LA-UR-05-1870

Approved for public release;
distribution is unlimited.

Title: Critical Infrastructure Protection Decision Support Syster (CIP/DSS) Project Overview

Author(s):
Brian B. Bush,
Lori R. Dauelsberg,
Rene J. LeClaire,
Dennis R. Powell
and
Sharon M. DeLand, Sandia National Laboratories
Michael E. Samsa, Argonne National Laboratory

Submitted to:
2005 International System Dynamics Conference
July 17-21, 2005
Boston, MA

Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview

B. Bush, L. Dauelsberg, R. LeClaire, D. Powell,
Los Alamos National Laboratory
P.O. Box 1663
Los Alamos, NM 87545
(505) 667-6485
bwb@lanl.gov, lorid@lanl.gov, rjl@lanl.gov, drpowell@lanl.gov

S. DeLand
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185
(505) 845-0011
smdelan@sandia.gov

M. Samsa
Argonne National Laboratory
9700 S. Cass Avenue
Argonne, IL 60439
(630) 252-2000
msamsa@anl.gov

Abstract

The Critical Infrastructure Protection Decision Support System (CIP/DSS) simulates the dynamics of individual infrastructures and couples separate infrastructures to each other according to their interdependencies. For example, repairing damage to the electric power grid in a city requires transportation to failure sites and delivery of parts, fuel for repair vehicles, telecommunications for problem diagnosis and coordination of repairs, and the availability of labor. The repair itself involves diagnosis, ordering parts, dispatching crews, and performing work. The electric power grid responds to the initial damage and to the completion of repairs with changes in its operating characteristics. Dynamic processes like these are represented in the CIP/DSS infrastructure sector simulations by differential equations, discrete events, and codified rules of operation. Many of these variables are output metrics estimating the human health, economic, or environmental effects of disturbances to the infrastructures.

Key Words: *critical infrastructure; consequence models; national security.*

Introduction

In the current and future cyber and physical threat environment, the United States needs a comprehensive approach to security for its critical infrastructure using vulnerability, consequence, and risk analyses. The approach must address uncertain and evolving threats, consider a wide variety of assets and infrastructures, and use consistent methodologies and criteria. The Critical Infrastructure Protection (CIP) Program sponsored by the U.S. Department of Homeland Security (DHS) has three primary goals:

1. Develop, implement, and evolve a rational approach for prioritizing CIP strategies and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks;
2. Propose and evaluate protection, mitigation, response, and recovery strategies and options; and
3. Provide real-time support to decision makers during crises and emergencies.

Decision makers need to understand the consequences of policy and investment options before they enact solutions, particularly for the highly complex alternatives available for protecting our nation's critical infrastructures in today's threat environment. The most effective way to examine tradeoffs between the benefits of risk reduction and the costs of protective action is to utilize a decision support system that incorporates threat information, vulnerability assessments, and disruption consequences in quantitative analyses through advanced modeling and simulation. Government (federal, state, local) and industry decision makers can make use of such a decision support system to prioritize protection, mitigation, response, and recovery strategies as well as to support red-team exercises and provide support during crises and emergencies.

A system dynamics modeling, simulation, and analysis approach is used to conduct consequence assessments and risk analyses (based on realistic threats, system/infrastructure vulnerabilities for the threats, and resulting consequences). These methodologies will allow decision makers to prioritize and invest scarce resources and to implement rational strategies for protection of various systems and infrastructures based on objective and dynamic modeling, simulation, and analysis.

Table 1. Infrastructures & Assets

Critical Infrastructures

1. Agriculture and Food
2. Water
3. Public Health
4. Emergency Services
5. Government
6. Defense Industrial Base
7. Information and Telecommunications
8. Energy
9. Transportation
10. Banking and Finance
11. Chemical Industry and Hazardous Materials
12. Postal and Shipping

Key Asset Categories

13. National Monuments and Icons
14. Nuclear Power Plants
15. Dams
16. Government Facilities
17. Commercial Key Assets

Goals

The Critical Infrastructure Protection Decision Support System (CIP/DSS) project is developing a risk-informed decision support system that provides insights for making critical infrastructure protection decisions by considering all seventeen critical infrastructures [1-3] (see Table 1) and their primary interdependencies. Initiated as a proof-of-concept in August 2003, the CIP/DSS project completed a prototype model and two case studies in February 2004. It

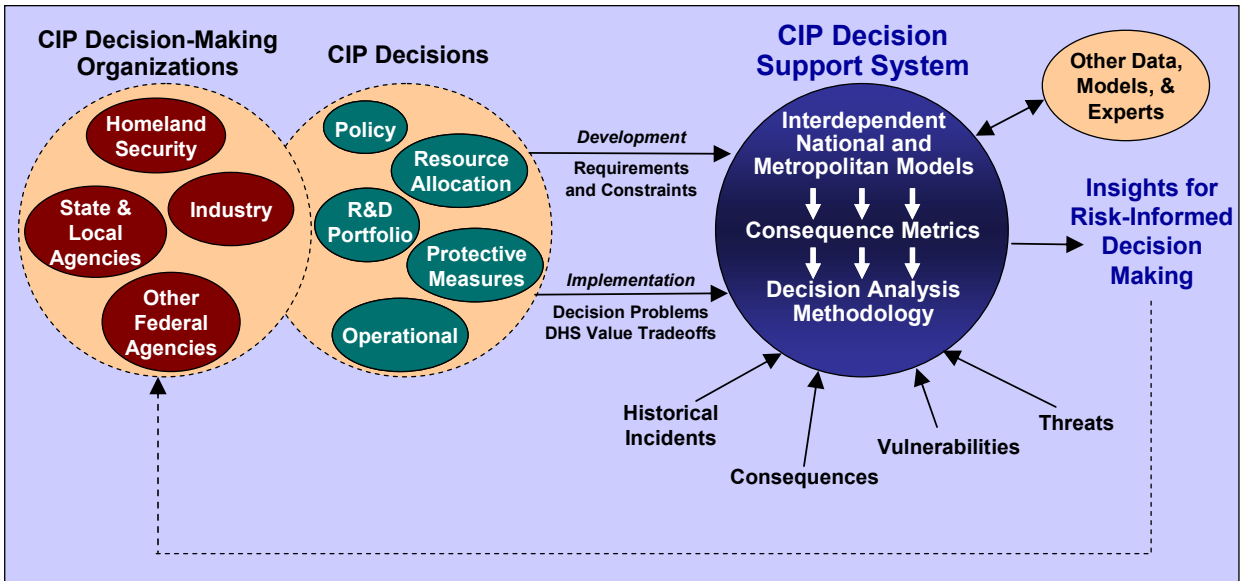

Figure 1. Relationship between CIP decision makers, decisions, and the CIP/DSS.

demonstrated how the CIP/DSS will assist decision makers in making informed choices by (i) functionally representing all fourteen critical infrastructures with their interdependencies, (ii) computing human health and safety, economic, public confidence, national security, and environmental impacts, and (iii) synthesizing a methodology that is technically sound, defensible, and extendable. Examples of questions that this decision support system is designed to address include:

- What are the consequences of attacks on infrastructure in terms of national security, economic impact, public health, and conduct of government—including the consequences that propagate to other infrastructures?
- Are there choke points in our Nation's infrastructures (i.e., areas where one or two attacks could have the largest impact)? What and where are the choke points?
- Incorporating consequence, vulnerability, and threat information into an overall risk assessment, what are the highest risk areas?
- What investment strategies can the U.S. make that will have the most impact in reducing overall risk?

Figure 1 emphasizes that the CIP/DSS supports a variety of decision makers and types of decisions, and leverages external knowledge, databases, and analysis tools.

Architecture

The decision support system includes consequence models for all the critical infrastructures, which are linked via their strongest interdependencies and coupled between the national and the metropolitan scales (see Figure 2). The accurate representation of interdependencies among infrastructures comprises the most unique feature of the CIP/DSS models: the system can track the propagation of a disturbance in the telecommunications sector, for instance, into the energy, banking, and government sectors. Moreover, respecting the differing national and metropolitan

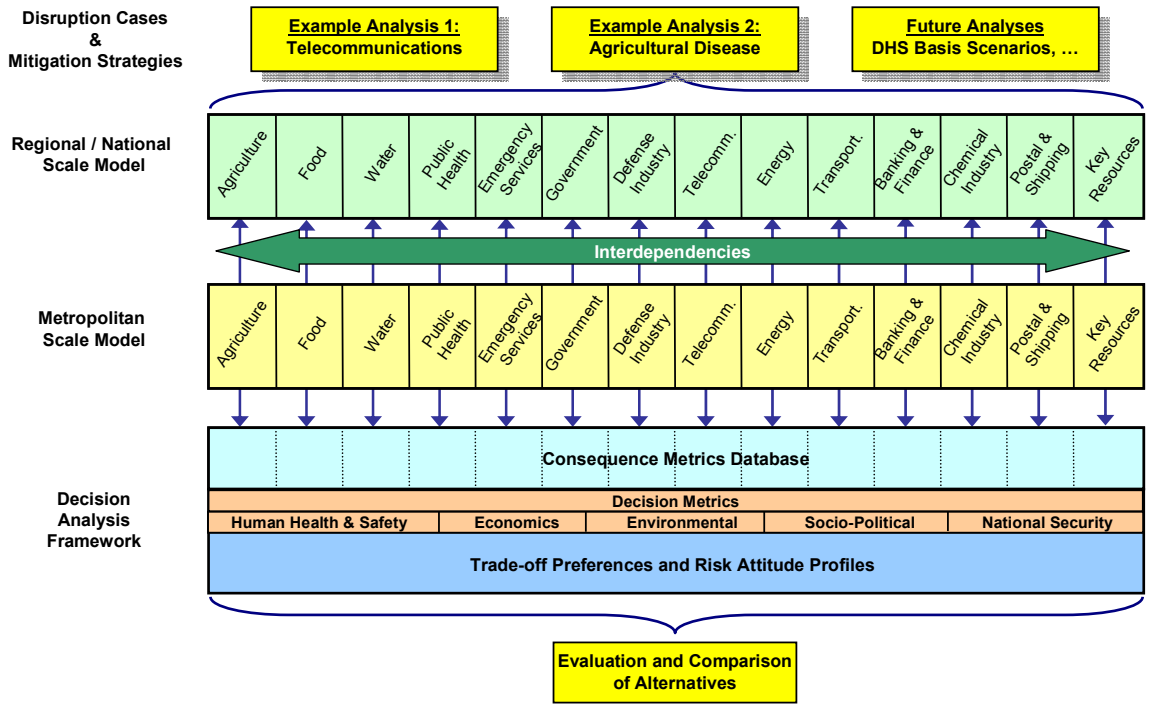

Figure 2. CIP/DSS architecture.

aspects of most infrastructures allows the CIP/DSS to resolve both inter-regional and intra-urban effects: some incidents, for example, might involve either localized effects or broad national impacts. The outputs of the consequence models are captured in a consequence database from which "decision metrics" tuned to particular decision-maker profiles are computed. Multi-attribute utility functions determined from interviews with decision makers are used to compare alternative infrastructure protection strategies and help build consensus among stakeholders in a decision.

The national and metropolitan consequence models are implemented using Vensim™ which reads input parameters from and writes output time series to an Oracle™ relational database of "consequence" metrics, which are abstracted into a much smaller set of "decision" metrics. The decision support software (written in Visual Basic™) access the decision database to compute utility values for various scenarios and alternatives.

Consequence Models

The consequence models simulate the dynamics of individual infrastructures and couple separate infrastructures to each other according to their interdependencies. For example, repairing damage to the electric power grid in a city requires transportation to repair sites and delivery of parts, fuel for repair vehicles, telecommunications for problem diagnosis and coordination of repairs, and the availability of labor. The repair itself involves diagnosis, ordering parts, dispatching crews, and performing repairs. The electric power grid responds to the initial damage and to the completion of repairs with changes in its operating capacity (the number of

megawatts that can be distributed to customers). Dynamic processes like these are represented in the CIP/DSS infrastructure sector simulations by differential equations, discrete events, and codified rules of operation. Figure 3 outlines the influences that generally are implemented in the critical infrastructure models.

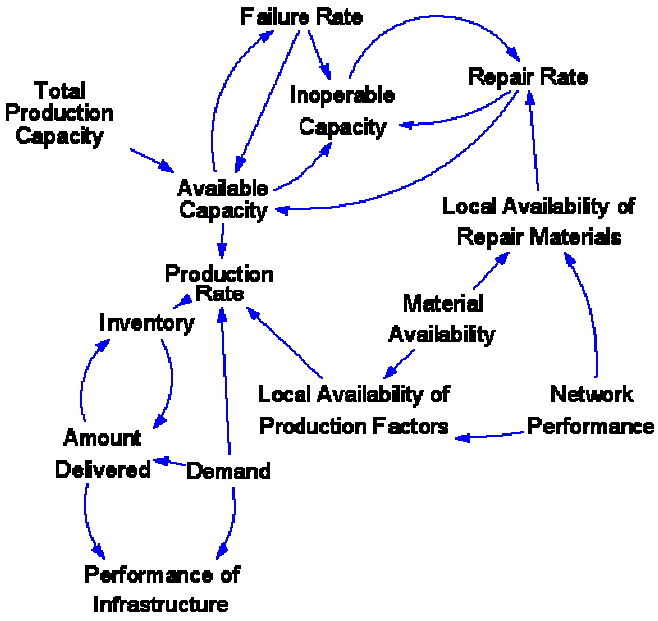

Figure 3. Generic influences in CIP/DSS critical infrastructure models.

Each critical infrastructure sector is divided into a number of "subsectors" which have a more uniform character and for which separate Vensim™ views are developed. For example, the emergency services sector is divided into (i) fire services, (ii) emergency medical services, (iii) law enforcement, and (iv) emergency support services. A custom-built Vensim™ model "linker" is used to assemble a unified multi-sector model from individual files each containing a single sector model: the linker identifies "shadow variables" present in models with dependencies on other sectors and resolves the references when the models are combined. This allows the development and testing of models at the sector level, but run analyses at the multi-sector level.

The CIP/DSS metropolitan model currently has about 4500 variables (see Table 2), including about one hundred interdependencies between subsectors (see Figure 4). In most cases these are "pure" systems dynamics models, but we have implemented discrete event or rule-based models for portions of several subsectors. The CIP/DSS national model has a similar size and complexity.

Table 2. Count of Vensim™ variables in metropolitan CIP/DSS consequence models.

Sector	*Count*
Agriculture	10
Banking and Finance	251
Chemical Industry and Hazardous Materials	42
Emergency Services	521
Energy	802
Food	373
General Urban	444
Global Data	29
Government	54
Information and Telecommunications	237
Key Assets	72
Postal and Shipping	43
Public Health	325
Scenario	925
Transportation	208
Water	156
Total	***4482***

Decision Support

The CIP/DSS team has conducted on ongoing series of formal and informal interviews of CIP decision makers and stakeholders in order to identify requirements for the decision support system, scope out the decision environment, and quantify the prioritization of consequences. The taxonomy of decision metrics derived from this research involves six categories: (i) sector-

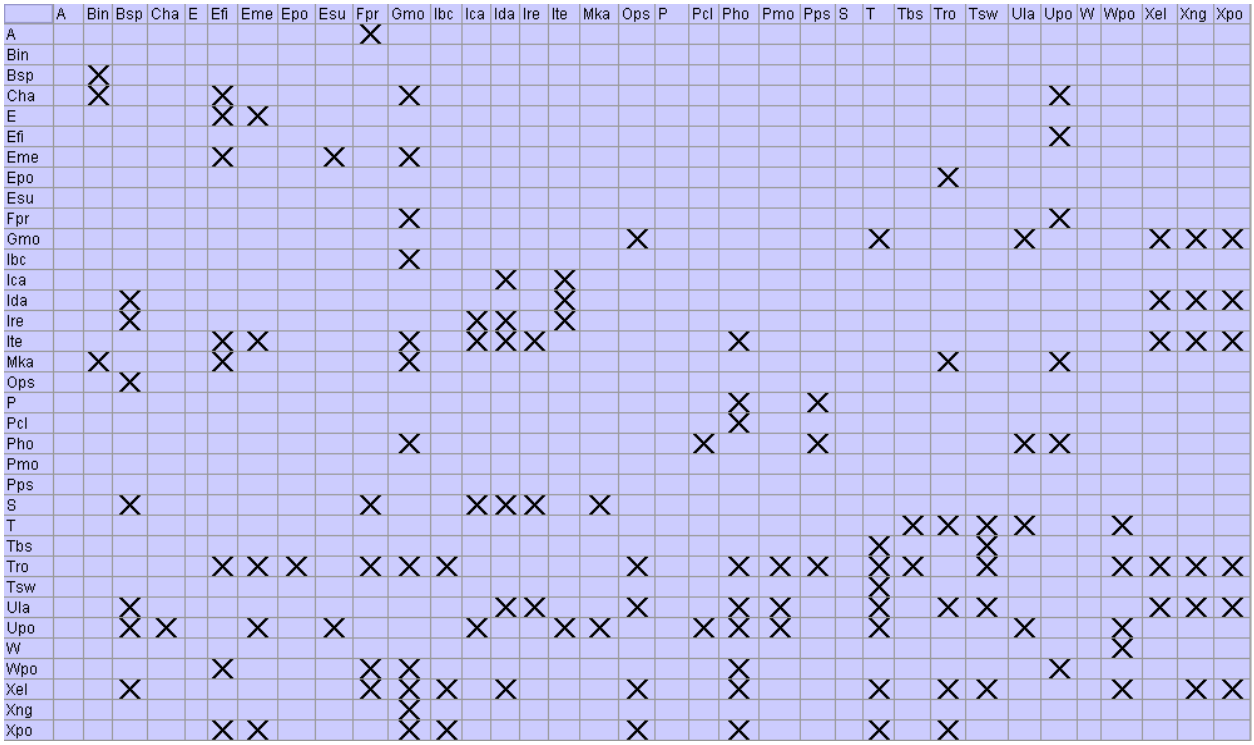

Figure 4. Subsector interdependency matrix for the metropolitan models in the CIP/DSS prototype: The critical infrastructure subsectors represented as columns have one or more functional dependency upon the subsector represented as rows. The subsector abbreviations are: *A*=Agriculture; *Bin*=Insurance; *Bsp*=Spending; *Cha*=Hazardous Materials; *E*=Emergency Services; *Efi*=Fire Services; *Eme*=Emergency Medical Services; *Epo*=Law Enforcement; *Esu*=Emergency Support Services; *Fpr*=Food Processing; *Gmo*=Government Monitoring; *Ibc*=Broadcast; *Ica*=Phone Calls; *Ida*=Data Networks; *Ire*=Telecommunication Repair; *Ite*=Telecommunications; *Mka*=Key Assets; *Ops*=Postal; *P*=Public Health; *Pcl*=Clinics; *Pho*=Hospitals; *Pmo*=Mortuaries; *Pps*=Pharmaceutical Supply; *S*=Scenario; *T*=Transportation; *Tbs*=Bus; *Tro*=Road; *Tsw*=Subway; *Ula*=Labor; *Upo*=Population; *W*=Water; *Wpo*=Potable Water; *Xel*=Electricity; *Xng*=Natural Gas; *Xpo*=Petroleum, Oil, and Lubricants.

specific, (ii) human health and safety—public and occupational fatalities, non-fatal injuries, illnesses, (iii) economic—immediate and interdependent costs of event, including the implementation and operating cost for optional measures, (iv) environmental—air and water emissions, non-productive land, and intrinsic value loss, (v) socio-political—perceived risk, public confidence, trust in government sector-specific effects, and market confidence, and (vi) national security—continuity of military and critical civilian government services. The preferences for three representative decision makers were encoded using structured interview techniques to arrive at multi-attribute utility functions consonant with the output of the consequence models and applicable to the case studies described below.

The primary building block for decision analysis in CIP/DSS is called a case. A case consists of consists of two or more scenario pairs; each scenario pair is composed of a *readiness scenario* and an *incident scenario*:

- *Base Scenario Pair*
  - *Base Readiness Scenario:* Business as usual conditions; consequences in the absence of terrorist events or other disruptions.
  - *Base Incident Scenario:* Postulated event occurs with no additional optional measures implemented, beyond what exists at the time.
- *One or more Alternate Scenario Pair(s)*
  - *Alternate Readiness Scenario:* A specific set of additional optional measures are in place; postulated event is not initiated.
  - *Alternate Incident Scenario:* Optional measures are in place; postulated event occurs.

Comparison of alternate scenario pairs with base scenario pairs indicates the effects that various investments and strategies, labeled here as optional measures (which include hardware, processes and strategies related to prevention, protection, mitigation, response, and recovery), could have if they were implemented by decision makers. Each scenario requires a separate simulation over a period of time (defined by the case) with the detailed national and metropolitan models.

Case Studies

The prototype CIP/DSS was exercised in two proof-of-concept case studies that demonstrated the project's feasibility. One case study—chosen to test the depth of representation in a few infrastructure sectors—involved an agricultural pathogen that affected the food chain and involved regional transportation quarantines. The other case study—chosen to broadly perturb many infrastructure sectors—involved a telecommunications disruption that degraded the operation of other infrastructure sectors. Decision metrics and utility values were computed for several investment alternatives that would mitigate the impact of the incidents.

For the telecommunications case study, we looked at two optional measures: (1) improve the restoration capability of the system, and (2) consolidate the targeted facilities away from dense urban areas. The former alternative was expected to reduce the secondary economic impact of the incident, while the latter alternative was expected to reduce the impact on human health and safety. Figure 5 illustrates how a risk-neutral decision maker would prefer no action so long as the annual likelihood of the event is less than one incident in 13 years. When the likelihood is between 1 in 13 years and 1 in 5 years that decision maker would prefer to improve the restoration capability; when the likelihood is greater than 1 in 5 years, that decision maker would prefer to consolidate facilities. The relative preferences are determined by the form of the decision maker's multi-attribute utility function.

Table 3. Standard incident categories.

- Biological
- Chemical
- Radiological
- Nuclear
- Explosive
- Physical Assault
- Insider
- Cyber
- Disaster
- Accident

We are also involved in a series of case studies to support decision making relative to a standardized set of scenarios defined by DHS (see Table 3). The first of these involves an infectious disease scenario with influence outlined in Figure 6. In addition to the propagation of the disease among the human population (simulated via an SEIR model), we model the use of hospital resources (beds, vaccines, staff), activities of emergency services personnel, quarantine strategies, reduced workforce

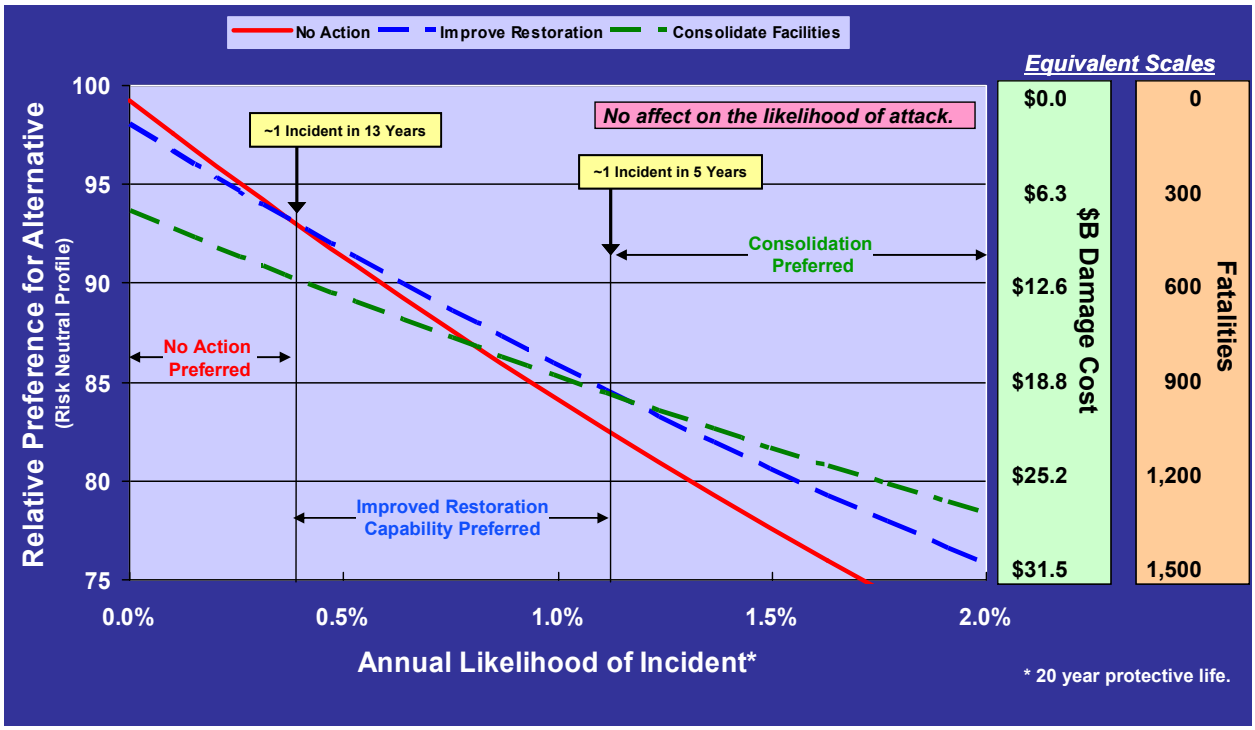

Figure 5. Tradeoff between alternative for improved restoration capability versus facility consolidation for telecommunications case study.

availability, and transportation system shutdowns. The overall case study process is outlined in Figure 7.

Ongoing Work

The CIP/DSS team is now focusing on building confidence in the initial prototype through the use of sensitivity studies, the modeling of historical incidents, and the broader involvement of stakeholders and domain experts. The architecture is also being broadened to account for general threats to critical infrastructures.

Acknowledgements

The CIP/DSS project is a tightly integrated joint effort of Argonne National Laboratory, Los Alamos National Laboratory, and Sandia National Laboratories, sponsored by the Science & Technology Directorate of the U.S. Department of Homeland Security. For more information please contact John Hoyt at John.Hoyt@DHS.GOV or (202) 254-6037.

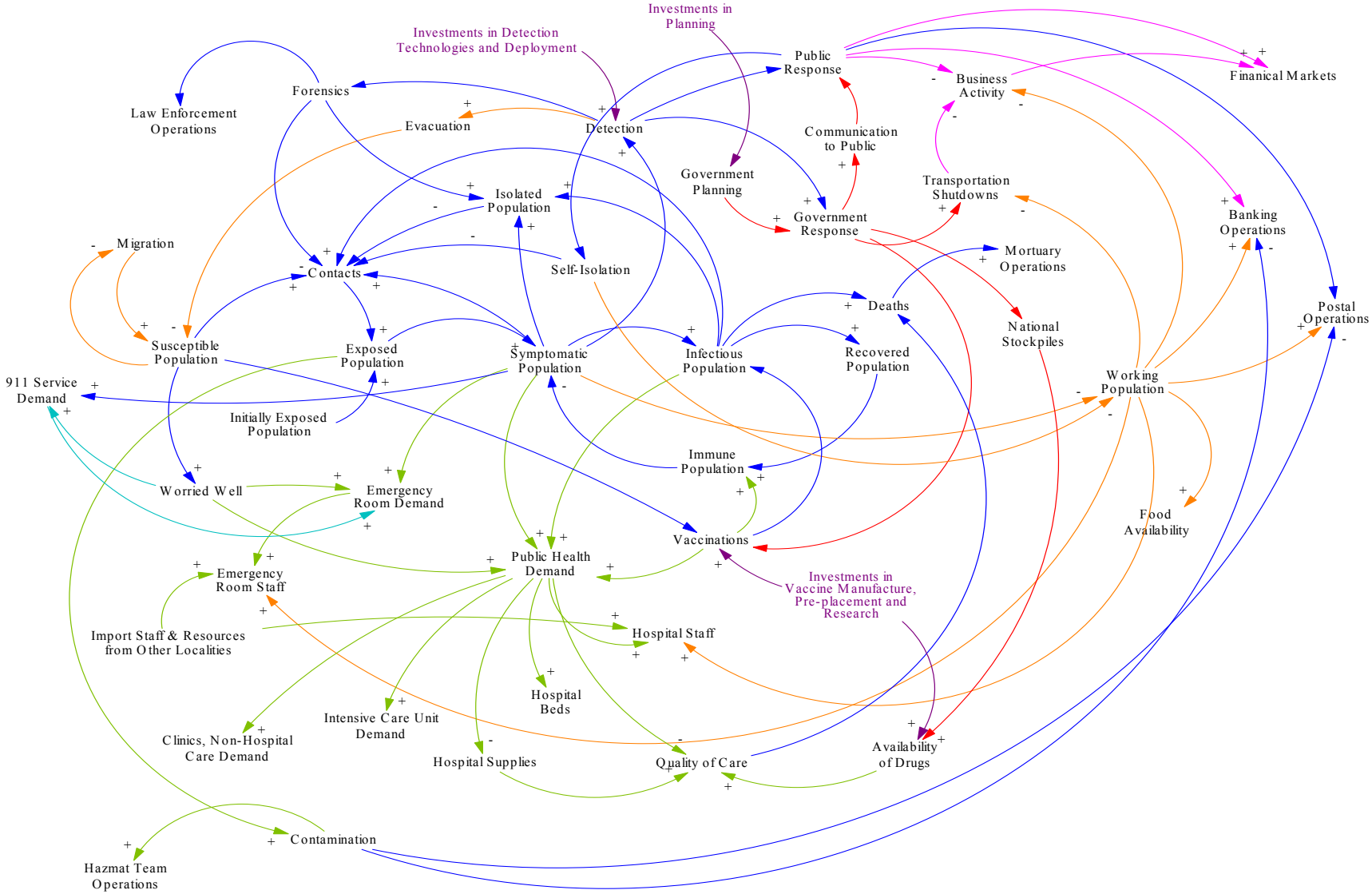

Figure 6. Influence diagram for cascading effects of infectious disease through critical infrastructures.

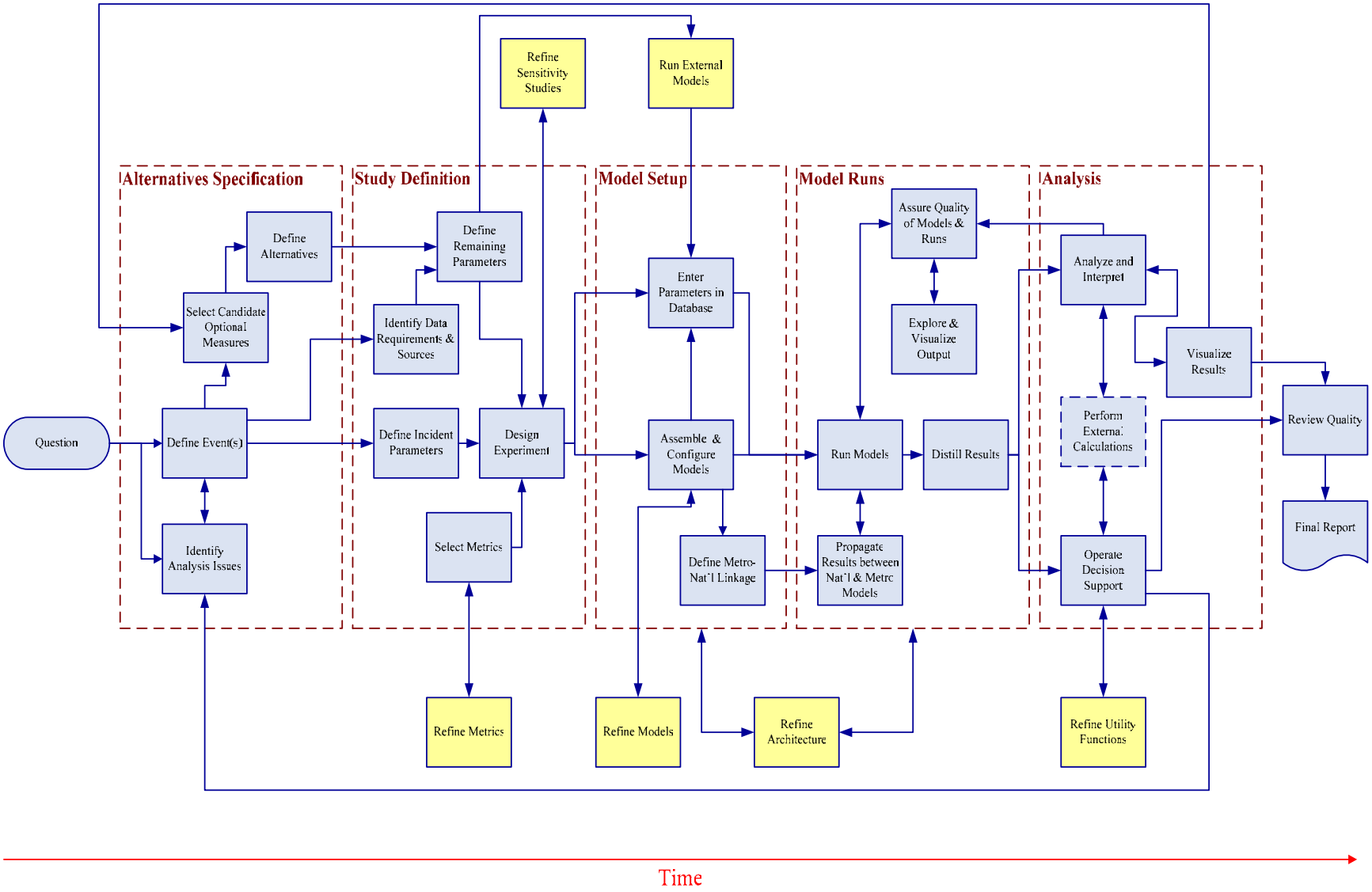

Figure 7. CIP/DSS case study process diagram.

References

[1] United States of America. Executive Office of the President. Critical Infrastructure Protection, Presidential Decision Directive (PDD) 63. N.p.: n.p., 1998.

[2] United States of America. Executive Office of the President. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. N.p.: n.p., 2003.

[3] United States of America. Executive Office of the President. Homeland Security Presidential Directive – 7 Critical Infrastructure Identification, Prioritization, and Protection. N.p.: n.p., 2003.