighbor
Steam Line	Steam	Buildings #2 and #3	Nearest Neighbor
Gas Line	Gas	Building #1	Nearest Neighbor

Finally, the functional relations among the infrastructure features are specified. Table 2 presents the three functional relations used in the example.

During analysis, the Analyst interface (Figure 3) is used to specify objectives and courses of action, and to execute and explore simulations. In the exam-

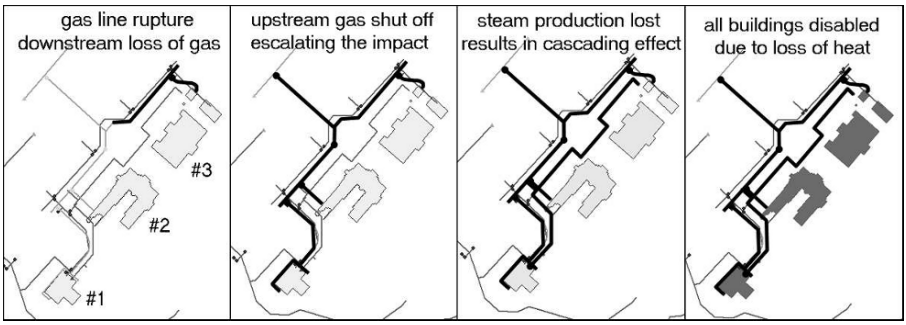

Figure 6. Example simulation (disabled features in bold).

ple, the objective is to maintain the operation of Buildings #2 and #3 (i.e., the analyst specifies an objective with the undesired effects of disabling these buildings). The course of action is initiated by a gas line fracture due to ongoing construction. Subsequent to the fracture, downstream gas is lost (Panel 1 in Figure 6). To contain the leak, a gas valve is closed one hour into the simulation as scheduled in the course of action. This results in the loss of the gas commodity to Building #1 (Panel 2). The loss of gas to Building #1 halts the production of steam (Panel 3). After twenty-four hours, Buildings #2 and #3 cannot function because they have no heat (Panel 4). The integrated modeling and simulation behavior demonstrated by the simulation is realized by the behaviors of the individual infrastructure models and the temporal, spatial and functional relations in the IME context and behavior ontology.

The simulations may be explored further, replayed and saved for subsequent analysis. Analysts may use the scorecard interface to examine the order of impact of simulation events and the plausible impact to each critical infrastructure. In addition, analysts can examine the event trace to understand and/or validate the event chain that lead to (un)desired effects. During the analysis, the ontology may be refined, e.g., by adding/deleting/modifying commodities, functional relations and/or temporal latencies, to explore "what-if" scenarios.

7. Conclusions

The new methodology for critical infrastructure modeling and simulation emphasizes the engineering and behavioral properties of individual infrastructures and enables analyses to be conducted in functional, spatial and temporal context. The methodology effectively captures the complex, multi-dimensional characteristics of individual infrastructures and the dependencies between infrastructures, helping provide insights into potential disruptions that can increase the efficacy of protection plans and response and recovery operations.

The methodology, as realized in the IME, is being actively used to explore and analyze critical infrastructures for large-scale geographic regions ($> 100{,}000$ square km). An integrated model also has been developed for an urban re-

gion (> 500 square miles with a population exceeding 800,000); the critical infrastructures in the integrated model include electric power, natural gas distribution, water distribution, telecommunications and transportation. Other applications include a corporate IT infrastructure model for a Fortune 100 company that integrates models for hardware, software, business applications, business processes and business units; and an urban neighborhood model covering roughly 1,000 contiguous acres that serves a population of more than 20,000.

Evaluation of the methodology is a priority [17, 18]. Verification and validation are enabled by the methodology's adherence to the principle of transparency. All analysis enabled by the ontology is completely transparent to analysts; event traces can be explored and questioned by subject matter experts. The result is an ongoing interleaving of analysis with verification and validation, which improves the underlying ontology and the resulting analysis.

Current research is focusing on augmenting the methodology and its underlying framework to accommodate non-deterministic models and infrastructure degradation. In addition, efforts are underway to enhance the expressiveness of the IME ontology and the IME visualization facility, especially the ability to view multiple infrastructure models along their functional, spatial and temporal dimensions.

References

[1] E. Casalicchio, E. Galli and S. Tucci, Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures, *Proceedings of the Eleventh IEEE International Symposium on Distributed Simulation and Real-Time Applications*, pp. 182–189, 2007.

[2] A. Chaturvedi, A society of simulation approach to dynamic integration of simulations, *Proceedings of the Winter Simulation Conference*, pp. 2125–2131, 2006.

[3] D. Dudenhoeffer, M. Permann and M. Manic, CIMS: A framework for infrastructure interdependency modeling and analysis, *Proceedings of the Winter Simulation Conference*, pp. 478–485, 2006.

[4] ESRI, ArcGIS Network Analyst, Redlands, California (www.esri.com/software/arcgis/extensions/networkanalyst/index.html).

[5] F. Flentge and U. Beyer, The ISE metamodel for critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp 323–336, 2007.

[6] O. Gursesli and A. Desrochers, Modeling infrastructure interdependencies using Petri nets, *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1506–1512, 2003.

[7] C. Lo and A. Yeung, *Concepts and Techniques of Geographic Information Systems*, Prentice Hall, Upper Saddle River, New Jersey, 2007.

[8] J. Locke, *An Essay Concerning Human Understanding* (books.google.com/books?id=cjYIAAAAQAAJ), 1690.

[9] J. Marti, J. Hollman, C. Ventura and J. Jatskevich, Design for survival: Real-time infrastructures coordination, presented at the *International Workshop on Complex Network and Infrastructure Protection*, 2006.

[10] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Report No. INL/EXT-06-11464, Critical Infrastructure Protection Division, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[11] PowerWorld Corporation, PowerWorld Simulator, Champaign, Illinois (www.powerworld.com/products/simulator.asp).

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

[13] L. Suchman, *Plans and Situated Actions: The Problem of Human-Machine Communication*, Cambridge University Press, Cambridge, United Kingdom, 1987.

[14] N. Svendsen and S. Wolthusen, Multigraph dependency models for heterogeneous critical infrastructures, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp 337–350, 2007.

[15] The White House, National Strategy for Homeland Security, Washington, DC (www.whitehouse.gov/homeland/book/nat_strat_hls.pdf), 2002.

[16] W. Tolone, D. Wilson, A. Raja, W. Xiang, H. Hao, S. Phelps and W. Johnson, Critical infrastructure integration modeling and simulation, *Proceedings of the Second Symposium on Intelligence and Security Informatics (LNCS 3073)*, Springer, Berlin-Heidelberg, Germany, pp. 214–225, 2004.

[17] A. Weeks, An Assessment of Validation Methods for Critical Infrastructure Protection Modeling and Simulation, M.A. Thesis, Department of Geography and Earth Sciences, University of North Carolina at Charlotte, Charlotte, North Carolina, 2006.

[18] A. Weeks, A. Schumpert, S. Lee, W. Tolone and W. Xiang, A new approach to verification and validation in CIP modeling and simulation, presented at the *Twenty-Sixth International ESRI User Conference*, 2006.