Interdependency Modeling and Emergency Response

Donald D. Dudenhoeffer,
May R. Permann
Steven Woolsey
Robert Timpany
Idaho National Laboratory
Donald.Dudenhoeffer@inl.gov
May.permann@inl.gov
Steve.Woolsey@inl.gov
Robert.Timpany@inl.gov

Chuck Miller
Anthony McDermott
Priority 5, Inc.
Chuck.miller@priority5.com
Tony.McDermott@priority5.com

Dr. Milos Manic
University of Idaho
misko@uidaho.edu

Keywords: Discrete Event Simulation, critical infrastructure, infrastructure interdependency analysis**.**

Abstract

In large-scale disaster events, infrastructure owners are faced with many challenges in deciding the allocation ofresources for preparation and response actions. This decision process involves building situation awareness, evaluating course of action, and effecting response. This paper describes a modeling and simulation system called CIMS© that presents a visual environment for assessing the causal effects of events and actions in complex environments. Specifically, CIMS© provides a framework for evaluating cascading effects associated with infrastructure interdependencies, thus providing greater situational awareness to infrastructure owners and decision-makers. This paper first presents the area of interdependency analysis and then presents CIMS© as a network framework for simulating the interactions between multiple infrastructures. Also introduced is the integration of infrastructure simulation with a decision support systems.

1. INTRODUCTION

In the past ten years, unprecedented disasters have occurred in the United States that have brought to the fore front the area of critical infrastructure protection. These events include the World Trade Center Attack (9/11/01), the Northeast Blackout (8/14/2003), Hurricane Katrina (8/29/05), Hurricane Rita (9/24/05), and even the Buffalo, NY Snowstorm (10/12/06). These disasters have challenged emergency response teams and stressed the critical infrastructures on both a local and national scale often exposing the highly interdependent nature of infrastructures and our general lack of understanding of these relationships.

1.1. Critical Infrastructure

The U.S. Patriot Act defines *critical infrastructure* as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. " [1]

Further, Congress set forth the following findings in Section 1016 of the U.S.A. Patriot Act:

- The information revolution has transformed the conduct of business and the operations of government as well as the infrastructure relied upon for the defense and national security of the United States.
- Private business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors.
- A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States.
- This national effort requires extensive modeling and analytic capabilities for purposes of evaluating appropriate mechanisms to ensure the stability of these complex and interdependent systems, and to underpin policy recommendations, so as to achieve the continuous viability and adequate protection of the critical infrastructure of the Nation. [2]

The U.S. Government further breaks the infrastructure into thirteen individual sectors, which are:

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base

- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping [3]

These sectors in turn contain individual infrastructures such as highways, rail systems, electric power generation and distribution, etc. Some of these systems are managed by government agencies, but the majority resides with industry.

Advances in information technology (IT) and the necessity to improve efficiency, have resulted in infrastructures that have become increasingly automated and interlinked. Most modern commercial infrastructures are composed of a collection of interconnected networks (both physical and computer-based) that serve different purposes and have many different owners. Numerous seemingly independent information and control systems coordinate resources and functions.

The complexity and interdependency of resource flow and function introduce nuances and potential vulnerabilities that are not always obvious. Indeed, even parts of the information residing on a single sub-network may have different purposes and different owners. Critical information and controls are passed between these component elements to coordinate necessary functions. The complexity and interdependency of this critical information flow introduces nuances and potential vulnerabilities into the infrastructure. Natural disasters, deliberate attacks or accidental system failures within infrastructures may result in cascading effects that are not readily apparent.

1.2. Infrastructure Interdependencies

> "One of the most frequently identified shortfalls in knowledge related to enhancing critical infrastructure protection capabilities is the incomplete understanding of interdependencies between infrastructures." [4]

This collection of infrastructure networks and their associated interdependencies creates a highly nonlinear and complex system, which as illustrated in the above quote, is inherently difficult for asset owners and decision-makers to fully comprehend. Coupled with primary and n-ary interdependencies, the resulting emergent behaviors especially during states of disruption as in emergency situations presents an even greater challenge in understanding. Figure 1 provides an illustration of this connectivity.

A formal model of this infrastructure and the interrelationships is presented in the following definitions:

1. *An infrastructure network, I, is a set of nodes related to each other by a common function. The network may be connected or disjoint. It may be directional, bi-directional or have elements of both. Internal relationships/dependencies within the infrastructure I are represented by edge (a, b) with a, b* $\in I$.

2. *Given* I_i *and* I_j *are infrastructure networks,* $i \neq j$, $a \in I_i$ *and* $b \in I_j$, *an interdependency is defined as a relationship between infrastructures and represented as the edge (a,b) which implies that node b is dependent upon node a. Depending on the nature or type of the relationship, this relationship may be reflexive in that* $(a,b) \rightarrow (b,a)$.

1.3. Interdependency Types

Interdependencies can be of different types. Dudenhoeffer, Permann and Manic [5] categorize interdependencies in regards to the following types of relationships:

1.3.1. Physical Interdependencies

A physical interdependency is a requirement, often engineering reliance between components. For example: a tree falls on a power line during a thunderstorm resulting in a loss of power to an office building and all the computers inside.

1.3.2. Informational Interdependency.

An informational interdependency is an informational or control requirement between components. For example: a supervisory control and data acquisition (SCADA) system that monitors and controls elements on the electrical power grid. A loss of the SCADA system will not by itself shut down the grid, but the ability to remotely monitor and operate the breakers is lost. Likewise, this relationship may represent a piece of information or intelligence flowing from a node that supports a decision process elsewhere. An example is the dispatch of emergency services. While the responders may be fully capable of responding, an informational requirement exists as to answering where, what, and when to initiate response.

1.3.3. Geospatial Interdependency.

A geospatial interdependency is a relationship that exists entirely because of the proximity of components. For example: flooding or a fire may affect all the assets located in one building or area.

1.3.4. Policy/Procedural Interdependency.

A policy or procedural interdependency is relationship that exists between entities due to policy or procedure that relates a state or event change in one infrastructure sector

component to a subsequent effect on another component. Note that the impact of this event may still exist given the recovery of an asset. For example: after aircraft were flown into the World Trade Towers "all U.S. air transportation was halted for more than 24 hours, and commercial flights did not resume for three to four days." [6]

1.3.5. Societal Interdependency.

Societal interdependencies or influences refer to the effects that an infrastructure event may have on societal factors such as public opinion, public confidence, fear, and cultural issues. Even if no physical linkage or relationship exists, consequences from events in one infrastructure may impact other infrastructures. This influence may also be time sensitive and decay over time from the original event grows. For example: air traffic following the 9-11 attack dropped significantly while the public evaluated the safety of travel. This resulted in layoffs within the airline industry and bankruptcy filings by some of the smaller airlines [7].

1.4. Cross Sector Modeling

Critical infrastructure interdependency modeling has many of the same challenges that one can expect with any modeling and simulation domain: data accessibility, model development, and model validation. Interdependency modeling is further complicated by the extremely large and disparate cross sector analysis required. One approach is to develop multiple sector representations within on modeling and simulation framework. Examples of this approach include the search efforts currently being conduced under the CIMPA program in Australia and the CIPDSS program in the U.S. sponsored by the DHS [8]. This approach, however, does not take advantage of the many extremely detailed single sector models have been developed. One driving research question asks: "How do we leverage these existing models into a common operating picture?"

While currently no standards exist that directly address infrastructure and specifically cross sector modeling, standards do exists for exchanging information between distributed simulations. The two most common methods are the High Level Architecture (HLA) and the Distributed Interactive Simulation (DIS) frameworks.

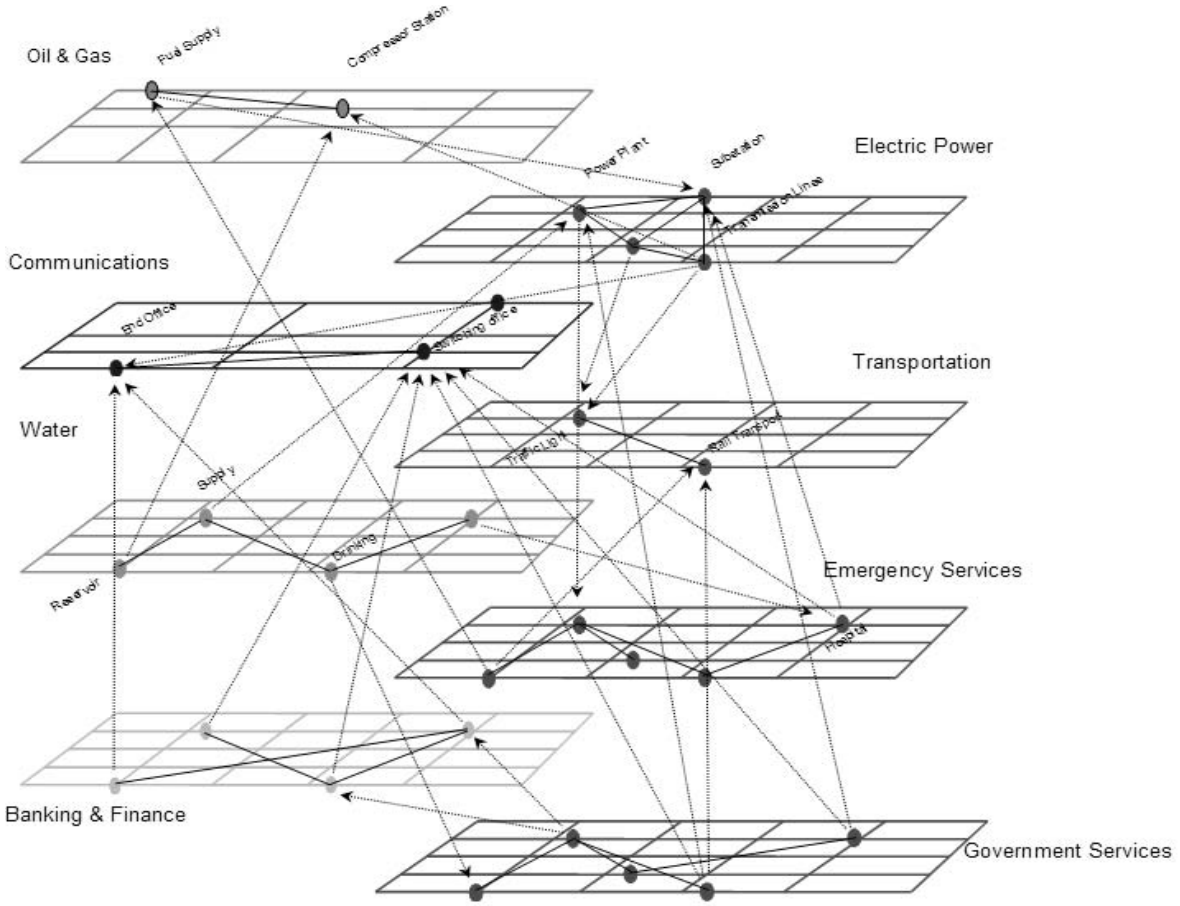

Figure 1. The interconnectivity of infrastructure sectors.

HLA, developed under the leadership of the Defense Modeling and Simulation Office is a general purpose high-level simulation architecture/framework to facilitate the interoperability of multiple types of models and simulations. The purpose of its development is to support reuse and interoperability across the large numbers of different types of simulations developed and maintained by DoD. Within HLA, simulation objects exist as federates in a larger simulation federation. HLA was approved as an open standard through the Institute of Electrical and Electronic Engineers (IEEE), IEEE Standard 1516, in September 2000.

DIS is another framework for linking real-time and potentially distributed simulations. Defined under IEEE Standard 1278, the chief objective of DIS was to create real-time, synthetic, virtual representations of the warfare environment. The simulation environment is created by interconnecting separate, distributed computers/simulators, called component simulator nodes.

Other methods of information exchange between models in either a simultaneous or batch method include the XML and GIS shape files. This method is currently used by Los Alamos National Laboratory and National Infrastructure Simulation and Analysis Center (NISAC) to relate impacts across different infrastructure models. In a broad sense, a damage profile based on expected physical damage is constructed first. An example of this is determining electrical power outage based on projected high wind profiles, surge, and flooding models associated with hurricanes. The physical impact of the event is transformed into impact on the power grid in terms of outage areas. This information is then passed to other models (water, financial, transportation, etc.) such that the corresponding impact in the electrical power sector integrates into other sectors.

2. CIMS©

The Critical Infrastructure Modeling System (CIMS©) is in ongoing development at the Idaho National Laboratory, a Department of Energy national laboratory. CIMS was developed to provide a portable and highly visual tools to identify and graphically display interdependency weaknesses and vulnerabilities to the critical portions of their infrastructure or operations. While a variety although small number of interdependency modeling tools exists, the focus and methodology of CIMS is slightly different.

CIMS© provides a high level modeling and simulation framework that permits building models "on the fly" in the event of natural disaster or emergencies. Multiple classes of models exist for emergency preparedness and response. One class of models characterized by a tremendous granularity in detail both in terms of the results and the data requirements to create the infrastructure representations. While offering a high level of precision, these models often have large computational requirements and suffer from data sensitivity. This class of models is very beneficial in data rich environments and for use in planning and pre-response. Once a disaster occurs, however, such models are often inflexible in dealing with partial information and the unknowns that most certainly arise in disaster situations. While most certainly permitting the integration so high fidelity models, CIMS© is designed to rapidly create high level models "on the fly" to adjust to damage and response profiles during an emergency. Decisions in such situation are rarely made with the luxury of complete information. The goal of CIMS© therefore is to provide a timely 70% solution from a high level state model. As an example, it may be sufficient for a decision maker to know that power is lost to a facility vice the particulars of the loss (i.e. volts, amps, etc.).

2.1. Simulation Architecture

The CIMS© architecture uses an agent-based approach to model infrastructure elements, the relations between elements, and individual component behavior. The key characteristic of the agent and the simulations is that each agent exists as an individual entity which maintains a state, senses input, and possesses rules of behavior that act upon the inputs and either modify the state or produce an output. Each network within the simulation is modeled as a connected graph, G = (N, E), where N represents the nodes within the network and E represents the edges between the nodes. Edges represent the only channel by which information or resources flow between nodes. Edges also represent the relationship, i.e. interdependencies, between infrastructures. Nodes and edges rely on present state and inputs, have their own algorithms and probabilities of action, and can be defined as having deterministic or probabilistic behaviors.

Within the CIMS© framework, one can develop high-level state models. Such models have been developed for key infrastructures such as the electrical power (transmission and distribution), transportation systems, computer networks, social networks, area demographics and key assets such as schools, government buildings, and industrial facilities. The true objective of CIMS, however, is to model the cross sector impact and not individual sector models. CIMS© contains a network architecture that permits the integration of individual sector models. This network interface is DIS compliant and can be customized for specific applications.

In the network representation, the nodes represent entities or assets of interest. The node's behaviors and dynamics may be modeled internally within CIMS©, the node may be functionally linked to an external simulation, or the node may be linked to a "live" external entity such as a sensor, a piece of equipment, or a human decision-making element. CIMS act as the linking mechanism to represent

and model the interactions between these individual sector models.

CIMS© is a discrete time step/discrete event simulation. The visualization is sequenced and updated as the simulation runs, to reveal the emergent or cascading system behaviors that develop as a result of the interdependencies between nodes. This makes the interrelationships between infrastructure networks and their consequences easy to quickly evaluate, facilitating the decision-making process. The goal of this simulation is not to produce an "exact" outcome, but to illustrate possible outcomes to enlighten the decision process.

Scenarios can be enacted through two different methods. First, to manipulate individual nodes or edges during "what if" analyses, the user can select specific nodes and edges and modify their state directly, removing or restoring capacity and watching the effect migrate through the system. Second, the user can develop baseline scripts tying together multiple events and observing the behavior. This can also be conducted in conjunction with individual node manipulation. An event manager within the simulation coordinates both internal and external event processing.

2.2. User Interface

The CIMS© framework has a native interface, Figure 2, that permits model development, simulation and analysis. The emphasis of the interface is strong user interactivity in a highly visual environment. The nodes and edges of the infrastructure network are displayed in a 3D visualization. Simple geometric represents such as spheres and lines, or tactical icons can be used to display key infrastructure elements. Colors can be associated with the state of the infrastructure elements or any other characteristic. Different infrastructures may be separated vertically in order to visually see the interconnections between them; likewise, infrastructure sectors may be further broken out. Visualization is further enhanced by the ability to incorporate potentially complex 3D objects. The model can be built upon an underlying bitmap, satellite photo, map, or chart. Nodes and edges are geo-referenced by latitude, longitude, and altitude or any other 3-dimensional representation. This structure permits the information to be quickly added to the model without the requirements of a geographic information system (GIS) database.

The network infrastructure also supports the integration of CIMS© into other visualization platforms. One such example is the integration of the CIMS© visualization into a distributed OpenSceneGraph viewer, Figure 3. CIMS© has also been integrated as a component plug in to TPS, an information aggregation and common operating picture (COP) application developed by Priority 5, Inc. TPS provides the ability to layer multiple data streams onto one functional canvas. Such data feeds include aerial imagery,

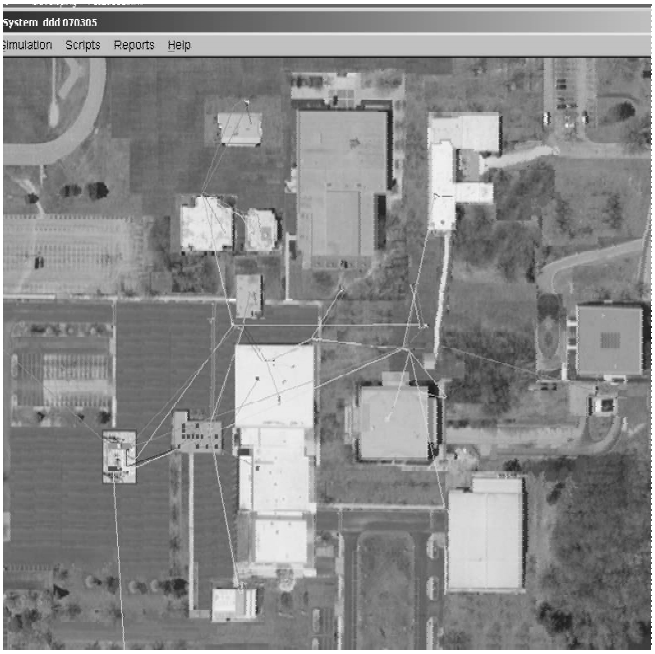

Figure 2. The native CIMS user interface illustrating a model of a mock facility.

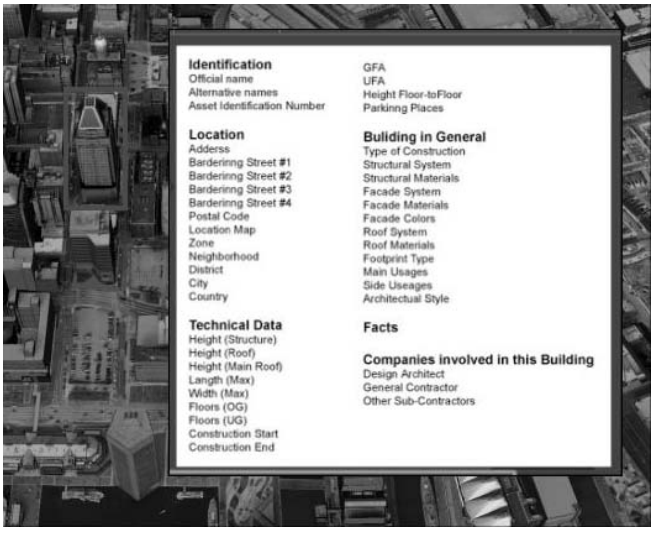

Figure 3. CIMS© possess the ability to select simulation entities and attach key information.

3D landscapes, critical asset databases, road and rail networks, network sensors, and live weather feeds. In this application, CIMS© sits as a layer onto of the steaming data. Thus, one is able to run a simulation on top of potentially real time data feeds. This provides the ability to conduct rapid planning for dynamic situations and simulate potential course of action against current state information.

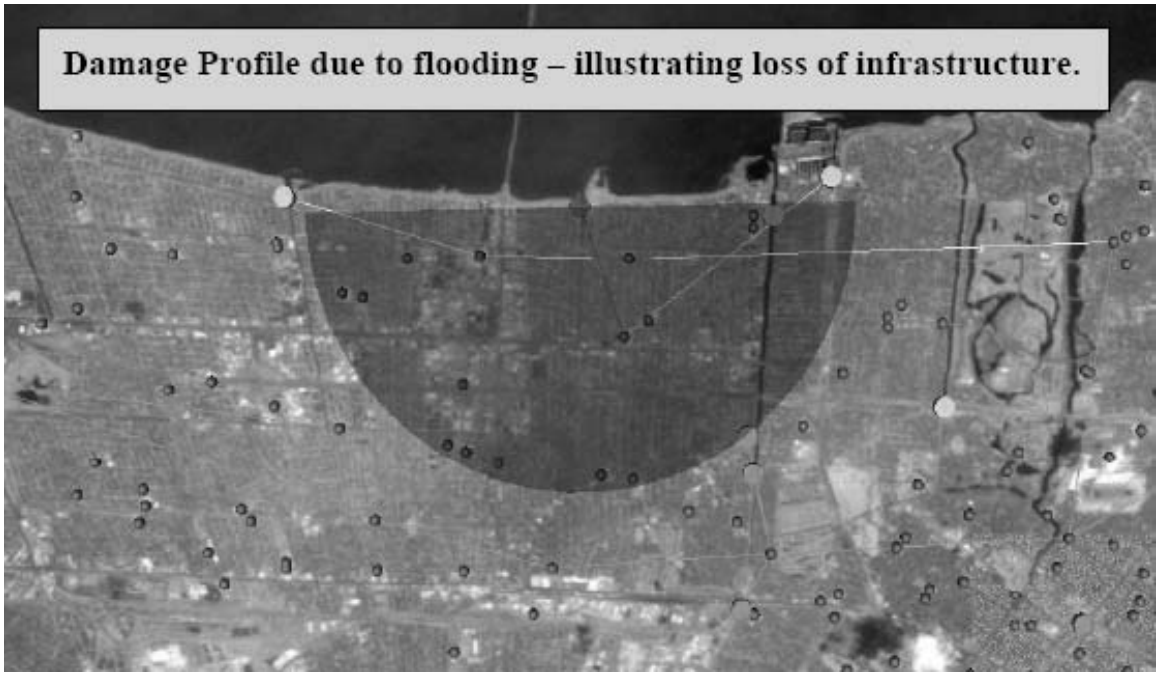

Figure 4. A model illustrating the infrastructure effect from a hypothetical flooding event.

2.3. New Orleans Model

Figure 4 shows both the impact of flooding on infrastructure components and the resulting cascading effects. This particular demonstration was developed to illustrate the power of CIMS© in assisting in New Orleans restoration planning activities. In this case, infrastructure planning issues included but are not limited to: high value assets near levees, low lying roadways, water removal capability, water removal pump power sources, and evacuation and access routing. Figure 4 illustrates an impact zone for one of the flooding scenarios. Here the electrical power grid is modeled with an evaluation of its loss. Key assets include schools, government facilities, hospitals, and water pumping stations. Red colored assets illustrate flooding damage. Yellow represents a loss of power to key pumping stations. The loss of electrical power which led to the loss of water pumping stations was a significant factor inhibiting dewatering thus recovery/restoration activities.

3. DECSION SUPPORT

Modeling and simulation of impacting events and infrastructure consequence is only part of the overall operational support system. Another key component is decision support. The following sections describe the adaptation of CIMS© with other analytical methods to support and enhance decision-making capability.

3.1. Mission Assurance

The discussion above referred to the modeling of physical assets in terms of nodes and edges. Another aspect that can be modeled is the concept of mission assurance. Mission success is based upon the ability to execute specific functionality. Mission assurance includes the analysis of risk and impact that events place upon such capabilities. When faced with an incident or event, this type of analysis is essential in answering the high level questions:

- How does the event affect mission capability?
- What is the set of potential actions necessary to adapt and mitigate the effects?

In this extension, a "mission" node is created. The output of this node is the base-functionality of the mission. Input to the node consists of all the supporting elements required to provide that functionality. Consider a key manufacture in the defense industrial base (DIB) whose function f_{ij} is the manufacturing of a special widget. This functional capability becomes the real interest and is modeled as a node. Dependencies for example could include raw materials, the supply line for raw materials, electrical power, water, a specialized worker force and the supporting work force. Each of these inputs or dependent elements may have different weightings in terms of mission impact. Figure 5 illustrates this concept.

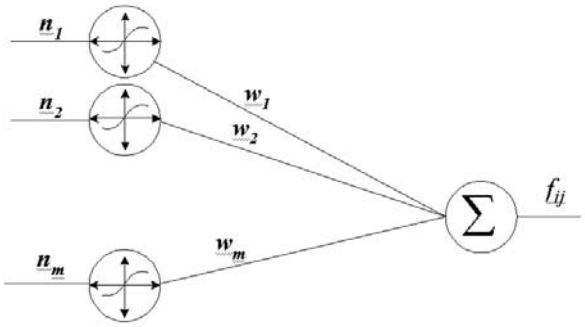

Figure 5. Modeling mission capability as the weighted functions of dependent nodes.

3.2. GACIA

GACIA, or the Genetic Algorithms for Critical Infrastructure Analysis, is an active research program at the Idaho National Laboratory being conducted for the U.S. Air Force Research Laboratory. The object of the project is to utilize genetic algorithms to search the complex topography of the problem space in CIMS© to identify potential solutions against specific cost functions. This integration was achieved by allowing the GA to access and affect the simulation agents' attribute and state values [9].

This GA is being developed for integration with CIMS© to determine the optimal infrastructure assets to protect from attack or restore in a disaster situation. This will define the critical sub-network for the infrastructure of concern given information such as:

- List of critical assets;
- Relative importance of each infrastructure asset;
- Cost to protect the individual assets;
- Cost to repair the individual assets;
- Cost to destroy the individual assets; and
- Time to repair the individual assets.

The GA uses this information to evaluate the resilience of infrastructure configurations by using methods such as disabling arbitrary assets and letting the infrastructure stabilize through the CIMS© simulation. This can assist decision makers in determining the optimum (or ranking of) assets to restore or protect from attack or other disaster.

The goal of this research is to address the following areas:

- Identify the critical sub-network(s) (i.e. the sub-graph(s) of the graph G whose elements include only those assets required to sustain a set of critical assets or specific functionality);
- Identify potential damage mitigation actions: i.e. which nodes can be protected before attack/accident/natural disaster, or which nodes should be restored first after the event; and
- Identify weaknesses in the network.

GA population bit arrays are constructed in which each bit represents the state value corresponding to each infrastructure asset being modeled in CIMS©. A "0" indicates that the asset is nonfunctional; a "1" indicates that it is operational. Figure 6 illustrates the linkage between the GA chromosome and the simulation model. A population of these bit arrays is "born" and then evolved over multiple generations to identify and rank potential solution sets against the fitness function. The GA identifies over multiple generations the asset combination that contains the most critical assets (as defined) along with those assets necessary to support them. The GA is combined with the CIMS© simulation to assist in the analysis of this complex and non-linear of the problem space.

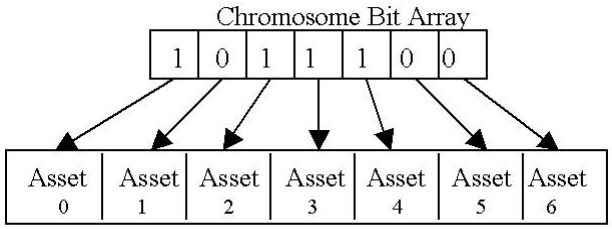

Figure 6. The association of individual asset (node) state with the bits in a GA chromosome.

3.3. DeSuSCIA

DeSuSCIA, or the Decision Support System (DSS) for Critical Infrastructure Analysis, is also an active research program at the Idaho National Laboratory being conducted for the U.S. Air Force Research Laboratory. The object of the project is to employ multiple criteria multiple alternative (MCMA) DSS algorithms to perform weighted ranking of critical sub-network, generated through data mining by GACIA. Figure 7 shows the webe interface for DeSuSCIA.

As GAs typically produce a near-optimum solution, as a result of each run of GACIA, a similar but slightly different sub-network of concern for the infrastructure will be identified. Therefore, a finite set of alternative sub-networks will emerge as a result of the cross-over and mutation of consecutive generations of vectors representing various infrastructure assets. Although any of alternative network from this finite set of sub-networks is of concern, further refinement through ranking via a MCMA DSS (DeSuSCIA) identifies the most critical among all previously sub-networks data mined by GACIA. In addition to top ranked critical network, all other network will be ranked according to their criticality.

The set of criteria for determining a top critical sub-network is similar to the information used by GACIA (critical assets, importance of each infrastructure asset, cost to protect, repair, and destroy those assets, and the time to repair individual assets).

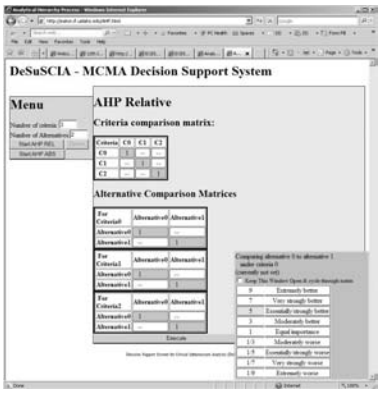

Figure 7. The web interface of the DeSuSCIA application

4. CONCLUSION

The purpose of this paper has been to present the concept of infrastructure interdependency modeling as a needed component in emergency planning and preparation. In addition, a modeling and simulation package called CIMS© has been described which permits provides a integrating framework for pulling together cross-sector models into a single federation. Also discussed was the concept of coupling decision support tools directly with the simulation to harness the power of multiple tools in enhancing coarse of action analysis for the decision makers.

The CIMS© software represents one approach to this difficult and complex problem space. The key concepts to derive from this paper are the need for understanding of the interrelationships between infrastructure sectors and the needs to couple infrastructure and emergency response tools to reflect the interconnectivity of today's environment.

ACKNOWLEDGMENTS

The CIMS© software was prepared by Battelle Energy Alliance, LLC under Contract No. DE-AC07-05ID14517 with the U. S. Department of Energy. The United States Government is granted for itself and others acting on its behalf a non-exclusive, paid-up, irrevocable worldwide license in this software to reproduce, prepare derivative works, and perform publicly and display publicly, by or on behalf of the Government.

Part of the power of the CIMS© software is the flexibility to integrate multiple images and data sets. Pictometry International Corp., www.pictometry.com, a world leader in digital, oblique aerial imaging, provided visual imagery and 3D models for the model of Baltimore shown in Figures 3.

Reference List or References

1. United States Congress, "U.S.A. Patriot Act", 2001, http://www.epic.org/privacy/terrorism/hr3162.html
2. Ibid.
3. Office Of Homeland Security, "National Strategy for Homeland Security, 2002, p. 30.
4. Mussington, D., "Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development." RAND:Science and Technology Institute, Santa Monica, CA, 2002, p 29..
5. Dudenhoeffer, D., M. Permann, and M. Manic, , "CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis", *Proceedings of the 2006 Winter Simulation Conference,* IEEE, December 2006, pp 478– 485.
6. U.S. Department Of Energy Office Of Critical Infrastructure Protection, "Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center A Case Study, November 8, 2001", p. 3.
7. Ibid.
8. Pederson, P., D. Dudenhoeffer, S. Harley, and M. Permann, "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research", https://www.pcsforum.org/library/files/1159904563-TSWG_INL_CIP_Tool_Survey_final.pdf, INL/EXT-06-11464, Idaho Falls ID, August 2006.
9. M. Permann, "Genetic Algorithms for Agent-Based Infrastructure Interdependency Modeling and Analysis", Proceedings of Spring Simulation Multiconference 2007, SCS, March 2007.

Biography

DONALD D. DUDENHOEFFER is research scientist for INL in Idaho Falls, ID. He received his Masters of Science degree in Operations Research from the Naval Postgraduate School in 1994. His research interests include critical infrastructure modeling and simulation, military operations, command and control.

MILOS MANIC is the Graduate and Undergraduate Program Coordinator for the CS & ECE program, Center for Higher Education of University of Idaho at Idaho Falls, and an Assistant Professor at the Computer Science Dept., teaching graduate courses and workshops. He holds a Ph.D. in Computer Science from University of Idaho Boise and a Masters in Electronic Engineering and Computer Science from University of Nis. His research interests include artificial intelligence, decision support systems, and software reliability.

MAY R. PERMANN is a research scientist at the INL in Idaho Falls, ID. She received her B.S. in Computer Science from Idaho State University. Her research interests include Cyber Security with a focus on SCADA systems, high performance computing (HPC) and GAs.