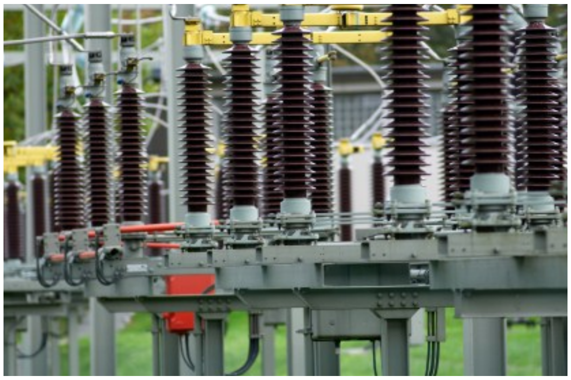


A REGIONAL RESILIENCE/SECURITY ANALYSIS PROCESS FOR THE NATION'S CRITICAL INFRASTRUCTURE SYSTEMS

DECEMBER 2011

ASME INNOVATIVE TECHNOLOGIES INSTITUTE, LLC

Prepared in fulfillment of Subcontract 4000100594 between UT-Battelle, LLC, operator of Oak Ridge National Laboratories, and ASME Innovative Technologies Institute, LLC.

This material is based upon work supported by the U.S. Department of Homeland Security under U.S. Department of Energy Interagency Agreement 43WT10301. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

ASME INNOVATIVE
TECHNOLOGIES
INSTITUTE, LLC

A REGIONAL RESILIENCE/SECURITY ANALYSIS PROCESS FOR THE NATION'S CRITICAL INFRASTRUCTURE SYSTEMS

Jerry P. Brashear, Ph.D.
Principal Investigator
Senior Fellow, ASME-ITI
The Brashear Group, LLC

J. Reese Meisinger
President, ASME-ITI

James T. Creel
Project Manager, ASME-ITI

Gretchen Crutchfield,
Project Specialist, ASME-ITI

Theodore W. Hamilton
Research Associate, ASME-ITI

Kevin Heaslip, Ph.D.
Alion Science and Technology

Frederick Krimgold, Ph.D.
Virginia Tech

William Louisell, Ph.D.
Alion Science and Technology

Adam Rose, PhD
University of Southern California

Joost Santos, Ph.D.
George Washington University

Prepared in fulfillment of Subcontract 4000100594 between UT-Battelle, LLC, operator of Oak Ridge National Laboratories, and ASME Innovative Technologies Institute, LLC.

DECEMBER 2011

ACKNOWLEDGEMENTS

This is the report of the first phase of a project that was designed for three to four years. In the first year, its objective was to test the feasibility of developing a business process to analyze regional risk and resilience. Feasibility is demonstrated in this report by describing and exemplifying the process. The later years of the project were designed to move from feasibility to a fully operational, automated and user-friendly process tested in the field. Discussions on next steps will be explored.

The U.S. Department of Homeland Security Science & Technology Directorate, Infrastructure and Geophysical Division, headed by Christopher Doyle, financially supported this project. The insight into urban and infrastructure resilience and encouragement offered by Chris and his staff, especially Michael Matthews and Dr. Mary Ellen Hynes, were invaluable in initiating the project.

The Southeast Region Research Initiative (SERRI), part of the Oak Ridge National Laboratory, under the direction of Warren Edwards, provided funding, direction, contract management and ample assistance for the project. He and his staff, especially David Landguth and David Lannom, were highly instrumental to developing on-site opportunities and day-to-day guidance. It is prepared in fulfillment of Subcontract 4000100594 between UT-Battelle, LLC, operator of Oak Ridge National Laboratories, and ASME Innovative Technologies Institute, LLC (ASME-ITI).

This project was part of a program of R&D by ASME-ITI, as a contribution to homeland security everywhere, which began shortly after September 11, 2001. The program consisted of a series of projects that produced and tested the RAMCAP process, tailored it to eight sectors and an American National Standard (with the American Water Works Association), a feasibility study of using financial portfolio techniques for infrastructure investments, and culminated in the present project. With this demonstration of the scalability of the RAMCAP concept and the feasibility of the regional business process, ASME-ITI's parent, the American Society of Mechanical Engineers, has concluded the program has fulfilled its objectives and, accordingly, is leaving the field of infrastructure and regional and resilience.

The authors wish to express their deep gratitude to the personnel of infrastructures, cities and regions who have allowed the process to be tested in their communities. These include the National Capital Region (the District of Columbia, Virginia, Maryland and the counties and cities within the region); Danville, VA; Hampton Roads, VA (the cities and counties around the mouth of the Chesapeake Bay); the Metropolitan Government of Nashville and Davidson County, TN; and to the numerous utilities and other infrastructures that hosted RAMCAP field-testing over the years.

The authors also wish to thank Decision Lens Inc., led by David and Daniel Saaty, for making their remarkable product and the exceptionally able assistance of Ms. Laurie Schott available to the project. Their contributions are seen especially in Chapters Two and Ten.

TABLE OF CONTENTS

FIGURES, TABLES & EQUATIONS

List of Figures

List of Tables

List of Equations

ACRONYMS

AADT	Average Annual Daily Traffic
AHP	Analytic Hierarchy Process
ANSI	American National Standards Institute
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASME-ITI	American Society of Mechanical Engineers – Innovative Technologies Institute, LLC
AWWA	American Water Works Association
BAF	Building America’s Future
BBB	Below Base Budgeting
B/C	Benefit/Cost Ratio
BEA	Bureau of Economic Analysis
BICE	Board on Infrastructure and the Constructed Environment
BZPP	Buffer Zone Protection Plan
CCAdj	Capital Consumption Adjustment
CCTV	Closed-Circuit Television
CSIS	Center for Strategic and International Studies
DCPP	Dynamic Cross Prioritization Plot
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
EMO	Evolutionary Multi-objective Optimization
EMS	Emergency Medical Services
EPA	U.S. Environmental Protection Agency
ERM	Enterprise Risk Management
EUT	Expected Utility Theory
FDA	U.S. Food and Drug Administration
FS	Fire Suppression
GDP	Gross Domestic Product
GIS	Geographic Information System
GMU	George Mason University
GUI	Graphical User Interface
HAZMAT	Hazardous Material(s)
IDS	Intrusion Detection Systems
IIM	Inoperability Input-output Model
IVA	Inventory Evaluation Adjustment
LAPI	Local Area Personal Income
LOS	Level of Service
MAUT	Multi-Attribute Utility Theory
MAVT	Multi-Attribute Value Theory
MSL	Mean Sea Level
NAICS	North American Industry Classification System
NASBO	National Association of State Budget Officers
NCR	National Capital Region
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanic and Atmospheric Administration

OMB	Office of Management and Budget
PCE	Personal Consumption Expenditure
PET	Punctuated Equilibrium Theory
PIM	Police Incident Management
POS	Point of Service
PPBS	Planning-Programming-Budgeting System
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RIMS II	Regional Input-Output Multiplier System
ROR	Rate of Return
RR/SAP	Regional Resilience/Security Analysis Process
SAFETY Act	Support Anti-terrorism by Fostering Effective Technologies Act of 2002
SBP	Strategic Business Plan
SCADA	Supervisory Control and Data Acquisition
SEUT	Subjective Expected Utility Theory
SPG	Senior Policy Group
SSG	Sector-Specific Guidance
SVA	Security Vulnerability Assessment
TBB	Target Base Budgeting
ULI	Urban Land Institute
VLD	Vulnerability Logic Diagram
VSL	Value of Statistical Life
ZBB	Zero Base Budgeting

SOUTHEAST REGION RESEARCH INITIATIVE

In 2006, the U.S. Department of Homeland Security commissioned UT-Battelle at the Oak Ridge National Laboratory (ORNL) to establish and manage a program to develop regional systems and solutions to address homeland security issues that can have national implications. The project, called the Southeast Region Research Initiative (SERRI), is intended to combine science and technology with validated operational approaches to address regionally unique requirements and suggest regional solutions with potential national implications. As a principal activity, SERRI will sponsor university research directed toward important homeland security problems of regional and national interest.

SERRI's regional approach capitalizes on the inherent power resident in the southeastern United States. The project partners, ORNL, the Y-12 National Security Complex, the Savannah River National Laboratory, and a host of regional research universities and industrial partners, are all tightly linked to the full spectrum of regional and national research universities and organizations, thus providing a gateway to cutting-edge science and technology unmatched by any other homeland security organization.

As part of its mission, SERRI supports technology transfer and implementation of innovations based upon SERRI-sponsored research to ensure research results are transitioned to useful products and services available to homeland security responders and practitioners.

For more information on SERRI, go to the SERRI Web site: www.serri.org.

DISCLAIMER

ASME Innovative Technologies Institute, LLC
This work is published with the understanding that ASME Innovative Technologies Institute, LLC (ASME-ITI), the American Society of Mechanical Engineers (ASME), and its authors and editors are supplying information, but are not attempting to render engineering or other professional services. If such engineering or professional services are required, the assistance of an appropriate professional should be sought.

ASME-ITI, ASME, ANDTHEIR REPRESENTATIVES AND EMPLOYEESMAKE NOWARRANTY, EXPRESSED OR IMPLIED, REGARDING ANY FACTS OR OPINIONS CONTAINED OR EXPRESSED IN THIS DOCUMENT.

ASME-ITI, ASME, and their representatives and employees make no warranty, expressed or implied, regarding the reliability or usefulness of any information, formula or process disclosed in this report.

ASME-ITI, ASME, and their representatives and employees shall have no liability to any person or entity that reviews this report based upon the information, facts, opinions, formulas or processes expressed or disclosed in the report. Without limiting the generality of the foregoing, ASME-ITI, ASME, and their representatives and employees shall have no liability to any third parties, as no benefit to third parties is intended or implied.

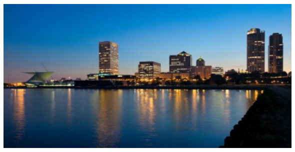
ASME-ITI, ASME, and their representatives and employees do not represent or provide any warranty, expressed or implied, that use of information, facts, opinions, formulas or processes expressed in this report would not infringe on any third party rights.

In no event shall ASME-ITI, ASME, or any of their representatives or employees be liable to any person or entity for damages of any kind (direct, special, incidental, consequential, or punitive) for any kind of injury (personal, property, or economic) incurred by any reader or any third party that may arise, either directly or indirectly, from any facts, opinions, information, formula or process disclosed in this report. Nor shall ASME-ITI, ASME, or any of their representatives or employees be responsible for any errors, omissions, or damages arising out of the use of information contained or disclosed in this report.

For additional information or to receive a copy of this publication, please contact:

ASME Innovative Technologies Institute, LLC
1828 L Street, NW Suite 906
Washington, DC 20036
info@asme-iti.org
www.asme-iti.org

EXECUTIVE SUMMARY



A Regional Resilience/Security Analysis Process for the Nation's Critical Infrastructure Systems

The Challenge

Hurricanes Irene, Katrina and Ike, the floods of the Mississippi and Cumberland, the Joplin and Tuscaloosa tornadoes, the Minneapolis bridge collapse, the Northeast Blackout, the aftermath of the Deep Horizon oil spill and, of course, September 11 all underscore the value of resilience and security, especially on the scale of metropolitan regions. At the core of any region's resilience and security are its "hard" lifeline critical infrastructures – water and wastewater, energy, transportation, telecommunications – and its core public services and economic base – public health and safety, state and local government, education, banking and major employers, healthcare, food and shelter.

Dependencies within and between infrastructure systems, services, businesses and economic sectors affect societal well-being and the ability of the community and region to rebound from potentially catastrophic events. Identifying and addressing these dependencies can prevent "cascading" failures that compound the negative effects of natural or man-made events. Metropolitan regions are the scale of the greatest concern – that is where multi-state and national infrastructures converge to provide direct services, where local infrastructures, in their immediate interactions with each other and with larger-scale infrastructures, can most readily cascade from isolated events to regional disaster, and where the majority of the population resides – because consequences are greatest.

The vital role of interdependent infrastructures has been recognized by the federal government since the 1990s, but practical tools have yet to be developed to properly assess the levels of security and resilience of regions and their infrastructures and to evaluate options for enhancing their security and resilience. This report offers an objective business process for identifying and evaluating ways that metropolitan regions can enhance their security and resilience within available financial and human resources. This project describes such a system, called the Regional Resilience/Security Analysis Process, or RR/SAP. The purpose of the present project was to develop a prototype RR/SAP as a test of its feasibility.

Design Objectives

Basic design objectives for RR/SAP have been developed from two directions. The first, in order to efficiently advance resilience and security under conditions of uncertainty and severe resource constraints, was to adapt the financial risk analysis and portfolio optimization methods to apply to infrastructure investments on the scale of a metropolitan region. The second, to assure relevance and practicality, was to base RR/SAP on fieldwork in several actual regions with critical infrastructure systems, core community services, and key elements of the business base.[1] As design objectives, the RR/SAP must:

- Be quantitative, objective, and repeatable;
- Estimate loss (for risk), service outage (for resilience) and benefits and costs of improvement options in terms directly comparable across sites and sectors as they impact *each,* the owner of the system and the regional public it serves, respectively;

---

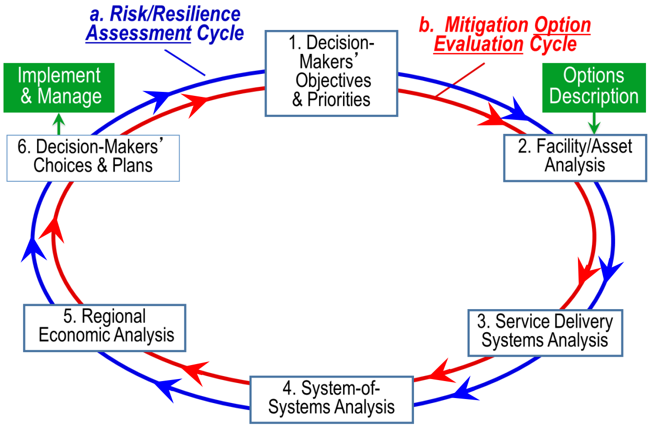
[1] The first statement of design specifications was in Brashear, *et al.,* 2005, which examined the risk and resilience analysis requirements of the National Capital Region. Fieldwork in the Hampton Roads region of Danville, Virginia and Nashville, Tennessee contributed invaluably to the current design.

- Produce *expected* (i.e., probability-weighted) values of losses and outages that incorporate the likelihood of unwanted events and the vulnerability to them;
- Estimate benefits and costs in terms that can be directly compared to the evaluations of *unrelated* investment options with which they must compete in budgetary decision-making;
- Include the effects of dependencies and interdependencies explicitly;
- Be directly usable in capital and operating budget-making decisions of local, state and business organizations;
- Be capable of being carried out and maintained by on-site, non-specialized, non-expert staff, with perhaps a modest amount of training;
- Permit re-analysis over time to measure progress and to establish accountability; and
- Be maintained and updated regularly.

The Business Process

RR/SAP (*Figure 1*) consists of a Risk/Resilience Assessment Cycle to identify the most serious risk/resilience challenges facing the region and its infrastructures, public safety functions and major industries and to set a baseline for comparisons, followed by a Mitigation Option Evaluation Cycle to estimate the value, benefits and costs of alternative investment options. For the region and each infrastructure system, the *risk/resilience assessment cycle* builds in six forward-looking phases.

Figure 1. **The Regional Resilience/Security Analysis Process (RR/SAP)**



1. ***Decision-Makers' Objectives & Priorities:*** Decision-makers use a rational process to define and rank their objectives, criteria, metrics and priorities for resilience, continuity, security and any other criteria of value.
2. ***Facility/Asset Analysis:*** Key facilities and their assets undergo an in-depth, *confidential* risk/resilience analysis to identify the threats and hazards (with their likelihood of occurring), vulnerabilities and direct consequences to each infrastructure's basic facilities and assets using a well-established American National Standard analysis process.
3. ***Service Delivery Systems Analysis:*** Systems models analyze the geographically extended service delivery process to ascertain how a failure of an asset or facility would propagate across the system and be managed by the systems control processes.
4. ***System-of-Systems Analysis:*** The dependencies and interdependencies among the systems are examined as they interact in a model that connects the respective systems models into the regional system to observe the potential for failures in one infrastructure system to directly cause failures in others' assets and delivery systems – the "cascade" of failures.
5. ***Regional Economic Analysis:*** An adaptation of classic input-output analysis estimates the consequences of infrastructure failures to the whole regional economy, including "ripple" effects, as well as lost jobs, wages and local sales taxes.
6. ***Decision-Makers' Choices & Plans:*** Decision-makers rank the areas of risk and resilience identified from these analyses and initiate the MitigationOptions Evaluation Cycle.

The *mitigation options evaluation cycle* defines possible investment "options" – new projects, programs and/or investments to enhance the resilience, continuity, security, or other high-priority objectives. It then revisits phases 1 through 5 to define precisely how *and* how much the programs and investments would improve resilience, security and the other criteria; what they will cost; and which would be the most valuable to the owners of the respective systems *and* to the region's citizens, respectively. This information is displayed for decision-makers when the evaluation cycle reaches phase 6. Decision-makers review these evaluations in the budget process to determine which (if any) will be chosen and included in their plans. Those that are selected are implemented, monitored and managed.

The Products

Each participating organization receives *confidential* reports of:

- All vulnerability, risk, and resilience assessments of their facilities and service delivery systems, from the perspectives of both the owners and the community served, respectively;
- Vulnerabilities due to disruptions of systems on which their facilities depend;
- Mitigation options for enhanced security and resilience;
- Evaluations of the return on investment, net benefits and benefit/cost ratios of the options again from the two perspectives, in a form compatible with budget submissions; and
- A final, integrated report of all analyses, findings, evaluations and recommendations, in context of the dependencies with other facilities.

In addition, senior officials of state, local and regional *authorities* will receive reports of:

- A confidential regional assessment of security and resilience of each critical infrastructure and the full system-of-systems by which the region operates;
- Confidential evaluations of options that the region might take and benefit/cost ratios suitable for use in budget making; and
- A non-confidential report to the public summarizing the major issues and the options the public agencies have determined to pursue

The overall business process as applied is documented and installed in a suitable organizational framework that builds the region's continuing analytic capability.

Feasibility

This process has been developed from first-hand experience in nine infrastructure sectors and subsectors, an American National Standard (ASME-ITI, 2010), four regions ranging in size from 50,000 to several million people and numerous regional disasters.[2] Its feasibility has been tested at all these levels and has proven practical, reliable and useful for supporting difficult public and private decisions. This report describes each phase of RR/SAP and demonstrates this feasibility.

Alternative Roll-Out Strategies

The process, once further developed, could be offered as a service by one or more major consulting, technology or engineering organizations. The federal government could determine that the process could be the core of a "bottom-up" national resilience program and support its enhancement and dissemination as a way to stimulate self-help and local determination, or as an adjunct to its grant

---

[2] The elements of RR/SAP have been refined in multiple regions that have encountered a hurricane, heavy flooding and terrorist attack.

programs while maintaining a set of comparable regional assessments by which national progress could be measured. It could serve as standard analysis required for projects advanced for funding by the proposed national infrastructure bank. User communities and cross-regional information sharing could spread innovative options and best practices.

The Outcome

The outcome of widespread use of RR/SAP can be rational, public-private collaboration toward analysis-based priorities and investments that make regional infrastructure systems and community facilities more resilient, secure and reliable. Such an outcome will lead to a more resilient, secure nation that benefits all its citizens, businesses and society as a whole.

CHAPTER 1

Background, Rationale and Overview of the Regional Resilience/Security Analysis Process

1.1 The Challenge

It has taken tragedy to direct public attention to the deterioration and growing vulnerability of America's critical infrastructure and the need for more secure and resilient systems. Hurricane Katrina, the Minneapolis bridge collapse, flooding along major rivers, tornadoes, and the Northeast Blackout of 2003 represent avoidable catastrophes and needless economic disruptions (ASME-ITI, 2009). The criticality and vulnerability of infrastructure has even attracted the attention of terrorists, as the attacks in New York, Madrid, Tokyo and London attest.

1.1.1 Definition of Infrastructures

Executive Order 13010, signed by President Clinton in 1996, defined critical infrastructures as "so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States" and included "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services and continuity of government."

The U.S. Department of Homeland Security (DHS) in the National Infrastructure Protection Plan (NIPP) has expanded the concept to "critical infrastructures and key resources" and added food and agriculture, health and healthcare, defense industrial base, information technology, chemical manufacturing, postal and shipping, dams (including locks and levees), government facilities, commercial facilities, critical manufacturing and national monuments and icons, for a total of 18 (NIPP, 2009).

The National Research Council (NRC) Board on Infrastructure and the Constructed Environment (BICE) has argued that five "lifeline" infrastructures are the most critical because all the others depend on them for survival. These are power, telecommunications, transportation, water and wastewater systems (BICE, 2009).

Physical infrastructures are the lifelines that deliver essential services that society and the economy depend on to function. These include transportation, energy, water and wastewater and communications. This paper focuses on these five, agreeing with BICE, but expecting that the results will ultimately apply to many of the 18 sectors identified by DHS as well as to other business, industrial and community facilities.

Other systems that depend on these "hard" infrastructures, often called "soft" infrastructures, are the institutions that deliver higher order services and include public safety, governance, law enforcement, education, agriculture, finance, commerce, manufacturing, cultural/recreational services, etc. Soft infrastructures require the services of the hard infrastructures to function and hard infrastructures are dependent on one another. The present project addresses primarily the hard infrastructures and public safety functions, although other, "soft" infrastructures will be added for a more comprehensive analysis in the future. Disruptions to the five "hard" infrastructures can entail widespread disruptions to the entire region in which they occur, with possibly severe consequences for human health and safety and significant economic losses.

Physical infrastructures are the lifelines that deliver essential services that society and the economy depend on to function.

The current status of these vital infrastructures is broadly regarded as poor. After an in-depth review of American infrastructure, the American Society of Civil

Engineers (ASCE) issued a "report card" grade of D, citing threats to human life and economic performance and recommended investment of $2.2 trillion over the next five years, roughly half of that incremental to expected levels of investment (ASCE, 2009). The U.S. has spent less and less as a percentage of Gross Domestic Product (GDP) since its peak in the late 1950s (CBP, 2008). Building America's Future (BAF), led by former Governors Rendell (D-PA) and Schwarzenegger (R-CA) and Mayor Bloomberg (I-NY) issued its infrastructure status report (BAF, 2011) with the summary in the title: "Falling Apart and Falling Behind."

1.1.2 Infrastructure Investment Decision-Making: "Under-investing and Investing in the Wrong Projects

But the problem is much greater than simply insufficient investment. According to a distinguished bipartisan commission that included two sitting Senators, two former Senators, three sitting governors and a number of former cabinet members and ambassadors, convened by the Center for Strategic and International Studies (CSIS), "America's economic well-being and physical security depend on safe and reliable … infrastructure… But we are both under-investing in infrastructure and investing in the wrong projects: *new investments are critically needed, but we lack the policy structures to make the correct choices and investments…* A centralized infrastructure project approval process would force all infrastructure modes to be evaluated using common methods and parameters" (CSIS, 2006). The commission was not specific as to a particular set of "common methods and parameters." Establishment of objective, transparent methods that use "common methods and parameters" that yield directly comparable estimates of benefits and costs of alternative investments is the *sine qua non* of rational allocation of limited resources.

The vast bulk of existing infrastructure our society and economy depend on ...has been poorly maintained and is subject to failure from a variety of causes.

The National Economic Council and the U.S. Department of the Treasury has released a report on "Economic Analysis of Infrastructure Investment" (2010) that found, "Federal funding for infrastructure investments is not distributed… using economic analysis or cost-benefit comparisons…[the process] virtually ensures that the distribution of investment…is suboptimal from the standpoint of raising national productive capacity."

Investing limited resources in resilience/security of hard infrastructures that would otherwise go directly to increased productive capacity must be carefully considered and thoroughly justified to yield a rational solution. Resilience/security investments, whether by the public or private sector, must compete with other kinds of investments on common terms and succeed only when they produce economic and social benefits that exceed those of other capacity-raising investments. In new infrastructure, fortunately, capacity-increasing and resilience/security-enhancing objectives can often be combined in initial, integrated design and engineering stages. This approach, however, will have its greatest impact in the future and only if adopted today. The vast bulk of existing infrastructure our society and economy depend on was built well before the current interest in resilience and security, and has been poorly maintained and is subject to failure from a variety of causes. Threats and hazards of all kinds can disrupt the flow of basic lifeline services and propagate throughout their service areas.

1.1.3 Calls for Solutions

Both the private sector and federal, state and local governments have noted the need for prompt, prudent action:

- A national infrastructure bank has been introduced in every Congress since 2007 and is part of the Obama Administration's jobs proposals – each time with the understanding that a transparent, rational, consistent process will be used to select project for investment.

- The Urban Land Institute (ULI), along with Ernst & Young, recently published a report calling for action on this pressing national need. While supporting many of the same recommendations as BAF, ULI recommended "the White House should consider setting national goals and managing objectives through a high-level infrastructure czar and/or commission" (ULI, 2009).
- In a separate study, Ernst and Young concluded that "impact of aging or inadequate infrastructure" ranked third among risks for commercial real estate, after only the "credit crunch" and "global economic and market conditions," and higher than such threats as the "global war for talent" and climate change (Fleming, 2009).
- Infrastructure investment is likewise a critical concern for organizations such as America 2050 and the National Governors Association (Springer, 2009).
- Title IX of the 9/11 Commission Recommendations Act requires establishment of a system of national standards, accreditation and certification to encourage business continuity (in infrastructure, another name for resilience).
- The Rockefeller and Sloan Foundations have mounted a major program to encourage continuity and resilience.
- The American Society for Industrial Security, the International Standards Organization, the American National Standards Institute Homeland Security Standards Panel, and other groups are working to establish an environment in which security, continuity, resilience and risk management are commonplace.
- Independent advisory panels to the President and to the Secretary of Homeland Security in the last administration endorsed resilience as a national objective, an initiative also advanced by Business Executives for National Security.

- The NRC's BICE study cited earlier – in which sustainability is broadly defined to mean systems that are able to meet the needs of current and future generations by being physically resilient, cost-effective, environmentally viable, and socially equitable – and suggests a solution framework, to quote:
    - *"A broad and compelling vision* that will inspire individuals and organizations to pull together to help meet 21st century imperatives by renewing the nation's critical infrastructure systems. Such a vision would focus on a future of economic competitiveness, energy independence, environmental sustainability, and quality of life, not a legacy of concrete, steel, and cables.
    - *"A focus on providing the essential services involving water and wastewater, power, mobility, and connectivity* – in contrast to upgrading individual physical facilities – to foster innovative thinking and solutions.
    - "*Recognition of the interdependencies among critical infrastructure systems* to enable the achievement of multiple objectives and to avoid narrowly focused solutions that may well have serious, unintended consequences.

  - "*Collaborative, systems-based approaches* to leverage available resources and provide for cost-effective solutions across institutional and jurisdictional boundaries.
  - "*Performance measures* to provide for greater transparency in decision making by quantifying the links among infrastructure investments, the availability of essential services, and other national imperatives" (BICE, 2009).
- The CSIS commission, quoted above, set in motion the formation of BAF, which published a report on U.S. transportation infrastructure that included among its recommendations for a "Smart National Strategy" the following:
  - "Establish strict national criteria for investments…and include new requirements that state officials conduct cost-benefit analysis…
  - "Prioritize improving capacity and efficiency at economic junctures that have national significance" (BAF, 2011).

The attention of the United States government on protecting critical infrastructure has grown since the establishment of the President's Commission on Critical Infrastructure Protection as stipulated in Executive Order 13010 (The White House, 1996). Several federal directives have been issued to underscore the need for disaster planning and management. Such directives [see Department of Homeland Security (DHS) 2003a, 2003b] call for the development of risk analysis tools to prepare the nation against disruptive events, prevent the occurrence of dire consequences, and ensure efficient response and recovery in the aftermath of such events. The National Response Framework (DHS, 2008) and National Infrastructure Protection Plan (DHS, 2006, 2009), the National Preparedness Goal (DHS, 2011) among others have been formulated to support the realization of such goals.

A consensus clearly exists that more investment in infrastructure is needed, that security and resilience should be among the objectives and selection criteria and that rational, holistic analyses of infrastructure investments on a metropolitan scale should guide those choices. Across all these groups, the clear message is that money is not the only requirement for turning American infrastructure around. A major systemic shortcoming exists in the way we decide on which infrastructure investments to make. But no industry group, professional society, research organization, blue ribbon panel, or coalition has developed a methodology for consistent, rational infrastructure investment valuation and selection. *The United States is currently ill-equipped to make the needed priority and resource allocation decisions, so we risk spending trillions of dollars over the coming decades on the wrong decisions, buying and rehabilitating the wrong infrastructure and passing up a huge opportunity to get it right.*

A major systemic shortcoming exists in the way we decide on which infrastructure investments to make.

1.2 Project Evolution, Objectives & Design Requirements

The intellectual heritage of the present project owes debts to three earlier projects: (1) a requirements assessment of the National Capital Region (NCR); (2) the development and testing of Risk Analysis and Management for Critical Asset Protection (RAMCAP); and (3) a feasibility study of adapting modern financial portfolio optimization methods for use in allocating capital to real (non-financial) infrastructure investments.

1.2.1 The National Capital Region Risk/ Resilience Assessment

The earliest precursor to the present process was a study of preparedness for terrorism risk and resilience of the NCR (McCarthy and Brashear, 2005). It strongly recommended that the metropolitan region is the appropriate scale of infrastructure value, risk/resilience and portfolio analysis. The NCR is a target-rich environment as the seat of government, military and intelligence headquarters, home of many of the world's financial and economic development institutions and the fourth largest regional economy in the U.S. The NCR abounds with iconic and functional targets. Natural hazards and interruptions of vital dependencies and interdependencies among infrastructures also threaten to diminish the functioning of this region.

The NCR Senior Policy Group (SPG), the homeland security advisors to the mayor of Washington and the governors of Virginia and Maryland, reasoned that improving the quality of risk and resilience analysis that supports risk management would be vitally important to addressing these threats. The SPG commissioned the University Consortium for Infrastructure Protection,[3] to evaluate the quality of risk/ resilience analysis for resource allocation in the region as a whole and in each of seven critical infrastructures and to recommend ways to improve that quality for the sectors and the region as a whole. The sectors were electricity, natural gas and fuels; potable water and wastewater services; healthcare; public safety, fire suppression and emergency medical care; transportation and shipping; financial services; and telecommunications.

[The National Capital Region project] strongly recommended that the metropolitan region is the appropriate scale of infrastructure value, risk/resilience and portfolio analysis.

The criteria for evaluating the quality of risk management were whether the sector and region exhibited, on an ascending scale:

1. Awareness of the value of critical infrastructure protection and resilience;
2. Availability of high quality risk management tools appropriate for use in the sector;
3. Resource allocation decisions for security and resilience were based on objective, quantitative risk/resilience assessment, with choices based on risk reduction and resilience enhancement relative to the costs to achieve them;
4. Extent that security/resilience programs are implemented in a timely and effective way; and
5. Evaluation of program performance for effectiveness and enhancement.

To judge the quality of risk management for criteria 2 and 3, a very basic risk/resilience analysis process standard was defined and used to critique the processes in place in the infrastructures and the region as a whole. Evaluation of the seven sectors and the region as a whole suggested that the NCR adopt a strategic goal to significantly enhance the security and resilience of the NCR from disruptions to the critical infrastructures. Such resilience would be marked by the ability to withstand attack without service interruption, to continue operations despite or during an attack, and/or to restore service quickly. Its hallmarks (and the basis for its metrics) are reliability, continuity of service and minimized loss due to disruption. Progress toward this goal can be made through four broad recommendations:

1. *Develop a public-private partnership to facilitate and coordinate risk and resilience governance.* The partnership is needed to establish a holistic, regional perspective to

---

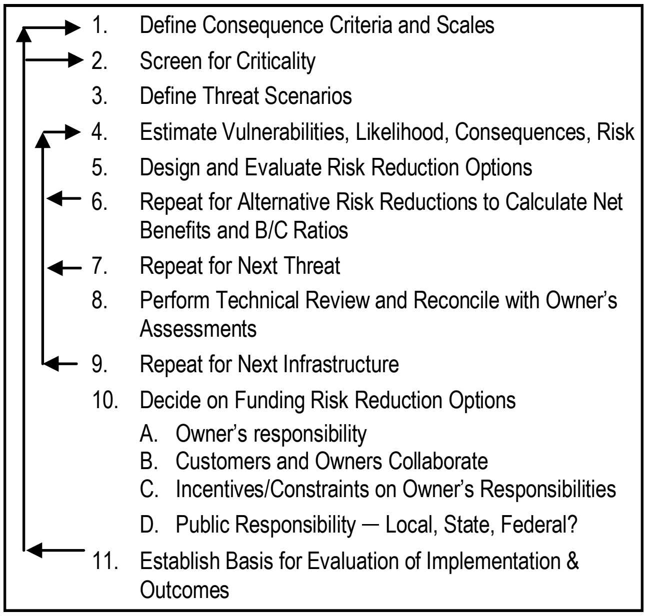
[3] The Consortium and its leadership were: George Mason Univ. School of Law, leader (John A. McCarthy and Jerry P. Brashear); Virginia Tech (Fred Krimgold); Univ. of Maryland (Gregory Baecher); Univ. of Virginia (Gregory Saathoff); James Madison Univ. (George Baker); and Howard Univ. (Kathleen Kaplan).

complement the individual jurisdictions and infrastructure organizations to assess challenges to security and resilience and inform planning and resource-allocation affecting public and private, military and civilian sectors, individually and collectively.

2. *Conduct objective, quantitative, directly comparable all-hazards vulnerability, risk and resilience assessments and inventory for:*
    - Individual assets defined as socially critical or key elements of critical infrastructures;
    - Systems of facilities and other assets that make up an infrastructure;
    - Cross-system regional system-of-systems to capture dependencies and potential cascading failures; and
    - Regional economic analysis to capture all direct and indirect impacts of regional disruptions.
3. *Develop and implement countermeasures and mitigation programs.* Directly enhance the resilience of the NCR through the partnership and individual infrastructure owners using the results of the assessments of CI assets, systems and region to rank, select and fund high-value projects and programs.
4. *Evaluate the implementation and effectiveness of the programs.* Assure that the programs have been implemented as planned and that they are achieving their objectives. The most effective way to do this is to repeat the assessments from time to time to measure progress and identify new trends.

Among the detailed recommendations was the description of an analytic system to support decision-making on the metropolitan scale (*Figure 1.1)* that bears close resemblance to the logic of the business process developed in this project.

Figure 1.1 **Analysis Process for Regional Resilience**



1. Define Consequence Criteria and Scales
2. Screen for Criticality
3. Define Threat Scenarios
4. Estimate Vulnerabilities, Likelihood, Consequences, Risk
5. Design and Evaluate Risk Reduction Options
6. Repeat for Alternative Risk Reductions to Calculate Net Benefits and B/C Ratios
7. Repeat for Next Threat
8. Perform Technical Review and Reconcile with Owner's Assessments
9. Repeat for Next Infrastructure
10. Decide on Funding Risk Reduction Options
    A. Owner's responsibility
    B. Customers and Owners Collaborate
    C. Incentives/Constraints on Owner's Responsibilities
    D. Public Responsibility — Local, State, Federal?
11. Establish Basis for Evaluation of Implementation & Outcomes

The NCR project set new directions in thinking about infrastructure security by emphasizing resilience as an objective separate and distinct from security; by using the metropolitan region as the scale of analysis; by identifying the need for dual perspective (owner and public) assessments; by insisting on rigorously quantitative evaluation at multiple scales of analysis; and by stressing the notion of public-private partnerships as part of the regional solution. The NCR project identified the emerging RAMCAP, then in developed by the American Society of Mechanical Engineers (ASME), as a promising tool for asset-level analysis and hypothesized its integration with a holistic, systems approach to analyze and manage interdependencies at the regional scale – all precursors to the design of the current Regional Resilience/Security Analysis Process.

1.2.2 RAMCAP Development

RAMCAP was developed to advance the primary recommendation of an invited group of senior executives from industry and infrastructures, convened by ASME in 2002 at the request of the White House, to consider how best to protect the nation's infrastructures from attack. The recommendation was to develop an objective, rigorous risk analysis process that could be applied across infrastructures and regions with enough consistency to assure genuine comparability. Without such a process, rational allocation of resources to protect infrastructure would be impossible.

Under sponsorship of the DHS Office of Infrastructure Protection, ASME-ITI developed RAMCAP, a facility/asset based risk/resilience analysis process, tailored it to nine industries and developed it into an American National Standard for water/wastewater systems. Over the period of its development, the process was updated three times to incorporate a variety of improvements.

RAMCAP is discussed in more detail in Chapter Four, but for here it is sufficient to state that its basic tenets of quantification, consistency for comparability, key definitions and metrics, proxy approach for estimating terrorist threat likelihood, natural hazards analysis and process logic are seen throughout the process described in this report.

1.2.3 The Portfolio Feasibility Study

Since the middle of the last century (Markowitz, 1952, 1972; Bernstein, 1998), financiers have understood how to optimize risk and value under constraints as portfolios of financial assets. A reasonable approach to the infrastructure challenge would be to adapt the process for optimizing portfolios of financial assets to dealing with real (i.e., non-financial) infrastructure assets and then determining if analytic tools or methods exist to perform the necessary tasks. To the extent they exist – requiring no major methodological discovery or invention – the business process would be deemed feasible. The conclusion was that an infrastructure portfolio optimization process was indeed feasible, given a few adjustments.

ASME-ITI organized a panel of infrastructure and risk/portfolio experts to define the needed methodology and the R&D to develop it. They were asked to address the need for an *objective, transparent business process for valuing and selecting outlays for both new and renewed infrastructure that would rationalize and optimize the infrastructure portfolio.*

The needed methodology must apply to all infrastructure investment proposals... using consistent definitions, processes, criteria and metrics to yield results ...

The needed methodology must apply to all infrastructure investment proposals – at least those involving taxpayer or ratepayer funds – using consistent definitions, processes, criteria and metrics to yield results that are directly comparable before the fact and sufficiently operational to serve as performance evaluation criteria after the fact. Tailored variations might be needed to deal with the diverse technologies, cultures and traditions of individual sectors, but the core definitions, calculations and processes should be common to all sectors to enable comparisons needed for rational resource allocation.

Economic impacts are almost universally recognized as key indicators in analyzing value and risks. Specifically defining “economic impacts” and “to whom” is necessary for either financial or infrastructure portfolios. The financial portfolio defines economic impacts as the return on investment, either in cash flow dollars or percentages and the “whom” as the investor who takes the risk of investing. Infrastructures also have “investors” – the stockholders and taxpayers, together, the “owners” of the infrastructure. In lifeline infrastructures, however, the general public, including but not limited to the infrastructure’s customers, has a vital interest because of the critical role the infrastructures play in the well-being of the public and the economy. For lifeline infrastructures, we must examine impacts from two perspectives: (1) the organization owning the asset; and (2) the regional metropolitan community. The logic for this dual analysis is illustrated in *Figure 1.2* and discussed more thoroughly in Chapter Four.

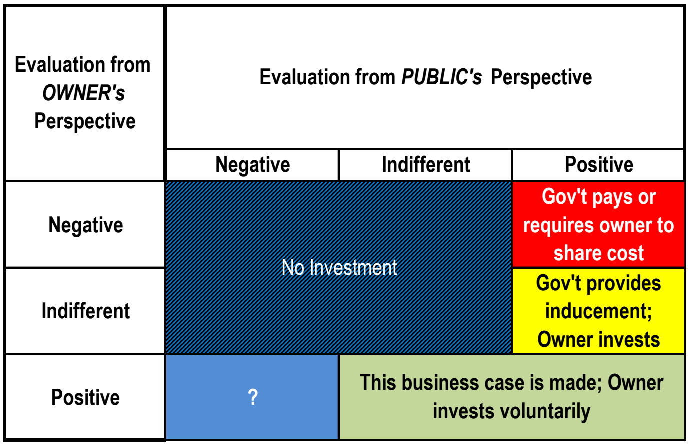
Conducting the analysis from the two perspectives *based on a common basis of specific asserts, threats and vulnerabilities with the two sets of relevant consequences* greatly facilitates the public-private discussions about who benefits and who pays. The dual perspectives allow analysts to see whether the owner can be expected to make the investment without incentives or if the public's participation is required (essentially based on what economists call externalities and public goods) to either avoid seriously negative options or stimulate positive ones. Looking at the situation in these terms also suggests new forms or partnerships between owners or between public and private organizations.

Losses from the owners' perspective (and investments to avoid them) are the usual framework for conventional private risk and portfolio analysis, while losses from the public's perspective (and investments to avoid them) are the usual framework for public policy analysis. Looking at both in the same analysis may be unique to the current approach. The point of the dual assessment is to identify where the benefits and losses fall and, therefore, who should pay the costs. By doing the analysis together, based on the same physical events, the potential for communications leading to the correct decisions and cost-sharing are facilitated.

The methodology should focus squarely on the expected value consequences of inaction versus those of investing in alternative solutions (the difference between them is benefits of the investment). It should first and foremost estimate the value of the project – the probability-weighted multi-attribute objective of the investment. It should also estimate the level of risk (probability-weighted undesirable consequences) and resilience (probability-weighted service outage after disruption) relative to a number of potential adverse events and the value of reducing risk and enhancing resilience. It should assess each investment opportunity in the systems context, including how it interacts with other facilities with which it is interdependent, and should consider non-structural and technological alternatives to the structural solution.

...dual perspectives allow analysts to see whether the owner can be expected to make the investment without incentives or if the public's participation is required...

Figure 1.2 **Economic/Financial Consequence Analysis: Two Perspectives Needed**



Evaluation from *OWNER's* Perspective	Evaluation from *PUBLIC's* Perspective		
	Negative	Indifferent	Positive
Negative	No Investment		Gov't pays or requires owner to share cost
Indifferent			Gov't provides inducement; Owner invests
Positive	?	This business case is made; Owner invests voluntarily	

Table 1.1 summarizes the feasible solution, showing the conventional financial portfolio optimization approach in the left-hand column, the approach adapted for infrastructure investments in the center column and the available analytic tools to implement it in the right.

As the right-hand column of table indicates, analytical tools exist that can perform each of the necessary phases, so feasibility is established. The next step is to *define, build and test a prototype of the needed business process to further establish the feasibility of the approach – the purpose of the present project.* The rest of this document reports this prototype and concludes that the approach is fully feasible.

1.2.4 Design Requirements for a Regional Resilience/Security Analysis Process

The results of the NCR study, RAMCAP's development history and the portfolio feasibility study define the desired design requirements for the business process to be developed and tested in the present project. Considerations concerning the necessity that the process must be compatible with and provide information directly to the budgeting processes of infrastructure organizations and other decision-makers, examined in Chapter Two, also contributed to these specifications. The design requirements for the desired management process are:

1. *Comparability.* The RR/SAP system must integrate fully with the processes for allocation of investments across all classes of infrastructure. It should demarcate independent elements while highlighting interdependencies between assets and systems, within and across regions and possibly other classes of investment. Terms of analysis must be consistent across systems and departments to provide for uniform comparison of costs and benefits related to specific investment options. Comparability of metrics is essential to the evaluation of trade-offs in the budget process. Consistent and comparable metrics are also essential for re-measurement over time for accountability and to acknowledging changing situations.
2. *Multi-criteria.* The RR/SAP must be holistic in its criteria for success not only incorporating economics, but also societal, technological and other issues. Valuation must accommodate a series of desired objectives for infrastructure including resilience, safety, infrastructure adequacy, economic growth, distributional equity, environmental sustainability, and efficiency and effectiveness in government. The process of selection between investment options must take into account the multiple objectives of the range of legitimate decision-makers. The relative valuation of investment outcomes must reflect a balanced consensus of relevant parties, both public and private. Investment in regional resilience must be based on equitable distributions of costs and benefits.
3. *All Outcomes.* The RR/SAP must consider all outcomes. Both potential upside gains and downside losses should be included in the valuation. It cannot focus exclusively on risks and outages, but on accomplishing positive objectives as well. The RR/SAP must provide adequate consideration for the range and distribution of negative consequences of resilience/security measures for particular subgroups in the region. These must be carefully balanced

Table 1.1 **Comparison of Financial Portfolio Optimization and Infrastructure Portfolio Optimization (with Tools)**

Financial Assets	Infrastructure Assets	Analytic Tools
1.Develop goals, objectives, constraints, metrics: private perspective	1. Same, but both public & private goals, etc.	Analytic Hierarchy Process (AHP)
2. Value existing portfolio – value risk; private perspective – gap analysis	2. Same, except from both owner's & public's perspectives	Regional input-output; engineering-economics risk/resilience baseline analysis
3. Assess new investment opportunities individually	3. Same, for new & renewal investment projects	Engineering-economics risk/resilience analysis of options (RAMCAP)
4. Estimate financial correlations among existing & new assets or market (covariance/beta)	4. Same, except estimate physical interdependencies among existing & new assets	Individual infrastructure distributed service systems models; regional systems-of-systems model
5. Optimize investment portfolio – maximize value at accept-able risk level, within constraints (budget & other)	5. Same, but assure feasible private investments are made; then maximize value within public constraints	Portfolio optimizer
6. Select portfolio – private perspective	6. Same, but from public's perspective only	Sensitivity analysis using the above tools

with intended resilience/security benefits to others in the region.

4. *Innovation.* The RR/SAP must be adaptive and the framework must permit investments in new infrastructure and new ways of providing infrastructure services in the same paradigm as renewal/replacement of old infrastructures. Concern for resilience should not rely solely on facility hardening and restriction of development. Innovative approaches to enhanced resilience should be incorporated with other relevant values such as sustainability and equity of access. Patterns of infrastructure service delivery can be modified to enhance both security and service.

5. *Uncertainties.* For the RR/SAP to be robust, it must capture uncertainties in its estimates. There are significant uncertainties related to frequency and intensity of natural hazards and even greater uncertainties related to the nature, consequences and timing of malicious attacks. These uncertainties must be represented as accurately as possible to avoid over or underestimation of risks. There are also significant uncertainties related to facility and system performance during extreme events and the potential for cascading failures. The analysis must represent a range of potential credible outcomes to provide the most useful presentation of investment options and their consequences. Treatment of uncertainty may take any of several forms, including scenario analysis, sensitivity analysis, estimation of full distributions of key uncertain parameters (coupled with some form of Monte Carlo simulation), etc.

> *Dependencies within systems can lead to cascading failures that propagate service loss far beyond the initially impacted asset or facility.*

6. *Dependencies.* As noted above, cities and their infrastructures are complex, highly interdependent systems. The RR/SAP must recognize and capture these dependencies and interdependencies. The analysis must illuminate the implications of dependencies within and among infrastructure systems. Dependencies within systems can lead to cascading failures that propagate service loss far beyond the initially impacted asset or facility. For example, the loss of an electric power transmission line may lead to the overload and failure of adjacent lines. Cross-system dependencies are less obvious than, for example, a loss of power to a pump that may cause a decrease in water supply that impedes fire suppression and interrupts communications due to loss of cooling of major equipment. Understanding the consequences of infrastructure dependencies and interdependencies is key to evaluating the potential benefit of avoiding cascading failures.

7. *Comprehensiveness.* The RR/SAP must support integrated decision-making amongst private and public actors – especially in identifying and valuing “public goods” and “economic externalities.” Regional critical infrastructures are owned and managed by both public and private sector organizations. In terms of regional resilience, these public and private systems are inextricably intertwined and interdependent. Water, sanitation, roads and public safety are typically public. Electric power, fuel and communications are typically private. All are essential to regional resilience. To the extent possible the tools developed for regional resilience/ security analysis should be comparable and yield compatible results to facilitate comparison and performance tracking.

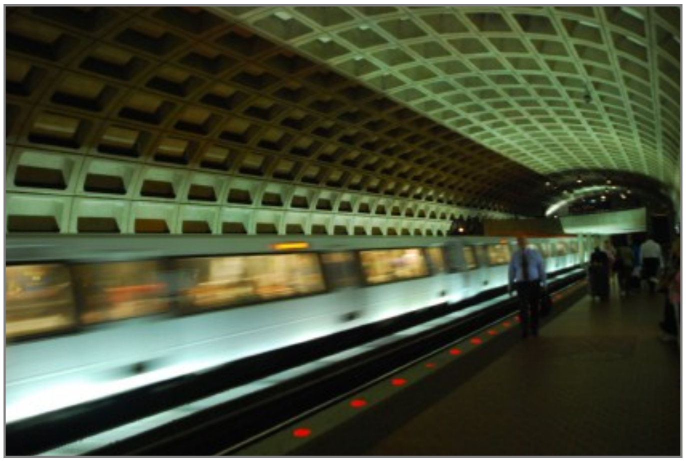
8. *Portfolio.* The RR/SAP must provide a full contextualized, portfolio view of investments and their performance. The ultimate purpose of the RR/SAP is to optimize the total regional investment in resilience by buying down risk in the most

efficient way possible. This objective is complicated by the complexity of the threat and the complexity of the target. Resilience is intended to be multi-hazard and requires response to a range of threats of varying predictability. Resilience also requires mastering the complexity of a system of infrastructure systems and their potential interactions. Investments in regional resilience/security must be made in the context of all other demands on public and private resources. The justification for investment in risk reduction and rapid recovery must compete with a range of worthy and necessary investments. The objective of RR/SAP is to provide guidance to a reasonable and balanced level of investment in security and resilience.

9. *Defensible.* To be defensible in the face of countervailing pressures, the RR/SAP must be objective, transparent, and consistent with accepted risk-analysis norms and must produce directly comparable estimates of value, cost, risk, resilience and benefits for all investment options. To the extent possible, all elements of the analysis must be open to the public and comprehensible. Where uncertainties exist, they must be clearly identified and quantified. The analysis must be evidence-based, making full use of available relevant data on hazards, vulnerabilities and consequences from all reliable sources. Consequences of potential investments must be presented in concrete terms that support informed decision-making.
10. *Simplicity and Credibility.* The RR/SAP must be, at its core, simple enough to be used at management levels within the infrastructure, municipal or regional organization with a minimum of outside expertise or training, using data that are readily available. The RR/SAP must fit into the existing framework of annual budget processes. The budget is designed and driven by the principal executives who set the goals and objectives for the enterprise or jurisdiction, but it is constructed from the bottom up, possibly involving every unit of the organization. Significant values and activities of any organization are reflected in the budget and in the processes of negotiating values and priorities into quantifiable results.

1.3 Overview of Regional Resilience/ Security Analysis Process: A Business Process to Meet the Requirements

The portfolio project suggests the needed phases of desired business process. As illustrated in *Figure 1.3,* the RR/SAP consists of two broad cycles:



A. ***The Risk/Resilience Assessment Cycle*** ("assessment cycle') designed to quantify the current situation relative to the multi-attribute objectives set for the infrastructure, including resilience and security. It directs attention to the most important risk/resilience areas. This cycle sets the baseline of "do nothing" against which options for improvement can be compared.

B. ***The Mitigation Option Evaluation Cycle*** ("evaluation cycle") designed to define, quantitatively evaluate and select for funding specific investment options to enhance resilience and/or security and add value relative to a multi-attribute objective. The attractiveness of each option is the way in which it improves on the baseline assessment.

Each cycle is made up of the same six phases, shown as boxes in the figure. Near each phase are bullet points that summarize the results of the specific phase. The six phases, in brief are:

1.3.1 Phase 1: Decision-Makers' Objectives and Priorities

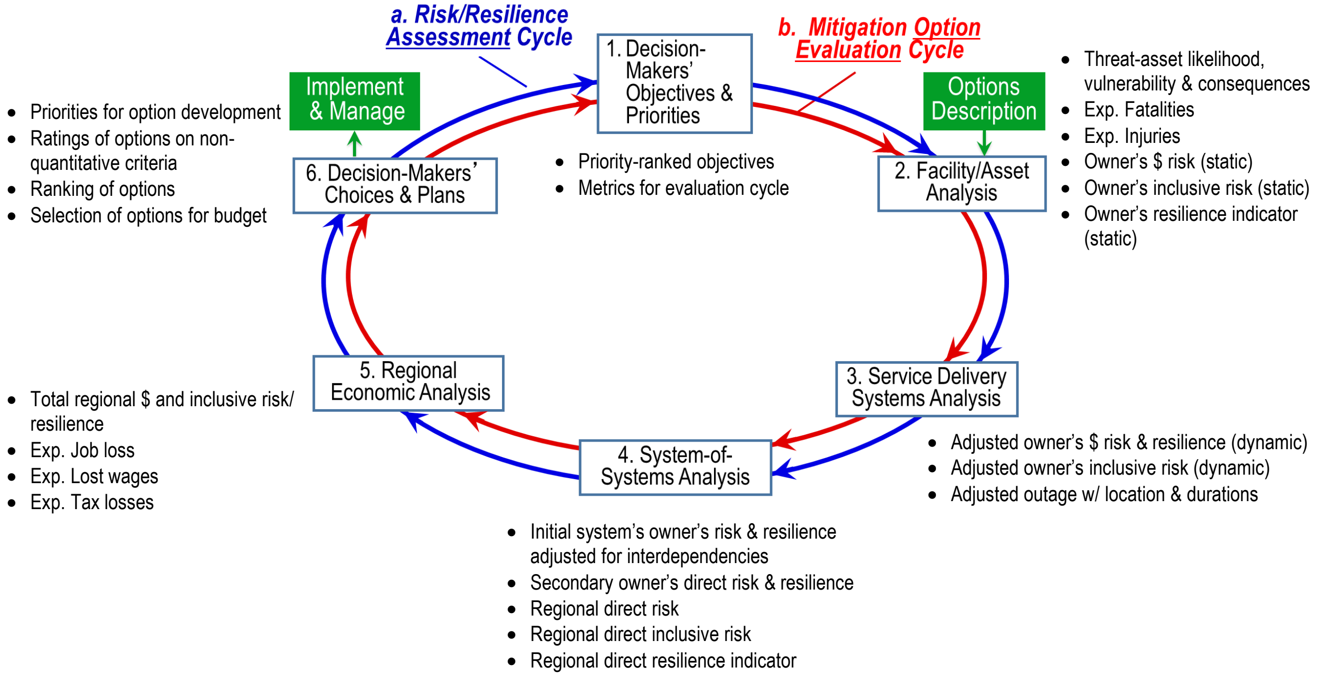
Phase 1 defines the objectives of the decision-makers, determines priority weightings and specifies concrete metrics by which options for improvement will be judged. The tool used to complete this phase is the Analytic Hierarchy Process (AHP) (as implemented in software by Decision Lens, Inc.). In the evaluation cycle, this phase refines and re-prioritizes the objectives in light of the findings of the assessment phase and the specific areas for improvement defined by the decision-makers at the end of the assessment cycle.

This phase is described at length in Chapter Three.

1.3.2 Phase 2: Facility/Asset Analysis

Phase 2 is a static risk/resilience analysis based on RAMCAP, developed by ASME Innovative Technologies Institute, LLC (ASME-ITI) and updated for this new process. In the assessment cycle, specific high-priority threat-asset pairs are determined based on facilities and assets essential

Figure 1.3 **Regional Resilience/Security Analysis Process (RR/SAP)**



to the mission and critical functions of the infrastructure or other entity being analyzed.

Potential hazards that arise due to dependencies on other infrastructures are identified in this phase by convening systems control experts from two infrastructures together (e.g., power and water) and having them identify on maps where one system's services support the other (e.g., what power substation and major transformers supply power to specific, critical drinking water pump stations). While additional potential points of dependency hazards may be identified in later phases, this step initiates these analyses and sets a tone of shared risks and common solutions across infrastructures.

Each threat-asset pair, threat likelihood, vulnerability and consequences is estimated quantitatively and combined as the baseline owner's *risk* (probability-weighted fatalities, injuries, and financial losses to the owner and inclusive risk, which combines them all) and *resilience indicator* (probability-weighted service outage, the product of the daily unmet demand and the number of days). The specific risk equation is:

$$\textit{Owner's Risk}_{ta} = \textit{Consequences}_{ta} \times \textit{Vulnerability}_{ta} \times \textit{Threat Likelihood}_{ta} = C_{ta} \times V_{ta} \times T_{ta}$$

Eq. 1.1

Where:

Consequences = fatalities, serious injuries and financial losses, individually or collectively ("inclusive risk"), to the owner of the system.
Vulnerability = the conditional likelihood that, given that the event occurs, the estimated consequences will follow.
Threat likelihood **=** the likelihood the initial event will occur.

This is the same risk equation used in the *National Infrastructure Protection Plan* (DHS, 2009) and an American National Standard (ANSI/ASME-ITI/AWWA J100-10, 2010). When used in the inclusive form of owner's risk, fatalities and serious injuries are converted to dollar terms using the liability to the owner, after insurance.

The specific equation for the owner's resilience indicator has two options, depending on whether decision-makers prefer to think about resilience in units or dollars. The dollar version, of course, is the version to be used in any cross-sector comparisons. The equations are:

$$\textit{Owner's Resilience Indicator}_{ta} = \textit{Service Denial}_{ta} \times \textit{Vulnerability}_{ta} \times \textit{Threat Likelihood}_{ta}$$

Eq. 1.2

Where:

$$\textit{Service Denial}_{Units} = \textit{Severity} \times \textit{Duration of Outage}$$

Eq. 1.3a

Or

$$\textit{Service Denial}_{\$} = \textit{Severity} \times \textit{Duration of Outage} \times \textit{Average Unit Price}$$

Eq. 1.3b

Where:

Service Denial = amount of service or products denied due to a disruptive event.
Severity = the number of units denied per day, usually measured from expected or "acceptable" level of demand.
Duration of Outage = the number of days the outage lasts.
Average Unit Price **=** the average price paid by customers in the affected area before the disruption.

In the option evaluation cycle, options are analyzed through the same process to estimate the amount of *reduction* in risk and/or the resilience indicator that will result from the option's effects on threat likelihood, vulnerability, consequences or outage. The differences between baseline risk and resilience and those with the option assumed to be in place are the *benefits* of the option.

Phase 2 is described in more detail in Chapter Four.

1.3.3 Phase 3: Service Delivery Systems Analysis

Phase 3 is a dynamic analysis of each infrastructure's (or other entity's) distributed service delivery process based on the SmartMoves network analysis tool developed by Alion Science and Technology Corporation. It models the distribution of services of each system individually across its service area as it encounters the threat-asset pairs defined in the previous phase.

In many infrastructures, the operations of advanced supervisory control and data acquisition (SCADA) systems and operating specialists adjust system routings to minimize the amount of outage experienced by customers, in particular special customers for whom a service interruption would be very damaging. The operations of SCADA to re-route services is complemented by manual over-rides by expert engineers and operators to further minimize and direct outages. This dynamic look at system operations often shows that the static analysis in the previous phase overstated the magnitudes and/or durations of service outages, so the owner's risk and resilience indicators are adjusted to incorporate the dynamic analysis. Usually, these adjustments will affect the lost revenue portion of the financial consequences in the risk estimate and the service outage portion of the resilience indicator estimation. The risk and resilience equations are the same, but the estimated consequences and service outages are adjusted to incorporate the more dynamic estimates.

...high-priority threat-asset pairs are determined based on facilities and assets essential to the mission and critical functions of the infrastructure ...

This phase also locates the outages geographically, the necessary step toward analyzing interdependencies. As specific geographic service areas and the amount of flexibility in operations are captured, knowing which assets of each system can service what geographic area makes the next phase feasible.

These analyses are conducted in both cycles. In the assessment cycle, adjusting the owner's risk and resilience indicators makes for a more correct assessment. In the evaluation cycle, the options that reduce likelihood, vulnerability, consequences or outages defined in Phase 2 are incorporated into the adjusted estimates. In addition, options that change the distribution management system can be evaluated for their own contributions to the enhanced resilience and security. These would be included in the adjusted owner's risks.

Phase 3 is discussed more fully in Chapter Five for non-transportation infrastructures and Chapter Seven for transportation.

1.3.4 Phase 4: System-of-Systems Analysis

Phase 4 also uses SmartMoves, but in this instance, the individual systems are analyzed together as they interact and support – or fail to support – one another. In the assessment cycle, each threat-asset pair is analyzed through the system-of-systems model to estimate where failures of the threat-asset pair leads to failures or reductions in service in other systems. The damaged system may be found to be damaged still further as the failures in the systems on which it depends causes additional damage to the initial system. For example, failure of the water system might affect the water-cooled computer that drives the power company's SCADA, causing a secondary damage to the power system. This, in turn, could damage the water system by denying power to the pump station that could send water to the power company's offices where the SCADA is housed, a true case of interdependency. The system-of-systems model simulates the workings of all the systems modeled to the point in time of the analysis (including systems that are not "hard" infrastructures, e.g., public safety functions and major economic entities) to follow the propagation of failures and to estimate the additional risks to the owners of each affected system.

The risk and resilience indicator to each of the secondary systems can be calculated based on *their* damage, if any, lost revenue and service outage, weighted by the initial threat-asset pair's likelihood and vulnerability. The impacted systems should include these risks in their analysis and should consider whether they need to take steps to manage them from their side or to cooperate with the initial system as it seeks to enhance its own security and resilience.

The sum of the risks and the sum of all the resilience indicators across all impacted systems – initial and secondary – is the regional direct risk and regional direct resilience indicator:

$$\textbf{\textit{Regional Direct Economic Risk}}_{ta} = \Sigma\ \textbf{\textit{Owner's Financial Risk}}_{ta} \tag{Eq. 1.4}$$

And

$$\textbf{\textit{Regional Direct Resilience Indicator}}_{ta} = \Sigma \textbf{\textit{Owner's Resilience Indicator}}_{ta} \tag{Eq. 1.5}$$

These quantities are always partial because they can include only the systems that are explicitly included in the system-of-systems model at the time of the analysis. They are, however, valid measures of risk and resilience for the systems that *are* included and they are specific enough to identify all the systems at risk, the magnitude of these risks and the geographic areas of the region that would be impacted by these events. This can be very useful information to decision-makers who must view risk and resilience from a more holistic, regional perspective.

A more comprehensive, inclusive risk estimate would combine the direct economic risks with an allowance for the human casualties. For reasons explained in Chapter Four, the values of \$7.0 million per fatality and \$1.7 million per serious injury are used in this process:[4]

$$\begin{gathered}\textbf{\textit{Inclusive Direct Regional Risk}}_{ta} = \\ \textbf{\textit{Direct Economic Regional Risk}}_{ta} + \\ \textbf{\textit{[(7.0 mill.}} \times \textbf{\textit{Fatalities}}_{ta}\textbf{\textit{)}} + \\ \textbf{\textit{(1.7 mill.}} \times \textbf{\textit{Injuries}}_{ta}\textbf{\textit{)}} \times \textbf{\textit{T}}_{ta} \times \textbf{\textit{V}}_{ta}\textbf{\textit{]}}\end{gathered} \tag{Eq. 1.6}$$

This is the most inclusive, *direct* risk measure at the threat-asset pair level that the RR/SAP provides and should be of great interest to regional decision-makers. Its virtue is that it tracks directly through specific system failures to the original threat-asset pair, defining numerous points at which options could be developed to enhance resilience and security. In the assessment cycle, these system-of-systems model estimates of risk and resilience indicators are tied directly to specific threats to specific assets or facilities. This information is invaluable in setting priorities for developing improvement options in Phase 6.

In the evaluation options, the estimated differences in these indicators due to implementation of the specific options are the benefits on which regional and owners' decisions can be based.

Phase 4, the system-of-systems analysis, is described more fully in Chapter Six.

1.3.5 Phase 5: Regional Economic Analysis

Phase 5 moves away from the specificity of direct modeling to analyze the total regional economic impacts of specific adverse events. It uses the Inoperability Input-Output Model (IIM), developed at George Washington University and the University of Virginia and applied to numerous large-scale infrastructure risk/resilience analyses. It estimates the total economic loss to the regional GDP and each of the sectors that make it up. This includes all direct losses and all "ripple effect" losses. By extension, it also estimates lost jobs, wages and

---

[4] This is the "value of a statistical life" as the average of those used by three federal agencies, as described in Chapter 4.

local sales and use taxes. For decision purposes, all of these are multiplied by the threat likelihood and vulnerability of the original threat-asset pair to yield the "expected" effects. At this level, the resilience indicator is the same as the risk indicator because both are concerned primarily with the consequences of service outages:

$$\textit{Regional Total Economic Risk/Resilience}_{ta} = \textit{Lost GDP}_{ta} \times V_{ta} \times T_{ta} \qquad \textit{Eq. 1.7}$$

And

$$\textit{Regional Total Inclusive Risk}_{ta} = [\textit{Lost GDP}_{ta} + (7.0\ \textit{mill.} \times \textit{Fatalities}_{ta}) + (1.7\ \textit{mill.} \times \textit{Injuries}_{ta})] \times T_{ta} \times V_{ta} \qquad \textit{Eq. 1.8}$$

$$\textit{Expected Job Loss}_{ta} = \textit{Estimated Job Loss}_{ta} \times V_{ta} \times T_{ta} \qquad \textit{Eq. 1.9}$$

$$\textit{Expected Wages Loss}_{ta} = \textit{Estimated Wages Loss}_{ta} \times V_{ta} \times T_{ta} \qquad \textit{Eq. 1.10}$$

$$\textit{Expected Taxes Loss}_{ta} = \textit{Estimated Taxes Loss}_{ta} \times V_{ta} \times T_{ta} \qquad \textit{Eq. 1.11}$$

In the assessment cycle, these are the most comprehensive, holistic indicators of risk and resilience because they include all direct and "ripple" effects. Because of their inclusiveness, they are useful as indicators of impact, but for the same reason, are less effective in directing attention to the chain of events initiated by the threat-asset pair, so are less useful for guiding the evaluation cycle. In Phase 5 of the evaluation cycle, the full magnitude of the benefits is estimated, especially using the inclusive form, but these also include the greatest uncertainty.

Phase 5, IIM and the regional economic analysis are discussed in Chapter Nine.

1.3.6 Phase 6: Decision-Makers' Choices and Plans

In Phase 6, decision-makers make choices that actually move toward reduced risk and increased resilience. In the assessment cycle, the decision-makers review the current, baseline situation of risks and resilience levels to give direction and priority to the evaluation cycle. In general, the greatest risk and greatest expected outage should be given greater priority, but other considerations may cause adjustments to these decisions. Certain risks and resilience levels may be seen as tolerable and are set aside. The multiple risk and resilience indicators may be reviewed individually, but may also be combined. The weights assigned to the objectives in Phase 1 can be used to consolidate the multiple metrics into a unified score for initial screening. In general, it is recommended that expected fatalities, serious injuries, owner's risk and resilience (as adjusted in Phases 3 and 4), regional inclusive direct risk and regional inclusive total loss, as well as the overall weighted score, be examined to set priorities for the option evaluation cycle.
After the option evaluation phase has defined specific security and resilience enhancement options and evaluated their effects through Phases 1-5, Phase 6 again plays the critical decision role: choosing and funding the options that will make the most progress. Key metrics from all phases are summarized as in *Table 1.2* for both the region (five indicators) and the owner of the system that suffered the initial threat to the particular asset (two indicators).

Where the owner's business case appears to be met, the owner should be encouraged to make the investment. If the option is declined, the owner should confidentially explain why that is the decision to the impacted systems and those representing the regional public. For all options *not* implemented by the initially affected system owner, regional public authorities and the directly impacted systems and organizations can examine the regional benefits. Partnership opportunities to share costs to "buy down risk" and/or "buy up resilience and continuity" may be possible. As the last resort, the regional public authorities may

Table 1.2 **Summary of Benefits & Benefit/Cost Ratios for Available Options**

	Regional Community										Owner			
Benefit Metrics	Multi-Attribute Objective Value		Expected Casualties Avoided		Inclusive Direct Risk Reduction		Direct Resilience Indicator Reduction		Total Regional Risk/Resil. Improvement		Inclusive Risk Reduction		Resilience Indicator Reduction	
Option Descriptions	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $
A														
B														
C														
D														
E														
Etc.														

invest alone in high-priority options. All these decisions are, ultimately, budget decisions, committing capital and operating funds to carry out the security/resilience enhancing options.

Decision-makers in both public and private sectors need a degree of flexibility in making large-value decisions. Some decision-makers are reluctant to employ decision-support tools because they believe that having "hard" quantitative information will constrain their flexibility. This need not be the case with RR/SAP because they play key roles in the crucial decision points of the process, including:

- Establishing the goals, objectives, criteria and their relative weights – the highest level policy decisions – as the definition of value in the initial step;
- Setting overall budgets levels and basic "pools" within the budget for specific purposes;
- Adjusting the weights on the objectives and criteria at any step to capture an evolving appreciation for the nature of the challenges;
- Setting minimum levels of outlay for any proposed project or project type to mandate its inclusion in the budget;
- Defining logical relationships among the candidate projects – e.g., if A is selected, B must (or must not) be selected;
- Directing the respective budget pools to specific projects; and
- Including "distributional" equity constraints, e.g., a minimum level in the respective areas, jurisdictions or type of project.

The decision process is far better informed but never becomes a "black box" that subtracts power from the decision-makers who use it.

Once chosen, the selected options are implemented, their operations monitored and managed and their overall performance evaluated as part of the next round of the RR/SAP assessment cycle.

The overall RR/SAP should be repeated on a regular schedule, usually every two or three years, with updates as needed for changing and unexpected events.

Phase 6 is described in more detail in Chapter Ten.

1.4 The RR/SAP Design versus the Design Specification

RR/SAP fulfills all ten design requirements as defined in 1.2.4, as follows:

1. *Objectivity and Comparability:* RR/SAP is fully objective, transparent, quantitative and based on sound methodologies from decision science, systems engineering and economics. It is general to all classes of infrastructures and many other classes of investment in “hard” assets. Its applicability has been generalized to “soft” investments such as public safety in a limited feasibility assessment reported in Chapter Eight. Moreover, the regional estimates of need and benefits can be compared across regions, provided that all regions used the same approach.

2. *Multi-attribute value objective:* RR/SAP uses a multi-attribute objective function in which both ratio and ordinal scale information is quantified and logically and consistently weighted and applied to all investments options. In addition to the extent to which the demand for infrastructure services is satisfied effectively and efficiently, criteria relating to equity, sustainability, etc. – in addition to security and resilience – are explicitly included and weighted among the selection criteria. Further, the constraints used in the optimization can include such considerations as geographic distribution, minimum investment in certain classes of alternatives, meeting of prior commitments, etc.

3. *Public and owners’ perspectives:* The same engineering-economics and regional systems models and scenarios are used to estimate risks and resilience and to value new investments from both perspectives, based on common methods of estimating vulnerabilities, threat likelihoods, down time, but with differentiated estimates of the consequences to each. Benefits and costs to the owner of the systems struck by the adverse event, to other owners whose systems or facilities are impacted, and to the affected public are calculated for each relevant scenario.

4. *Innovation:* RR/SAP accommodates investments in new technologies and alternative infrastructure security and resilience solutions insofar as they are reflected in enhanced performance, reduced risk and/or improved resilience, or other elements of the multi-attribute objective.

RR/SAP accommodates investments in new technologies and alternative infrastructure security and resilience solutions...

5. *Uncertainties:* RR/SAP reflects uncertainties in two ways: First, it includes a significant number of scenarios representing alternative possible futures, in both the baseline estimates and in the cases where the proposed investments are made. The investments are evaluated individually and in combinations to define their unique contributions to the alternative future scenarios. Second, the models used are all amenable to systematic sensitivity analyses at all levels, e.g., the weightings applied to the criteria in the AHP, the performance of investment alternatives in the engineering-economics models and the performance of whole infrastructure systems and interdependent regional systems/economics models. Future methodology advances may permit movement from scenario analysis with single-point estimates to full probabilistic treatment of uncertainties in risks, performance and portfolio optimization. These advancements exceeded the scope of the present project but should be regarded as desirable for later iterations.

6. *Dependencies:* RR/SAP may be unique in explicitly capturing the dependencies and interdependencies within and across

infrastructure systems, especially at the metropolitan level, but conceivably extending also to multi-state regions, the nation and beyond. It also explicitly captures the logical linkages among the investments, e.g., the hydropower plant and the dam, the bridge and the road that leads to it.

7. *Comprehensiveness:* RR/SAP values infrastructure investments from the perspectives of both the owners and regional public, readily identifying public goods and externalities. The method permits examination of the business case for the investment from the owner's perspective so the owner can be encouraged to make the investment when it is justified. It examines the value from the perspective of the public so that public agencies can make high-value investments, directly or through partnering with the owner or others.
8. *Portfolio:* RR/SAP considers full portfolios of investments in full budgetary and regional contexts. Projects are analyzed and selected in the full context of the regional portfolio of existing and new infrastructure. The major dependencies and interdependencies are modeled to incorporate these relationships in the regional models and the resulting synergies are included in the benefit estimation. The portfolio is capable of drawing from multiple budget pools, funding multi-year projects partially, and meeting a variety of constraints, e.g., budgets, project linkages, multi-year commitments, geographic distribution, etc.
9. *Defensible:* RR/SAP meets all standards of economics, engineering and decision science and exhibits exceptional transparency, objectivity and consistency, permitting directly comparable estimates of all risks, resilience levels, benefits and costs.
10. *Simplicity and Credibility:* RR/SAP is capable of being applied by engineering, analytic, budgeting and planning staffs and communicated directly to key decision-makers – whether private sector, federal funding agencies or state and local governments, infrastructure owners – with a minimum of outside expertise or training, using data that are readily available. The inherent transparency and common-sense logic permit analysts and decision-makers to develop credence in the results of the approach by conducting any number of "what-if" analyses and comparing the results with their own direct knowledge. At the same time, the models are widely used so that experts can be readily located to assist with any training or modeling modifications that might become necessary from time to time.

This report shows that an infrastructure investment methodology can be developed that is capable of evaluating a multitude of diverse proposals while screening out the least promising and ranking the remaining projects according to multiple and varied criteria. Realization of this important goal has two requirements. One is consensus building within organizations that RR/SAP can contribute to better decision-making and convincing decision-makers that their performance will improve by using this approach. The other is continued development of the methodology. The present project is an in-depth feasibility study; it demonstrates that the process is both practical and valuable in meeting challenges that have been thus far ignored. Specific improvements, however, are required in every element of the approach, as is the integration of these improvements into a user-oriented package. These improvements are sketched in the remaining chapters.

Both paths are necessary. When decision-makers gain appreciation and acceptance of the need for this methodology, it must be available and mature enough to meet their expectations for decision support.

1.5 Benefits of Developing and Using RR/SAP

Introduction of a methodology that supports rational infrastructure decision-making will bring discipline to the jumble of processes by which America now makes these vital investments. It will reject “bridges to nowhere” early in the process, expose self-serving proposals and highlight those that are sound. It will elevate emerging values of safety, security, resilience, sustainability to their rightful position as decision criteria.

In the near term, the quality and consistency of infrastructure investment proposals, plans and capital budgets will improve. The reality of interdependencies and the logic connecting investment to the social benefits would be clearly defined, options would be compared, and strategic portfolios will be defined on regional and national scales.

Over the longer term, the outcomes will be measured by the quality and reliability of infrastructure services provided, the provision of new infrastructure services to a growing population, reduction in the number and duration of service denials and reduction of unit costs of the service as new, more efficient assets replace worn and obsolete ones. The primary outcome of use of RR/SAP will be a marked increase in the true value of investment in new and renewal infrastructures. Regional economies will expand in sustainable, equitable ways; safety, security and resilience relative to man-made and natural events will be materially enhanced; cascading infrastructure failures will be less likely and less frequent; and fewer “wrong” projects will absorb scarce resources. The results would increase the efficiency and competitiveness of American industry and contribute to the quality of life of all our citizens.

In brief, such an approach would bring “more bridge for the buck, more dam for the dollar, more levee for the levy.” It would delineate the difference between investing hundreds of billions of taxpayer and ratepayer dollars well and spending them poorly, between a significantly higher quality American infrastructure base and risking economic and social stagnation over the rest of the present century.

CHAPTER 2

The Decision Contexts of Security/Resilience Analysis and Their Design Requirements

2.1 Introduction

2.1.1 Who Provides American Infrastructure?

In the United States, infrastructure services are provided by both private and public – federal, state and local – organizations. As shown in *Table 2.1*, these organizations specialize in the services they provide. Data from 2008 are presented because that is the latest year available for private outlays. The public sector dominates capital expenditures in transportation, by far. The majority of federal and state infrastructure outlays are in highways alone. Indeed, in Congress, the word "infrastructure" is sometimes synonymous with "highways." Local governments also invest significantly in roads and highways, but dominate mass transit, water/wastewater services and, of course, the provision of public safety and emergency services (not shown in the table). The private sector provides energy and telecommunications, operating in both competitive (e.g., power generation) and regulated (e.g., local power distribution) markets. If security/resilience analysis is to be introduced, it will be through these organizations.

All these critical infrastructures come together in the most intense interdependencies in metropolitan regions, where the danger of cascading failures is greatest and the majority of the population resides. Managing security and resilience for such regions often requires the metropolitan form of government (combining county and municipal governments), regional authorities, or regional public-private partnerships. Even when none of these forms of regional organization is available, the solutions to resilience and security challenges often necessitate at least *ad hoc* regional cooperation across jurisdictions and the public-private interface. For that reason, we have adopted the regional perspective to define the decision context and the design requirements it imposes.

2.1.2 The Budget as Point of Impact

Nothing significant happens without cost and no costs are incurred in the modern organizations – local, state, or federal governments (or virtually all businesses of any size) – without being approved in either the operating or capital budget. The decisions that go into constructing

Table 2.1 **Federal, State, Local and Private Capital Outlays for Lifeline Infrastructures**
(Billions of 2008 U.S. Dollars)

		Federal [1]	State [2]	Local [2]	Total Public	Private [3]	Total
Transportation		78.9	63.0	37.7	179.6	32.1	**211.7**
	Ground	50.8	61.7	26.5	139.0	14.5	**153.5**
	Air	19.6	0.8	9.6	30.0	14.9	**44.9**
	Water	8.5	0.5	1.6	10.6	2.7	**13.3**
Utilities		11.1	3.4	34.6	49.1	104.3	**153.4**
	Water & Wastewater	9.3	0.7	34.1	44.1	0.0	**44.1**
	Energy	1.8	2.7	0.5	5.0	0.0	**5.0**
Communications		0.0	0.0	0.0	0.0	102.6	**102.6**
Total		**90.0**	**66.4**	**72.3**	**228.7**	**239.0**	**467.7**

[1] http://www.gpoaccess.gov/usbudget/fy08/pdf/hist.pdf
[2] http://www.census.gov/compendia/statab/2012/tables/12s0437.pdf
[3] http://www.bea.gov/iTable/iTable.cfm?ReqID=10&step=1

these budgets determine what gets done and what does not. Outlays to enhance security and resilience may appear in either budget. In general, activity programs are found in the operating budget and longer-term investments in construction, physical plant (new and major rehabilitations) and durable equipment comprise the capital budget.

For the RR/SAP to contribute to the security, resilience and value of a region's expenditures, it must be designed from the start to be useful in these budgeting processes. In non-federal agencies, operating budgets contain expenditures of a short-term nature, usually one year or less, for the daily operating functions of government. Public sector capital budgets contain funds for major investments in durable (multi-year) assets. In businesses, the equivalent distinction between operating expense and capital investment is virtually universal: operating outlays are "expensed" as incurred, while capital outlays are "booked" as assets and "expensed" or "recognized" by being depreciated over time as they are "used up." While many municipalities do not formally depreciate their assets, most have adopted the practice of separating the two components of the budget. Most state governments (NASBO, 1999) have separate operating and capital budgets. The two come together when a capital asset requires operating expenses and maintenance to perform its function. Debt service is usually included in operating budgets at both state and local levels.

Nothing significant happens without cost and no costs are incurred in the modern organizations...without being approved in either the operating or capital budget.

To pay for durable assets over the extended time of their service, state and local government capital investments are usually financed through bonds of various sorts, backed by general revenue, user fees, etc., although a number of "creative finance" alternatives have been introduced over the last two decades.

Table 2.2 **Public Budgeting Process Reform Stages**

Period	Budget Process Concept	Emphasis
Early 1900s	Line-item budget Executive budget	Control
1950s	Performance Budget	Management Economy & efficiency
1960s	Planning-Programming-Budgeting System (PPBS)	Planning Evaluation Effectiveness
1970s & 1980s	Zero-based budgeting (ZBB) Target-based budgeting (TBB) Below-base budgeting (BBB)	Planning Prioritization Budget reduction
1990s	New performance budgeting	Accountability Efficiency & economy

Source: Tyler and Willard, 1997.

Taxes, fees and grants from higher levels of government generally fund operating budgets.

The federal government has only an operating budget, which includes multi-year capital items as regular annual appropriations. This practice has been controversial for decades, but the politics of changing to separate operating and capital budgets have never been passed. If the proposed infrastructure bank becomes a reality, its portfolio may come to be seen as a sort of capital budget. Virtually all corporations and most other businesses use both operating and capital budgets, with operating budgets funded by revenues and capital budgets by a mix of equity capital and debt of various types.

2.1.3 Budgeting Processes

The process of budgeting in U.S. public agencies has evolved from very loose processes in the nineteenth century, marked by various forms of corruption to an increasingly analysis-based process stressing planning, performance and accountability. Tyler and Willard (1997) trace this evolution (*Table 2.2*) through a series of phases through which each was advanced as reform on the abuses of the previous phase.

Early twentieth century reformers promoted the use of line-item and executive budgets to consolidate control in the hands of the chief executive. *Line-item* budgets were itemized by the type of expenditure, e.g., labor or equipment, within executive departments. The *executive budget* placed responsibility for developing the budget in the hands of the executive and organized by departments as steps toward control and accountability. The budget served as a proposal to the legislative branch, which could approve or amend it.

In the 1950s, *performance budgeting* introduced a focus on what government does rather than items of expenditure, pointing to outputs of departments and accomplishments. *Program Planning Budgeting Systems* (PPBS) emphasized longer-range planning, quantitative analysis (especially benefit/cost analysis and cost-effectiveness analysis) and performance assessment. The objective was to budget to accomplish specified goals in the most efficient and effective way. Zero Base Budgeting (ZBB), Target Base Budgeting (TBB) and Balanced (or Below) Based Budgeting (BBB) were all variations on program budgeting, but with emphasis on base, or irreducible budgets as the starting point, forcing planners and analysts to justify their programs from a base level, often set at zero. *New performance budgeting* builds on the earlier performance budgeting, but with an emphasis on results or consequences to citizens from the direct outputs of the programs. Many of the advances in budget processes were drawn from successful innovations in the private sector.

Each of these changes was not a substitution for, but accretions to earlier processes. Thus, we see the basic line-item executive budget as the core process today, with elements added on to make it more advanced.

A similar evolution has taken place in corporations, with budgets moving from simple lists of authorizing expenditures to increasingly more objective and analysis-based versions. *Enterprise risk management* (ERM) is currently the most advanced stage, business process that integrates risk and portfolio analysis/management with operations as a single holistic risk package, which is actively managed on a daily basis. These budgets are based on in-depth assessments of all possible outcomes (up-side successes as well as down-side failures) of each major program or project under all possible circumstances. Advanced portfolio optimization techniques permit them to identify and fund the specific combinations of programs and projects that generate the greatest returns on investment at a level of risk that is tolerable to its management and board. These techniques are especially advanced among some of the leading energy and telecommunications companies.

Many of the advances in budget processes were drawn from successful innovations in the private sector.

For example, ERM systems for several major energy companies balance the risks and returns of programs as diverse as: active trading in energy commodities using futures and derivatives; daily operations of generation, transmission and distribution of natural gas and electric power; massive investments in construction and plant acquisitions with 40-year productive lives; and exploration and development of natural gas prospects. This huge range in timeframes, magnitudes of risks and payoffs and total capital at stake require highly sophisticated models of virtually all, with common metrics of benefits and risks. Of course, not all energy and telecommunications are this sophisticated and still use variations of the same general processes used in the public sector.

For RR/SAP to have an impact on these budgeting processes, it must meet their respective requirements. For advanced corporate planning and budgeting processes, this is largely a tailoring to the requirements of the specific organization. The foundation for using risk analysis in budget decisions is well established. The concept of resilience and examining the full external consequences of their decisions, however, is probably new to most private sector organizations. For virtually all public-sector infrastructure organizations and chief executives, risk-based planning and budgeting are relatively new.

To understand the processes of budgeting on a metropolitan scale well enough to define specific design requirements for RR/SAP, we examined the process as carried out in a relatively large metropolitan government, a large city, a large county and a smaller city. The amalgam of these is here called Metro City because it is not, strictly speaking, the exact process of any particular city. Metro City's processes are for illustrative purposes only.

2.2 Metro City's Budgeting Process

When we look at Metro City's budgeting process, it is important to remember that each city or county government approaches its annual budget process somewhat differently. Such differences reflect government structure, planning philosophy, economic necessities and historical precedent (Huddleston, 2005). That said, the process outline below reflects key elements that are common to budget planning across metropolitan areas of different sizes and structures.

2.2.1 *Overview*

The Metro City budget is the chief legal planning document for the city for the upcoming fiscal year. The mayor of Metro City is charged with setting the context for the budget, articulating the key policy priorities both broadly (i.e. more investment in public safety) and specifically (building of a highway overpass) and identifying the funding resources available as well as limitations on those resources (Huddleston, 2005). The mayor is concerned with both revenue and expenditure, balancing public opposition to higher tax revenues (in the form of property taxes) with the needs of the city to ensure the provision of public services. The mayor, as steward of the enterprise budget, is also in touch with the governor's office about balancing the city budget with state funds.

...it is important to remember that each city or county government approaches its annual budget process somewhat differently.

The budget context is communicated as a set of budget instructions to city department heads and budget officers. Metro City's mayor also publicly announces the major initiatives and budget line items in an annual public address to the city's residents and local media.

Metro City's government has both operating and capital budgets. The operating budget follows an annual schedule controlled by local law, while the timing of the capital budget schedule is subject to the mayor's discretion. Both processes are managed by the budget office, a component of the finance department, and are staffed by a budget director, a deputy director for the capital budget and budget examiners who review both capital and operating requests from the respective government departments. Each department contains one or more specialized capital and/or operating budget experts who work with the department's management and its budget examiner to prepare the budget submissions. In the capital budget, construction estimators and urban/regional planners in the general services and planning departments conduct additional reviews.

2.2.2 *Planning*

Both budgets are disciplined by planning processes. In Metro City, this consists of the Strategic Business Plan (SBP). Each department prepares a set of planning documents following a standardized format that lays out the department's operations as a long-term (3-5 year) mission, based on strategic goals and "lines of business" to perform the mission and performance measures to gauge progress. Individual lines of business are responsible for three levels of reporting: demand for services, outputs of services and results.

The SBP provides the structure for the accounting system, performance-informed budgeting, performance contracts, employee performance plans, regular evaluations from individual employee performance to department-wide performance, which is regularly published on the city's website for public awareness. The basic justifications for both operating and capital budgets are based on these plans and performance relative to them. While other local governments may use variations on these plans, most have some form of operational and capital planning that is reflected in the respective budgets and performance evaluations.

National professional standards, recognized "best practices" and insurance and bond rating service guidelines also set objectives for the departments to pursue. These are usually captured in the departments' SBPs and are often cited as specific objectives.

In addition to these operating plans, almost all local governments have some form of land-use and economic-development planning. These processes vary widely in the ability of the governments to enforce or implement the plans, but both contribute additional requests for operating and capital plans.

2.2.3 The Operating Budget Process

The operating budget process (*Figure 2.1*) formally begins with the mayor's guidance, issued in January, but the actual process in the departments is continuous. Managers and staffs of the departments note the needs to solve problems or improve performance by defining requirements for funding of various resources ranging from personnel to contracted services, to software and hardware, to new buildings and major equipment. These needs are communicated to management, who, if willing, advises the department's budget expert(s) to estimate the costs of meeting these requirements. If management deems the expenditure justified, it is included in the then-current working version of either the operating or capital budget (or both), to be included in the formal request at the appropriate time.

Most operating budgets begin with the assumption that the next year will closely resemble the current year, with positive or negative adjustments to meet the mayor's guidance and to cover any new initiatives or extraordinary situations. The mayor's guidance usually includes any major initiatives he or she wants to pursue as well as general guidelines for increments or decrements that are expected from the departments. Once the guidance is issued, the department budget experts work with departmental management to compile a draft budget highlighting the major decisions the departmental management must make to comply with the mayor's guidance. With these decisions, the budget expert finalizes the budget request and submits it to the budget office in February.

In March and April, the mayor's office (usually the appointed deputy mayor) and the budget office staff review the departments' requests and conduct hearings with the department heads and their budget experts. In these discussions, the department heads justify their requests on a number of grounds, including promises of improving performance on certain key metrics, such as dispatch time for emergency communications, time to site for the fire department, etc. Each department has a set of these performance indicators, a subset of which is published on the city's website. The budget director and examiners seek to understand the requests in detail, so they can represent them in the mayor's decision-making leading to the budget submitted to the council.

By May 1, the mayor submits the proposed budget and corresponding tax levy legislation to the Metro City Council. During May, the council holds hearings on each department's budget, with presentations by the budget office and departmental management.

The legislative process in Metro City requires three readings in council of any legislation before a vote is taken, which occur in later May and June. By June 30, the council must, by charter, pass both the balanced budget and property tax levy ordinances. The new fiscal year starts July 1, immediately after which the departmental budget experts translate the new budget into specific allocations to the respective divisions and offices of the department. This detailed reconciliation of the operating budget takes about one month, but the respective offices continue operating based on general guidance that accompanied the ordinances. As the fiscal year progresses, each department measures its performance relative to specific metrics, such as response time for public safety departments, feet of new sidewalk built for public works, etc.

2.2.4 The Capital Budget

Most major local governments have annual capital budgets, while others have one that is developed when the needs arise. Metro City takes up the capital budget at the initiation of the mayor, who usually elects to follow an annual process (*Figure 2.2*).

As with the operating budget, the departments are continuously developing elements for the next capital budget based on their long-term plans and emerging investment needs. The departmental budget experts, often assisted by engineer/ architect firms and/or the general services agency’s cost estimators, assemble the draft requests for capital outlays. Department management reviews these requests to select the

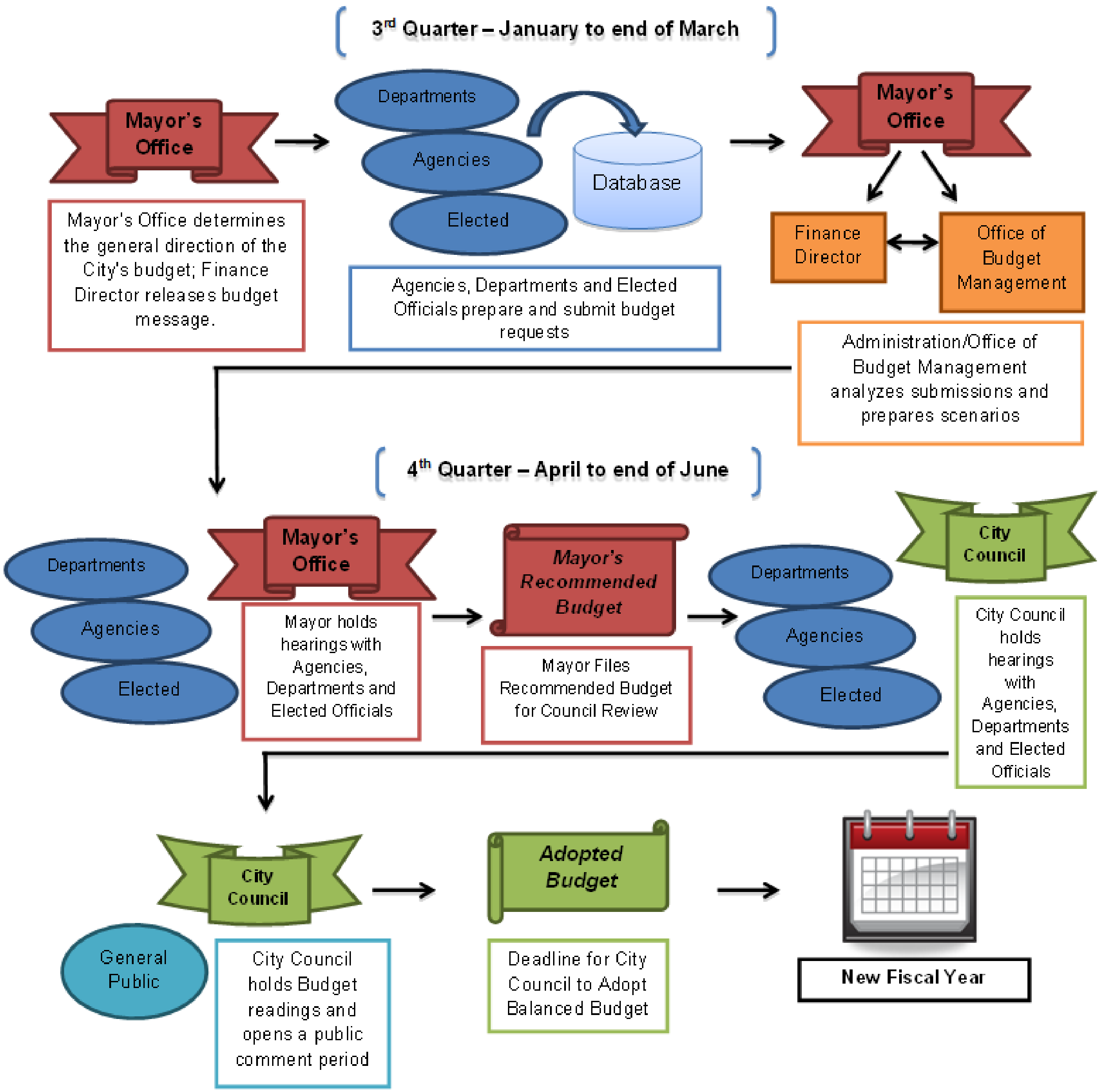


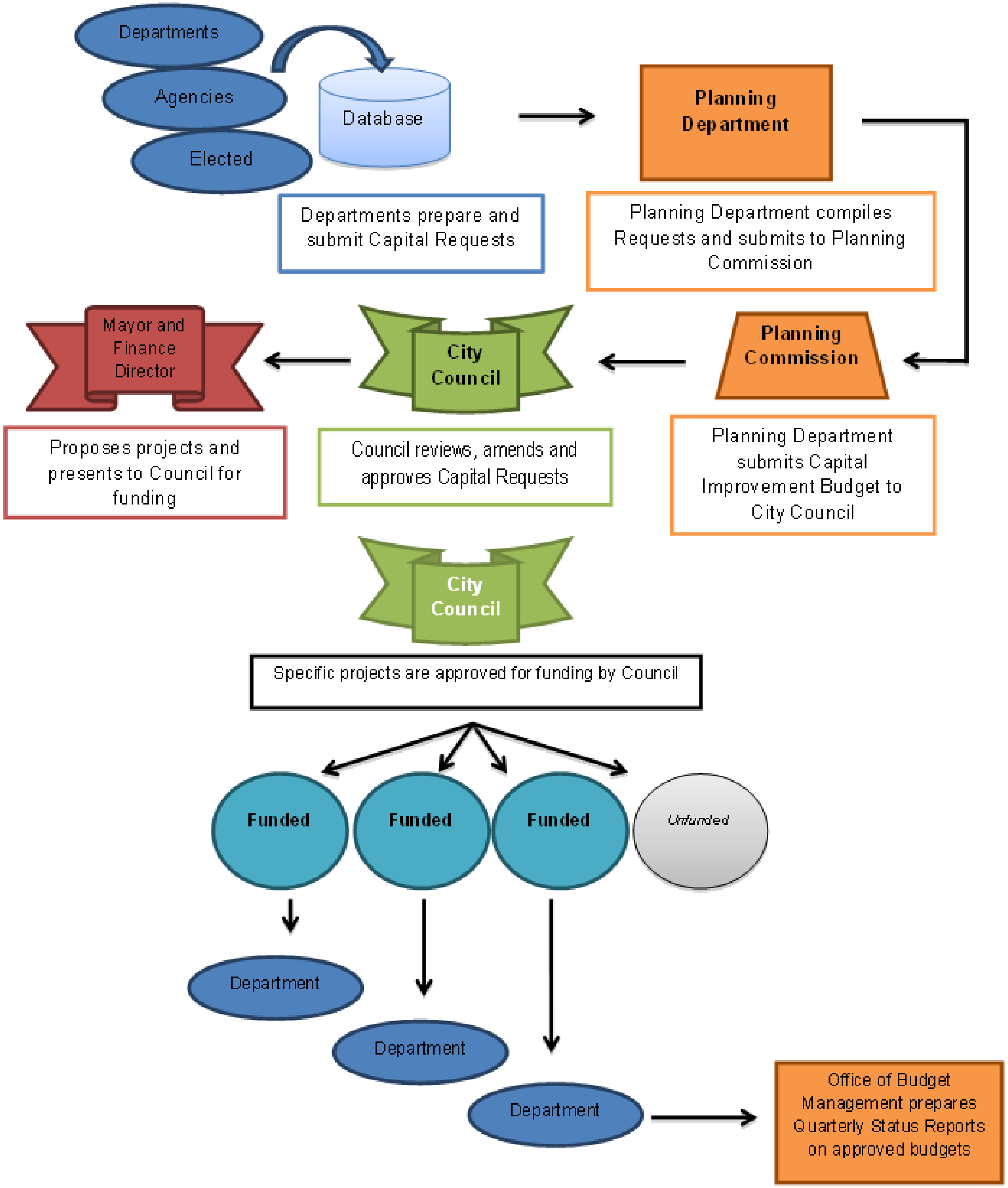
Figure 2.1 **Metro City Operating Budgeting Process**

items for inclusion in the department's capital request.

The formal capital requests are submitted to the planning department, which compiles them into the official capital plan, a multi-year plan. This document is a repository for the "needs and wants" of a capital nature, without assurance of future funding. By May 15 of each year, the planning department submits the capital plan to the Metro City Council, which reviews and approves it by June 15.

When the mayor issues a formal capital budget call, he or she, along with the finance director, present to the council a subset of the requests in the capital plan for specific funding. The council funds selected requests on a project-by-project basis for all major outlays. Smaller, more routine capital expenditures such as vehicle replacement

Figure 2.2 **Metro City Capital Budgeting Process**



The budget offices of many local governments also express keen interest in adding risk and resilience analysis to their standard planning and performance issues as addressed in departmental budgets.

are dealt with as a group. All requested items that are not funded remain in the capital plan until funded or withdrawn by the departments. The departments implement the funded projects using the standard procurement processes and the budget office monitors and reports progress quarterly.

2.2.5 The Status of Risk and Resilience in Planning and Budgeting

Most local governments regard risk as the requirement for insurance or self-insurance funded reserves and the avoidance of legal liabilities. The required planning and budget preparation processes do not include formal risk analysis of any kind. Avoided loss is seldom cited as justification for expenditure, but avoided or reduced outages or service delay or denial is frequently cited by time-sensitive public safety and infrastructure services as reasons to fund specific requests. Many of the performance measures used by public safety agencies, for example, are stated in response-time terms. In addition, employee safety is accorded a very high priority, frequently cited in budget justifications.

The budget offices of many local governments also express keen interest in adding risk and resilience analysis to their standard planning and performance issues as addressed in departmental budgets. These offices often recognize that they are uniquely able to address issues that affect multiple agencies, such as infrastructure interdependencies. In Metro City, the budget director chairs the Long-Term Planning Committee, which is made up of the department heads.

2.3 Lessons from the Case Study for Design of a Regional Resilience/ Security Analysis Process

2.3.1 Purpose of Section

In order for the RR/SAP to be effective, it must be architected using a set of design principles that are (1) compatible with existing processes and (2) enhance decision-making in a way that participants at all levels – politicians, policymakers, risk analysts and field staff – can benefit. This section reviews the case study to derive the basis for the design specifications in the next section.

2.3.2 Incrementalism and New Initiatives

Metro City resembles most modern local governments and many states. It exhibits all of the budget process phases. It has an executive responsible for the process, with specific costs justified by line items, linked with programs and plans defended on the basis of performance in both outputs and results. It lacks formal risk or resilience analysis, but does defend selected expenditures relative to response time and/or outage avoidance.

The budget process for Metro City outlined above reflects current practice but also suggests that conventional budgeting is prone to incrementalism (Wildavsky, 1964). As Wildavsky notes in Grove:

> Budgeting turns out to be an incremental process, proceeding from an historical base, guided by accepted notions of fair shares, in which decisions are fragmented, made in sequence by specialized bodies, and coordinated through repeated attacks on problems and through multiple feed mechanisms (Grove, 1965).

More contemporary research suggests that budgeting can be modeled as a process following punctuated equilibrium theory (PET), whereby long periods of equilibrating incremental change in budgets are “punctuated” by shocks to the system (change in levels of funding) which lead to significant changes in funding priorities. Jordan (2003) has studied local government budgets through the lens of PET and found that routine operating/maintenance expenditures are less prone to punctuation than developmental expenditures that are geared toward economic expansion. The difference in punctuation is significant for investments in resilience and risk reduction programs because such expenditures are likely to be considered routine expenditures and hence subject to cutting in tight budgetary environments.

One significant exception to this is when the metropolitan region has experienced a major trauma of a major natural hazard or human-caused event. Then, risk- and resilience-oriented expenditures are much more likely to seen as high priorities for immediate action.

Jordan (2003) also highlights key differences in capital and operational budgets. Operational budgets are short-term, tactical expenditure plans, driven by service delivery and maintenance within the current fiscal year. Expenditures are incurred and assets used up immediately. Such line items are often individually smaller in amount, but in aggregate, can be substantial. Thus expenditure authority may be more highly distributed across the municipal hierarchy with multiple stakeholders determining the use of funds and amounts requested often for their individual departmental or unit purposes, as opposed to a collective goal.

On the other hand, capital expenditures are multi-year investments usually of larger size designed to achieve strategic goals often around economic development, large-scale cost reduction, or security/resilience enhancement. The larger size and longer time horizon means that there is greater scope for cross-departmental collaboration and breaks with the incremental past. The implications for RR/SAP are that, while some resilience/security issues may be included incrementally in operating budgets (e.g., changes in operations or procedures), major new initiatives will be expressed in both operating and capital budgets (e.g., acquisition and installation of emergency generators in the capital budget, with fuel and labor to exercise and maintain them in the operating budget).

...expenditure authority may be more highly distributed across the municipal hierarchy with multiple stakeholders determining the use of funds and amounts requested often for their individual departmental or unit purposes as opposed to a collective goal.

2.3.3 Bottom-Up, Hierarchical Process of Budget Construction: Defining the Elements of RR/SAP

With the initial guidance from the mayor and finance director on the broad framework of annual metro-wide priorities, the budget construction process begins at the sub-department, unit level with the formulation of a request for operating and capital resources for the coming year. These requests are for the most part based on incremental variations of the previous year’s budget and the extended projections of a three-year planning cycle. The unit-level budget request usually reflects the incremental growth of service demand related to normal population growth and the impact of local revenue generation. The capital budget covers facilities expansion, retrofit and major equipment replacement and improvement. Risk/resilience analysis at the basic organizational unit level would focus on individual facilities and the assets they contain. Failures of specific facilities or assets can set off a series of failures that can affect whole service delivery systems.

Unit-level budget requests with justification are then combined at the division level. In the fire department, for example, there are three divisions: fire suppression, emergency medical services and fire prevention. Each division operates a discrete system that provides a specific service. Each of these service delivery systems can be analyzed based on the internal and external dependencies and threats to disrupt service. This requires a system-wide level of analysis that builds up from the facility/asset level but goes beyond to capture how they work together. Understanding how these systems operate allows insight into other hazards and helps identify points of dependency on other systems.

In this case the three division budget requests are unified by the fire department's budget officer for review and adjustment by the fire chief to assure the most appropriate balance of expenditures to address the immediate and long-term requirement of the department mission and the service systems it maintains. As the executive officer of the department, the chief-director has the perspective and position to see three systems as they operate in the overall region.

Departmental budget requests are forwarded to the budget office, where they are reviewed by a budget examiner with oversight over a relevant area such as public safety. At this level the department budgets can be compared and analyzed for duplication, overlap or inconsistency. It is also possible to examine the comprehensiveness of the multiple department response to crosscutting issues like resilience. The Metro City budget office is able to take a system-of-systems perspective and track the effectiveness of efforts to deal with such crosscutting issues.

The hierarchy of the budget process encompasses the specific detail of asset vulnerability to a range of relevant threats and allows for the coherent structuring of multi-agency initiatives to respond to potential direct and indirect impacts.

Finally, the departmental budgets are consolidated by the mayor's office in concert with the budget office and the department heads. This requires a broad understanding of the challenges and priorities of Metro City. The aggregate benefits to the whole region and their equitable distribution are primary issues at this level. The city council, in its deliberations, is concerned with the same issues, especially the distributional equity.

Following the path of budget construction from broad guidance to the bottom-level units, successively through divisions, departments, and the budget office to the ultimate decisions by the mayor and council suggests that four, *nested*, internally consistent tools are required:

- *Facility/Asset level* for use at the unit level to understand baseline security and resilience challenges and means for dealing with them;
- *System level* for use at the divisional or service-delivery system level up to the departmental level;
- *System-of-systems level* for use at the level of departments in interaction and the budget office; and
- *Regional benefit level* to look at the aggregate effects on the region as an economy at the mayoral/council level.

At each level, the risk-based tools should provide guidance to the budget process on the prioritization of discrete investments and on the combinations of investments necessary to realize significant enhancement of regional resiliency. These tools must be consistent and nested in the sense that each lower-level tool must provide data that the next higher level can use directly and consistently in decision-making.

The hierarchy of the budget process encompasses the specific detail of asset vulnerability to a range of relevant threats and allows for the coherent structuring of multi-agency initiatives to respond to potential direct and indirect impacts. These impacts include crosscutting cascading patterns of infrastructure failure. Each level of the budget process provides the opportunity for interactive and iterative dialogue on the relevance and contribution of specific expenditures to regional resiliency. At the top of the process there is the opportunity to select optimal combinations of departmental investments to best serve regional resilience and risk reduction.

What is required to address security and resilience is a suite of tools that are data-driven, with common metrics that can be compared horizontally across departments, vertically up and down levels of administrative hierarchy and longitudinally across time. Such an approach provides a dynamic, evolutionary picture of risk management within a municipal area allowing risk managers to better assess risk and budget managers to assess the performance of individual risk mitigation investments. The data-driven focus not only reduces ambiguity but de-politicizes investment choices by grounding decision-making in risk metrics.

2.3.4 An Opportunity for Cross-Agency Coordination

As discussed above, the conventional budgeting hierarchy provides limited opportunity for cross-agency coordination because individual departments are, correctly, highly focused on obtaining the resources each believes it needs to carry out its mission in an optimal manner. Yet opportunities exist for budget coordination in areas where performance of multiple departments depends on common resources, such as emergency telecommunications infrastructure during times just after major disruptions of service due to natural or man-made disasters. The experience of calling on other departments for help or the problems of coping with dependencies that were not anticipated heightens the awareness of the need to cooperate and support cross-departmental initiatives.

One traditional vehicle for such collaboration is the Capital Improvement Plan (CIP), a "wish list" of projects proposed by the departments and reviewed by the planning department and commission. This medium-term planning document sometimes sets out investment objectives in cross-departmental initiatives such as public safety, infrastructure, and regional economic development. The CIP articulates a vision for such investments but is generally more of a repository of desirable investments than an inventory of thoroughly analyzed initiatives.

Thus, while the CIP currently serves as an idea bank, it could also serve as a basis for structuring cross-agency coordination. This could be effective only if supported by an objective, quantifiable, risk-based approach for defining and evaluating the cross-agency options.

...opportunities exist for budget coordination in areas where performance of multiple departments depends on common resources

Other opportunities also exist, especially if assessing interdependencies among departments were a standard part of the annual budget process. Only the budget office has the cross-agency, independent, analytic perspective to conduct such analyses, but they are precisely the product of what was defined above at the system-of-systems level of analysis.

2.3.5 Evaluation of Options for Regional Risk Reduction in Highly Interdependent, Complex Infrastructure Systems

As noted earlier, conventional budgeting processes are generally not structured for system-of-systems approaches to risk reduction because bottom-up budget formulation is focused on maximizing resource allocation for individual departments. For example, the mission of fire suppression is assigned to the fire department. However, the accomplishment of this mission is critically dependent on other systems and departments, such as:

- The commercial communications system is critical to the timely initial reporting of fire incidents;
- The public emergency communications system is critical to the dispatch of response assets;
- The public works department's traffic control systems and debris removal systems

are critical to maintaining access to incident sites;

- The police department is critical for controlling traffic and crowds so the fire equipment and personnel can access the site quickly;
- The water department is essential for maintenance of water pressure in the fire hydrant and sprinkler systems; and
- Emergency medical services and hospital emergency rooms may play a vital role in treating victims of the fire or firefighters injured or overcome by smoke.

Each of these systems is critical to the fire suppression mission of the fire department but only two (fire suppression and emergency medical services) are included in the fire department budget. The budgets of the metropolitan government organizations first come together in the budget office, which is the only office potentially charged with maintaining the crucial system-of-systems perspective.

Typically, mission-specific priorities for operating and capital budgets are well administered by the current department level budget process. However, limitations occur when there are significant dependencies or interdependencies between departments. Where the functional and administrative systems are congruent, there is generally good understanding of requirements and ability to coordinate implementation. Difficulties arise at the interface of physical and administrative systems. These interface dependencies require the involvement of the oversight provided by the budget office perspective.

Possibly the most important role for risk-based management and budgeting is the coordination of multi-agency initiatives to reduce potential for cascading failures across systems at the regional scale. The budget office is unique in its comprehensiveness and in its authority. In the iterative process of budget construction, it is possible to introduce the consideration of risk reduction and long-term resiliency at every level through specific guidance. In the hierarchy of the budget process, it is possible to encompass the range of system/department dependencies and interdependencies.

2.3.6 A Vision of a Security/Resilience Process in Evaluating Budget Priorities

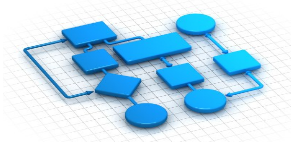
Moving a municipal or metropolitan government from a conventional budget process to a risk-informed approach is a multi-stage effort that requires several systemic changes. One of the key changes is the installation of RR/SAP, the principal information system underlying the risk-based budgeting system.

RR/SAP is hierarchical by nature which allows it to integrate directly into the conventional budgeting processes. At its base level, it provides risk profiles and metrics for individual assets and facilities (e.g., a fire truck, water pump or fire house). The asset manager can monitor replacement of assets, maintain mission readiness, and plan for additional assets as service needs change. At the divisional level, RR/SAP provides a system perspective for assessing risks and resilience of the systems it operates. At the departmental level, RR/SAP provides an aggregate view of risks across a portfolio of assets owned by the department, allowing the budget and risk managers to understand interdependencies and risk correlations among these assets.

Above the department level, RR/SAP looks at interactions among departments and between them and private organizations in the context of service risk, i.e., how changes in operational performance increase or decrease the risks for individual departments and groups of departments coordinating for a common service, like public safety. Finally, the ultimate levels of RR/SAP, likely to be only reviewed periodically by senior municipal officials, come from the system-of-systems and aggregate regional economic perspectives. These are provided so that senior managers can plan for macro-level events such as natural disasters or terrorist threats where expenditures are focused on managing systemic risks that involve coordination among different actors placed at varied levels of the municipal hierarchy.

Making RR/SAP compatible with the budget process means that it is introduced directly into the blood stream of the organization. The analysis of potential resilience/security investments will begin from the bottom up and be effectively integrated into the priorities of the organization. Specific RR/SAP tools for each level of the budget process will simplify its application. At any level of the process, some training of personnel may be required, so RR/SAP should include training materials and implementation assistance.

CHAPTER 3



Defining and Prioritizing Selection Criteria for Security and Resilience Investments & Programs

3.1 Setting Selection Criteria: Choice of Methods

When public authorities, coalitions or regional public-private partnerships allocate resources, numerous specific criteria come into play, reflecting the multiple constituencies and purposes of such organizations. Most businesses, especially those that provide infrastructure services, acknowledge that their strategies for success require balancing multiple, occasionally conflicting objectives. Even “maximizing shareholder wealth” can no longer serve as a singular purpose, as issues of short-term versus long, stability versus volatility, abiding by laws and regulations, attracting talent, environmental stewardship and sustainability, etc., find places among allocation criteria. Further, allocation of resources to programs and capital investments designed primarily to enhance security and resilience must compete successfully with programs and investments for quite different purposes in the general competition for resources.

The challenge, then, is to identify a way to define and prioritize selection criteria for the general allocation of resources under which programs and investments for security and resilience can compete. The overall Regional Resilience/ Security Analysis Process (RR/SAP), introduced in Chapter One, calls for the first step to be to establish decision-makers’ goals, criteria and priorities (*Figure 3.1*). The technology used in setting and weighting objectives and criteria can also be used to integrate the results from other parts of the analysis, specifically Phases 2 through 5 of the Evaluation Cycle, by consolidating all the values into a single weighted value score. The selected process should exhibit certain characteristics, including being explicit, transparent, repeatable, logically consistent, integrable with other parts of the analysis and validly representative of the purposes decision-makers seek.

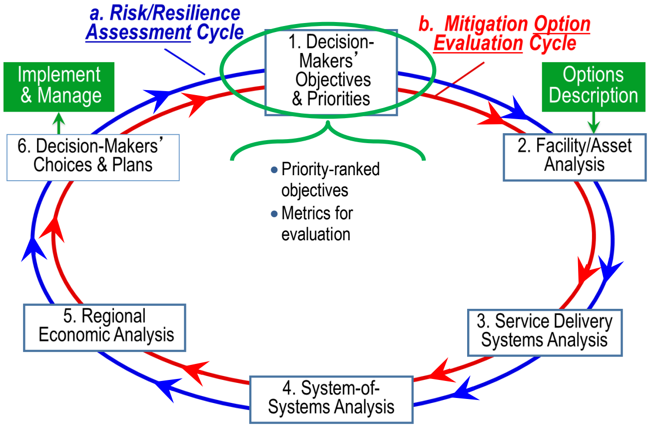


Figure 3.1 **RR/SAP Phase 1: Decision-Maker’s Objectives & Priorities**

Several techniques have been proposed for the class of decision problems encountered in this project, the choice (or ranking) of discrete alternatives relative to two or more criteria. The most venerable are *Multi-Attribute Utility Theory* (MAUT) and *Analytic Hierarchy Process* (AHP). MAUT dates back to von Neumann and Morgenstern's (1944) expected utility theory (EUT) and Savage's (1954) subjective expected utility theory (SEUT), with extensions to multi-attribute utility theory (Luce and Raiffa, 1957) and multi-attribute value theory (MAVT) (Keeney and Raiffa, 1976).

Saaty proposed AHP, an independent alternative, in the 1970s (Saaty, 1980) as a method for dealing with multi-criterion decisions or multi-attribute evaluation in a systematic, consistent manner (Saaty and Vargas, 1982 and Saaty and Alexander, 1989). AHP “provides a structured framework for setting priorities on each level of the hierarchy using pair-wise comparisons, a process of evaluating each pair of decision factors at a given level on the model for their relative importance with respect to their parent" (Decision Lens, 2009). AHP allows decision-makers to prioritize their strategic objectives, evaluation criteria and alternative choices to achieve an overall goal. AHP is simpler to understand, easier to use with real decision-makers, equally sound logically and provides important mathematical attributes that are useful in decisions of allocating resources to multiple options, as opposed to selecting a singular "best" option.

The challenge … is to identify a way to define and prioritize selection criteria for the general allocation of resources under which programs and investments for security and resilience can compete.

An acrimonious academic debate has appeared in the literature regarding the possibility and desirability of "rank reversal" when non-optimal choices are added to the set of criteria. Rank reversal, it is argued, violates transitivity (an axiomatic requirement of MAUT), so renders AHP as "flawed" (Dyer, 1990). Forman and Gass (2001) counter that neither MAUT nor AHP fulfills the axioms of the other – they are independent – and neither has been shown to lead to superior decisions. Under certain conditions, either can lead to "rank reversal," but this can be justified when the addition brings new dimensions to the choice problem. Luce and Raiffa (1957) recognized that some real-world decision problems can demonstrate rank reversal when it changes the decision-makers initial information, but thought of this as a new decision problem. They then limited their attention to decision problems that have no intransitivities.

For the purposes of RR/SAP, it is useful to remember that decision-making will nearly always involve group judgments, including compromises, negotiations, and multiple dimensions. Some degree of intransitivity may be inevitable. The impact of third-party candidates on U. S. presidential elections, for instance, illustrates the fact that introducing a "non-optimal" choice can shift the ranking of candidates if only two had been running. Much of the thinking about decision-making norms assumes an *individual* decision-maker, which is seldom the case in budget decisions in large organizations, public or private.

For resource allocation issues, the primary purpose of RR/SAP, AHP has two desirable characteristics. First, it is a "closed" system in the sense that when criteria are added or deleted, the weights are re-calculated to total to one, whereas, MAUT is an "open" system in which the addition or deletion of criteria results in an increase or decrease in the sum of the weights (Forman and Gass, 2001). This makes AHP more conducive to budget-making, where several options will receive funding in the order of their ranks (or their ranks divided by their cost in the case of Decision Lens). Second, when the criteria are structured as a hierarchy, it is necessary to multiply the priority value (or weight) of a lower-level element with the priority of an upper-level element. Often, it is desirable to use ratio scales[5] for resource allocation problems where alternatives are attached to the lower levels of the criteria hierarchy. AHP uses ratio scale information across the hierarchy of criteria and alternatives, whereas MAUT uses interval information particularly in valuating alternatives (Forman and Gass, 2001). With ratio scales, it is meaningful to say that a priority of

---

[5] Stevens (1946) defined four scales of measurement: (1) nominal, or the ability to discriminate and name items, e.g., categories; (2) ordinal, or the ability to order or rank items in a meaningful series, e.g., college football team ratings; (3) interval, or the ability to describe a quantity in terms where the intervals between any two are the same, e.g., temperature in Fahrenheit or Celsius; and (4) ratio scales, or interval scales with a natural zero, e.g., items that are counted. All arithmetic functions may be used with ratio scales, but only addition and subtraction may be used with interval data and no arithmetic functions can be used with the ordinal or nominal scales – although this error does occur.

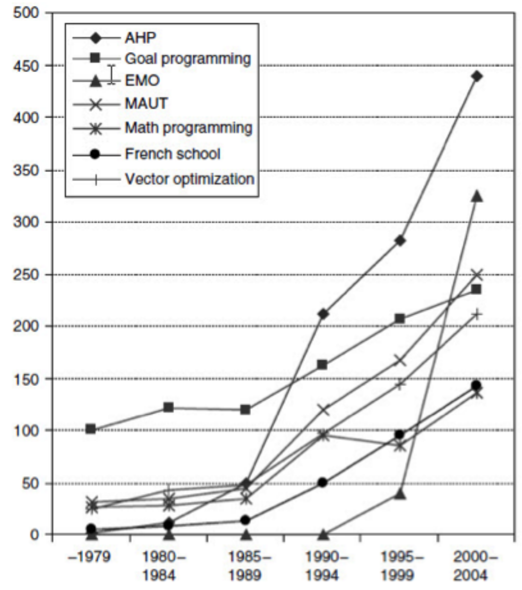


Figure 3.2 **Number of Publications About Leading Multi-Attribute Decision Methods**

0.2 is twice as important as one with a priority of 0.1, which is not possible using an interval scale.

Wallenius, *et al.* (2008) surveyed the publication histories of several methods of dealing with this class of decision problem and noted the significant growth of AHP articles relative to several other methods, including MAUT (*Figure 3.2*). [Note: EMO is "evolutionary multi -objective optimization" and the "French school" includes ELECTRE (in fact a family of methods) and PROMETHEE.]

Gass (2005) found that "AHP has become a widely popular MCDM [multi-criteria decision-making] in the US and in other countries [with] wide acceptance among academics and practitioners…It is the workhorse for solving [MCMD]. The AHP seems to have replaced MAUT and MAVT for solving such real-world… problems" (Gass, 2005).

AHP is widely taught in engineering and graduate business schools and has been adopted as a standard technique for dealing with this class of problems in such diverse settings as Fortune 100 companies (e.g., Pfizer, IBM, 3M, General Motors, Xerox, Kraft, Johnson & Johnson), state and local government agencies (e.g., Washington Metro, Maryland Transportation Agency), U.S. federal agencies (e.g., National Institutes of Health, NASA and the Departments of Defense, Homeland Security, Energy), National Football League teams (e.g., Green Bay Packers) and Major League Baseball teams (e.g., Oakland Athletics) for such diverse purposes as strategic planning, capital budgeting, R&D project ranking, nuclear clean-up, and player selection (Decision Lens, 2011, and Expert Choice 2011).

We chose to use AHP for this project because of its intuitive clarity, ability to readily include both ratio ("hard data") values and ordinal scale judgments (ratings on a directional scale, e.g., good, better, best") as converted to ratio scales, widespread acceptance by both academics and practitioners and ease of use.

AHP allows decision-makers to prioritize their strategic objectives, evaluation criteria and alternative choices to achieve an overall goal.

A number of firms offer versions of AHP software and consulting, one of the largest and most successful of which is Decision Lens Inc., founded and managed by two sons of Thomas Saaty, the inventor of the process. We chose this company to provide software and technical consulting to the present project because of (1) its significant market share, indicating wide acceptance; (2) its approach of providing intensive technical support, minimizing the learning time; and (3) previous, very positive experience with the software and consultants by some of this project's principals. In addition, the Decision Lens approach can be used to integrate the results of several steps of the RR/SAP: displaying the estimates of value from Phases 2 through 5 and rankings of the options developed and evaluated in the RR/SAP Evaluation Cycle as improvements over the current situation as determined in the initial Assessment Cycle. This is a feature that has particular attractiveness if large numbers of options are to be analyzed because it provides a way to integrate all the estimates in a decision-relevant way.

3.2 Analytic Hierarchy Process (AHP) Description

3.2.1 Overview of AHP

AHP begins with the decomposition of the overall goal of the decision into component objectives and subdivision of each of these into component criteria, and so forth to whatever additional levels are needed. Specific metrics are defined for each "end point" criterion. The example in this report uses three levels, but the process could be continued to several more levels to capture the desired level of detail. After the hierarchical structure is built, each element is rated against each of the others at the same level through "pair-wise comparisons" of the relative impact on or contribution to their common "parent," e.g., the criteria to their respective objectives, the objectives to the overall goal. The lowest level of the hierarchy defines the data or judgments that are used to characterize the decision options to be considered. These are combined into "weights" that sum to 1.0. The weights are used to describe the value or priority of the option relative to its contribution though the hierarchy to the overall goal. A consistency index identifies instances of circular logic for correction, so the goals and objectives exhibit a high level of internal consistency even though they may cover highly diverse dimensions.

3.2.2 Steps in AHP in the RR/SAP

AHP has been characterized in several ways, but to be consistent with other tools in the RR/SAP, AHP as used here is described as a series of steps. *Figure 3.3* shows these basic steps, while Section 3.3 contains an extended example. The first five, dark blue boxes represent steps in the process that are completed as the first phase in the RR/SAP; the three lighter blue boxes represent activities undertaken later in the process, but are described here to clarify the full logic of the process.

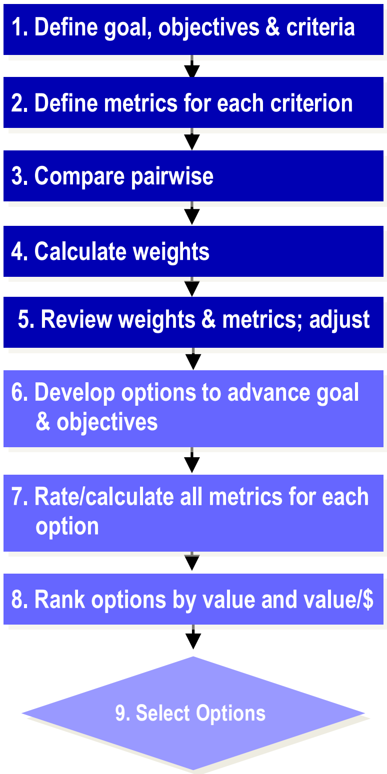


Figure 3.3 **Steps in the Analytic Hierarchy Process**

Step 1. Define goal, objectives and criteria. AHP builds on the well-documented idea that humans think in hierarchical terms, that any system or organization can be understood as a hierarchy in which higher-order elements can be broken down into lower-order elements. In using this idea for defining what is "good" or "valuable," the diverse objectives of a regional jurisdiction or coalition can define a useful set of criteria for resource allocation.

The process is to define carefully the "good" or "value" that the overall decision is to advance, which is a broad statement of what the end result of the correct decision would be. This broad statement is then broken down into its constituent objectives or characteristics. This is done by deconstruction of the overall goal into a set of objectives and then deconstructing the objectives into sets of selection criteria. In both cases, the operational question is: would the substantial advancement of all the constituent parts accomplish the ends of the next higher level?

More than the three levels used here can be added if the decision is more complex or the decision-makers desire a more fine-grained assessment of the options to be evaluated. The resulting hierarchy is usually displayed as a "tree" or organization chart.

Step 2. Define metrics for each criterion.
Specific metrics or indicators are defined for each of the end-points of the hierarchy. These metrics must be specific enough to differentiate among the options with respect to the criterion of objectives it purports to measure.

AHP builds on the well-documented idea the humans think in hierarchical terms, that any system or organization can be understood as a hierarchy in which higher-order elements can be broken down into lower-order elements.

When the criterion is amenable to measurement by a ratio or interval scale, a ratio scale metric (called "numeric" in the Decision Lens software) is assigned, for example, lives saved or dollar losses avoided. The mechanics of doing this are to set the minimum and maximum for the metric, allowing the software to place the assigned value on the scale. When the criterion is more suited to an ordinal scale, a set of descriptive phrases (e.g., very strong, strong, moderately strong, moderately weak, very weak) are assigned. In the Decision Lens software, these are called "verbal" scales. The numeric scales are automatically weighted by the numerical value on the scale (with weights distributed linearly from zero to one), but the verbal (ordinal) scales require weights to be assigned to each level.

Step 3. Compare pairwise.
This step compares the elements on each level of the hierarchy to establish relative weights. The comparison asks which of two elements makes a greater contribution to their common superordinate objective or goal and by how much, as estimated using a scale of 1 (same contribution) to 9 (nine times greater contribution). Groups of decision-makers usually discuss the relative contributions and then rate the pair. The decision-makers rate the comparisons individually and an average is computed. The software has options for ratings to be made anonymously or publicly, at the same time or spread over time, and with raters having the same or differentiated weights in the final rating.

Step 4. Calculate weights.
This step calculates the weights for the elements at each level. When all pairs are compared, Decision Lens calculates the average priority weight. The actual mathematics are complex, involving eigenvectors and matrix algebra, but are easily computed by the software and displayed to the decision-makers. The result can be thought of as the proportion of the votes or the priority each criterion received through the process of pairwise comparisons. If the decision-makers are uncomfortable with the weightings, they may go back and repeat some of the comparisons.

The software also calculates a consistency index. The consistency index reflects the extent to which the ratings avoid circular or contradictory logic and numerical imbalances, e.g., A > B, B > C, but C > A (where > means "is greater than, is preferred to, is more important than"). The consistency index ranges from zero to one; an index value of 0.1 or less is considered acceptably consistent. If an unacceptable index is calculated, the decision-makers may further adjust their ratings to improve the consistency. The software supports these reconsiderations by showing paired comparisons with the greatest mathematical inconsistency and suggesting the direction to move the judgments to improve the consistency.

Major inconsistencies may reveal the need to split some criteria, that is, to modify the statement of the objectives or criteria in Step 1. For example, if the criterion is fruit preference, one might prefer apples to pears to bananas to apples, but this is highly inconsistent. If, however, the criterion were split into "sweetness" and "crunchiness," two perfectly consistent preferences could be recorded, e.g., sweetness: pears > bananas > apples; and crunchiness: apples > pears > bananas. The dimensions of sweetness and crunchiness would need to be weighted for priority, but the whole problem is rendered consistent and the underlying dimensions are clearly identified.

Step 5. Review weights and metrics; adjust.
This is the final review of the criteria and weights. If the group is satisfied, the metrics and weights are ready for use in the decision process. If the group is less than satisfied, it may reconsider any or all the preceding steps and adjust their results. The point is to derive a set of criteria and weights that captures the objectives to be advanced by the decisions to follow. The discussion in this step is whether the full set of goals, objectives, criteria and metrics adequately defines the *value* that the subsequent decisions are to advance.

Step 6. Develop options to advance the goal and the objectives.
This step falls at the beginning of the RR/SAP Evaluation Cycle. The earlier Assessment Cycle has defined the current situation relative to the metrics and decision-makers have designated some elements of the situation as worthy of additional work to improve them. In this step, options that may add value are defined in sufficient detail to allow estimates of their effectiveness as measured by the metrics and the costs of implementing them. Phases 2 through 5 of the Evaluation Cycle make these estimates.

Step 7. Rate/calculate all metrics for each option.
This step is the work of all the rest of the Evaluation Cycle of RR/SAP. The Assessment Cycle has set the baseline of risk and resilience with no new options, where the Evaluation Cycle estimates the improvements the respective options will make. These differences are the values of the metrics and ratings. When weighted and combined, they define the value added by each option. When divided by their cost, they represent the incremental value per dollar of expenditure. These activities are addressed in detail in later chapters.

Step 8. Rank options by value and value per dollar.
This step displays the results of the analyses as options ranked by (1) their total value in advancing the agreed-upon goals and objectives and (2) their value/cost or benefit/cost ratio (i.e., their efficiency in generating value per dollar). (Note that in an advanced risk analysis that captures the full uncertainty in all these estimates, this step would be a portfolio analysis based on Monte Carlo simulation rather than a ranking, in which the value would be balanced against the aggregate uncertainty or financial risk. The analysis would display an "efficient frontier" of feasible option *combinations* for which no greater value could be obtained without greater risk and no lower risk obtained without loss of value.)

Step 9. Select options.
In this step, decision-makers review the rankings in light of the available budget or bonding capacity and select the options to be included in the operating and capital budgets. This is the step all the rest of RR/SAP leads up to and illuminates.

3.3 Example Use of AHP in an Infrastructure Option Selection

A small example problem was developed using the Decision Lens software. This section uses a series of outputs and screen shots to illustrate the logic of the solution through a simple step-by-step application of AHP. Members of the project team adopted the role of decision-makers. The following is strictly an example of the process and not a suggestion for goals and objectives for any real jurisdiction, partnership or organization.

Step 1. Define the goal, objectives and criteria.
The first step is to define the goal, objectives, and criteria the decision-makers will use to select options. In this case, the goal was to "select

Figure 3.4 **Screen Image of Defining Goal, Objectives and Criteria**

- Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan ar
  - Enhance Equity
  - Add Economic Growth
    - Expand employment
    - Expand tax base
    - Increase Attractiveness to Industry
  - Enhance Safety: reduce risk / enhance security
    - Avoid Fatalities
    - Avoid Serious Injuries
    - Avoid Department/organizational losses ($)
  - Improve Resilience: enhance continuity of service
    - Avoid Overall Regional Economic Loss ($)
    - Avoid Service/Function Outages
    - Avoid Direct loss to the public
  - Enhance the Effectiveness & Efficient of Local Government
    - Increase Effectiveness: Net Benefits
    - Improve Efficiency: Benefit / Cost Ratio
    - Augment Tax Revenues

- Population Growth
- Prosperity
- Efficiency of Government Process
- Cost Reduction
- Political implications
- Business improvements
- Likelihood of Success / Risk
- Health, Safety, and Welfare of Citi
- Tax base increase
- Improve opprtunity
- Continuity of government
- Continuity of business operation
- Re-distribute wealth
- Upgrade failing neighborhoods

Courtesy of Decision Lens Inc.

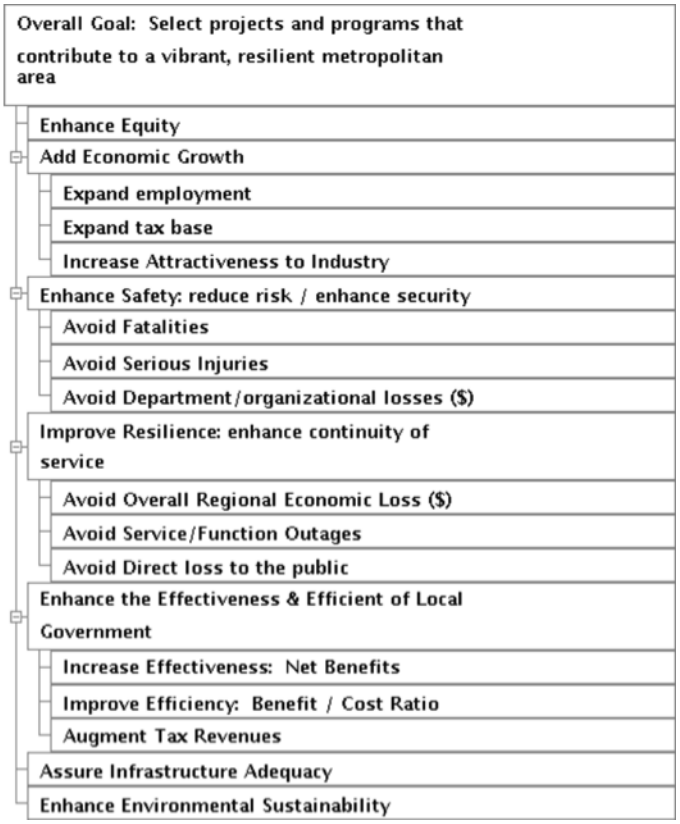
projects and programs that contribute to a vibrant, resilient metropolitan area." Objectives and criteria to advance this goal were developed through a "brainstorming" session in which a much larger list of ideas was offered and discussed. *Figure 3.4* shows the Decision Lens screen used to support this step. The objectives were defined as equity, economic growth, safety, resilience, government effectiveness and efficiency, infrastructure adequacy and environmental sustainability. Several objectives had subordinate criteria, as shown. The software also displays the results of the first step as a "tree" as shown in *Figure 3.5*.

Step 2. Define Metrics for Each Criterion. To define specific criteria, each criterion or end-point objective was discussed to determine an appropriate metric. For inherently qualitative metrics, ordinal scales such as in *Figure 3.6* were developed and the point values of each level assigned. Any specific value could serve because nothing requires the intervals to be equal.

If the criterion is inherently quantitative in nature, either interval or ratio scales, the natural metric was defined. In this case, the full range of expected values was assigned, as shown in *Figure 3.7*. The values estimated for each will be placed linearly between the two defined end-points. It is important to set them to accommodate the full range of estimates, but to avoid setting them any more broadly. If set more broadly than actually used causes only a portion of the full scale to be used, which could systematically cause under- or over-valuation inadvertently.

This process is continued until all criteria and end -point objectives have been assigned metrics. Defining metrics at this point in the process assures that metrics can be determined for each objective or criterion. If no genuinely acceptable metric can be defined, the objective or criterion may be too vague to be used, signaling the need to rephrase or delete it.

Figure 3.5 **Example Hierarchy of Goal, Objectives and Criteria**

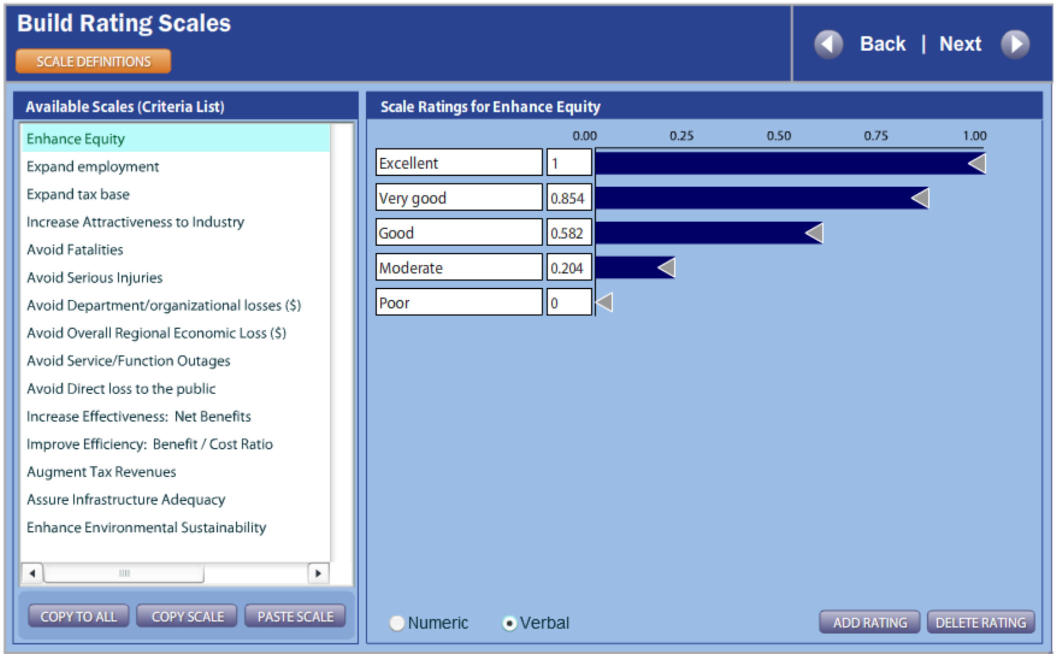


Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan area

- Enhance Equity
- Add Economic Growth
  - Expand employment
  - Expand tax base
  - Increase Attractiveness to Industry
- Enhance Safety: reduce risk / enhance security
  - Avoid Fatalities
  - Avoid Serious Injuries
  - Avoid Department/organizational losses ($)
- Improve Resilience: enhance continuity of service
  - Avoid Overall Regional Economic Loss ($)
  - Avoid Service/Function Outages
  - Avoid Direct loss to the public
- Enhance the Effectiveness & Efficient of Local Government
  - Increase Effectiveness: Net Benefits
  - Improve Efficiency: Benefit / Cost Ratio
  - Augment Tax Revenues
- Assure Infrastructure Adequacy
- Enhance Environmental Sustainability

Courtesy of Decision Lens Inc.

Figure 3.6 **Example of Metric Definition for Qualitative Metrics**



Available Scales (Criteria List)

- Enhance Equity
- Expand employment
- Expand tax base
- Increase Attractiveness to Industry
- Avoid Fatalities
- Avoid Serious Injuries
- Avoid Department/organizational losses ($)
- Avoid Overall Regional Economic Loss ($)
- Avoid Service/Function Outages
- Avoid Direct loss to the public
- Increase Effectiveness: Net Benefits
- Improve Efficiency: Benefit / Cost Ratio
- Augment Tax Revenues
- Assure Infrastructure Adequacy
- Enhance Environmental Sustainability

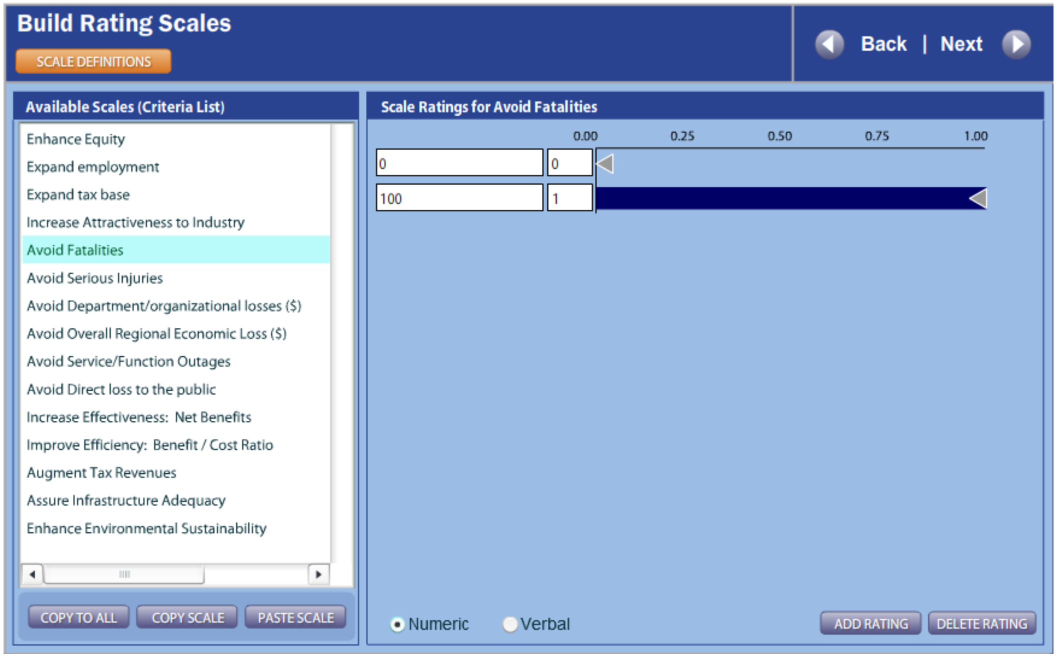
Scale Ratings for Enhance Equity

Rating	Value
Excellent	1
Very good	0.854
Good	0.582
Moderate	0.204
Poor	0

○ Numeric ● Verbal

Courtesy of Decision Lens Inc.

Figure 3.7 **Example of Metric Definition for Quantitative Metrics**



- Enhance Equity
- Expand employment
- Expand tax base
- Increase Attractiveness to Industry
- Avoid Fatalities
- Avoid Serious Injuries
- Avoid Department/organizational losses ($)
- Avoid Overall Regional Economic Loss ($)
- Avoid Service/Function Outages
- Avoid Direct loss to the public
- Increase Effectiveness: Net Benefits
- Improve Efficiency: Benefit / Cost Ratio
- Augment Tax Revenues
- Assure Infrastructure Adequacy
- Enhance Environmental Sustainability

0	0
100	1

● Numeric ○ Verbal

Courtesy of Decision Lens Inc.

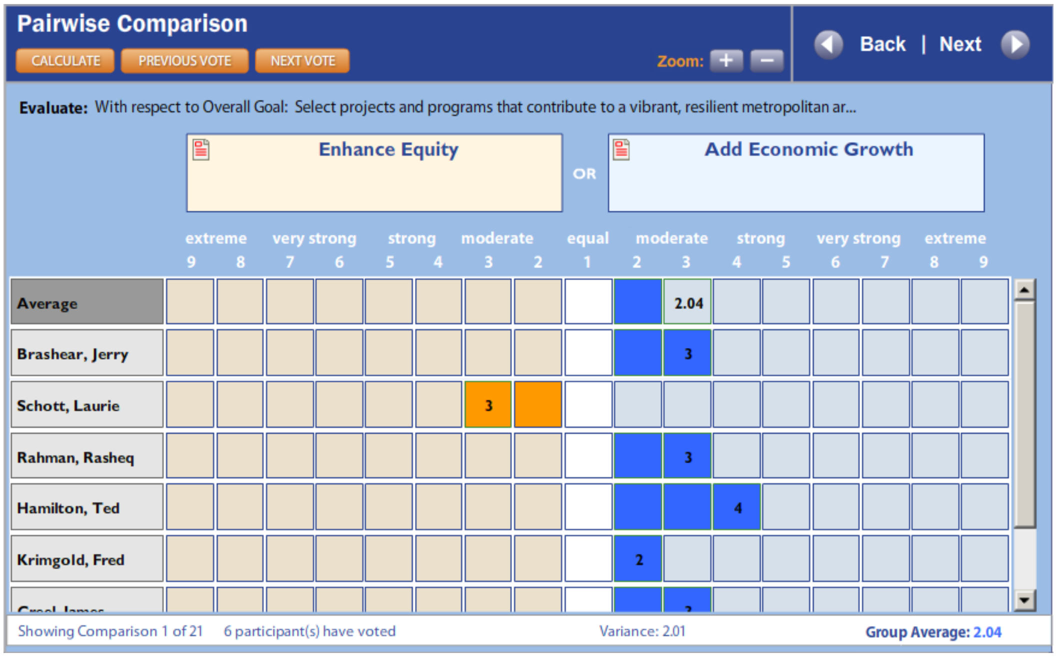
The full definitions of the goal, objectives, criteria and metrics used in this example are reproduced as Annex 3A. Annex 3B contains the scales used as metrics.

Step 3. Compare pairwise.

In this step, the elements at each "branch" of the hierarchy are compared with one another using a nine-point scale, indicating the degree one was preferred to or more important than the other. A rating of one means they are equal, while a higher number indicates the favored item is preferred by that ratio. For example, a rating of three indicates the preferred item is three times more important than the less important item. The decision-makers discuss each pair, then make independent judgments, as shown in *Figures 3.8* and *3.9*. The judgments are averaged and displayed. This process is repeated for each pair. In the present example, this requires 21 comparisons. (The software also permits the judgments to be made anonymously, at different times and places – using the online version – or with the respective stakeholders weighted for importance in calculating the average.)

In *Figure 3.8*, the judgment of the decision-makers was a general consensus, with one outlier being that economic growth was more important than equity by about double. The discussion was one of "expand the pie" versus "divide the pie," with "expanding seen as the prior step to

Figure 3.8 Example of Pairwise Comparison (Enhance Equity Vs. Add Economic Growth)



Evaluate: With respect to Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan ar...

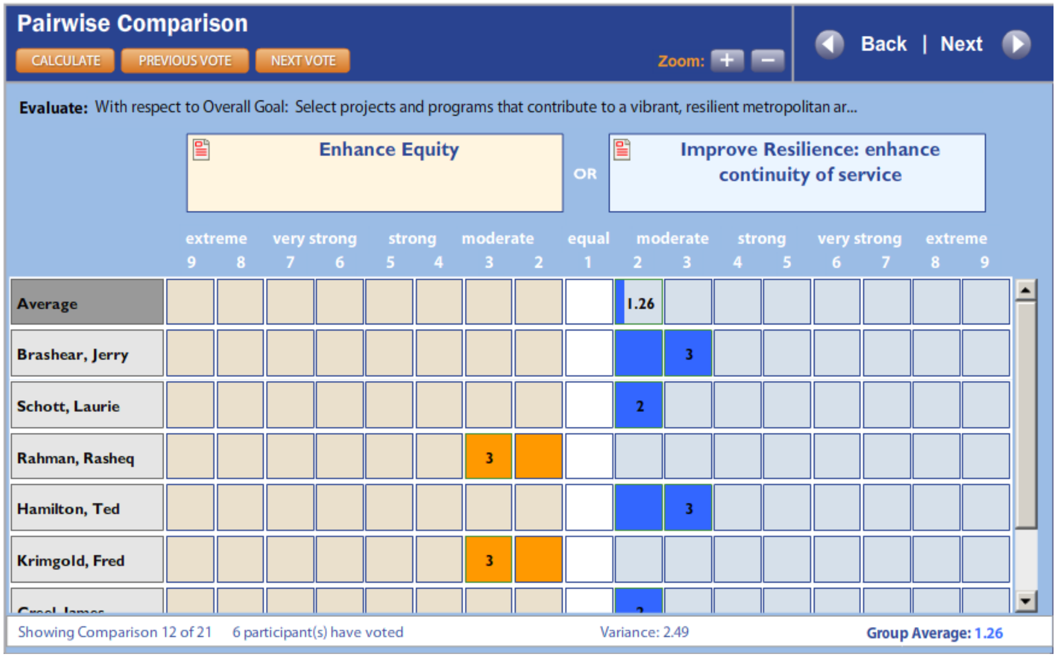
Enhance Equity OR Add Economic Growth

	extreme		very strong		strong		moderate		equal	moderate		strong		very strong		extreme	
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Average										🟦	2.04						
Brashear, Jerry										🟦	3						
Schott, Laurie							3	🟧									
Rahman, Rasheq										🟦	3						
Hamilton, Ted										🟦	🟦	4					
Krimgold, Fred										2							

Showing Comparison 1 of 21   6 participant(s) have voted   Variance: 2.01   **Group Average:** 2.04

Courtesy of Decision Lens Inc.

Figure 3.9 Example of Pairwise Comparison (Enhance Equity Vs. Improve Resilience)



Evaluate: With respect to Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan ar...

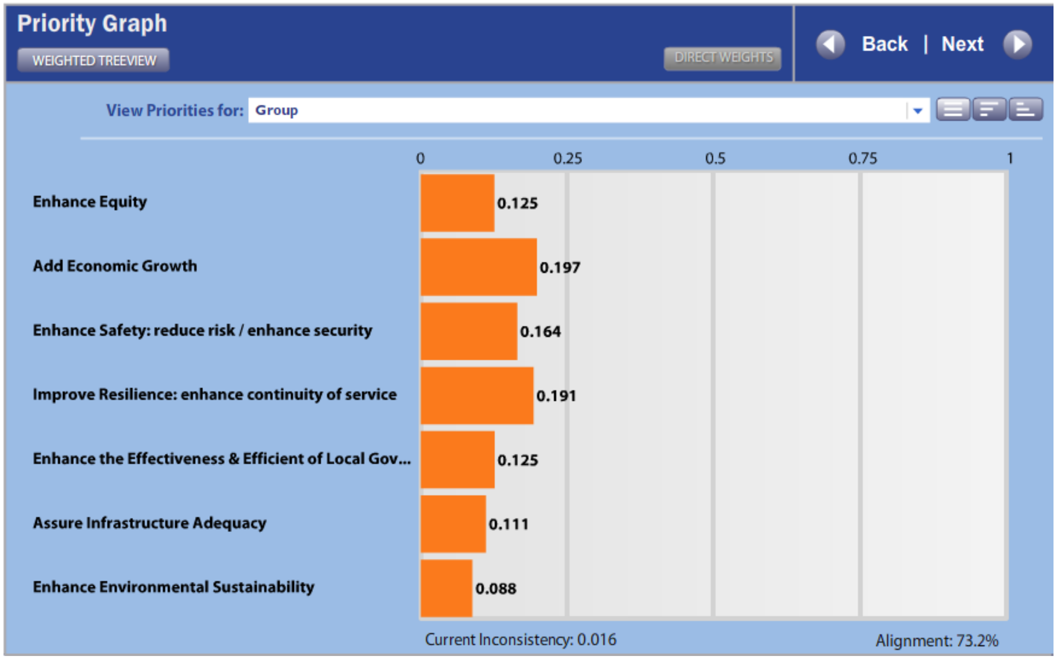
Enhance Equity OR Improve Resilience: enhance continuity of service

	extreme		very strong		strong		moderate		equal	moderate		strong		very strong		extreme	
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9
Average										1.26							
Brashear, Jerry										🟦	3						
Schott, Laurie										2							
Rahman, Rasheq							3	🟧									
Hamilton, Ted										🟦	3						
Krimgold, Fred							3	🟧									

Showing Comparison 12 of 21   6 participant(s) have voted   Variance: 2.49   **Group Average:** 1.26

Courtesy of Decision Lens Inc.

Figure 3.10 **Priorities for the Example Objectives**

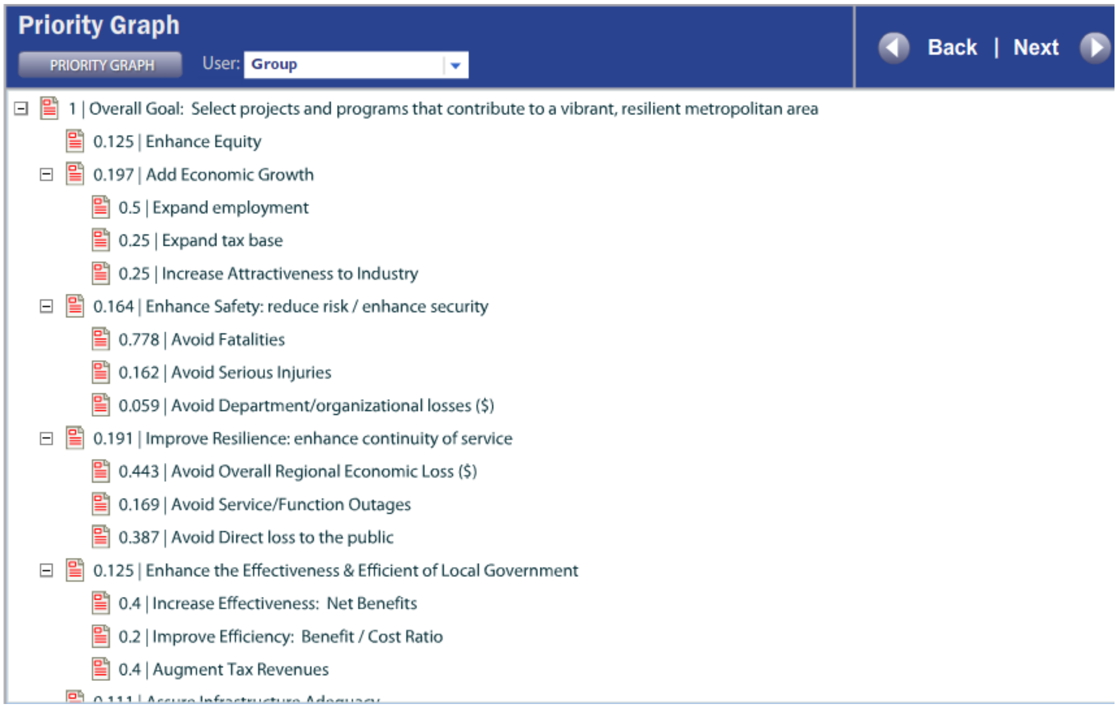


Courtesy of Decision Lens Inc.

"dividing." In *Figure 3.9*, by contrast, the group was split in its opinion, with judgments going both ways, resulting in a very slight preference for the group as a whole favoring "improved resilience" over "enhanced equity" by about 26%.

Step 4. Calculate weights.
These paired comparisons are combined to yield overall priorities (weights) for each objective and criterion. *Figure 3.10* shows the weights assigned to the objectives in graphical form as the software displays them.

The consistency index shows a very good consistency (significantly less than 0.1). Had this index been greater than 0.1, the decision-makers would review their judgments for possible re-estimation. The software indicates which pairs add the most inconsistency, so locating where the inconsistencies lie is clear. The decision-makers are not compelled to change their judgments, but



- 1 | Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan area
  - 0.125 | Enhance Equity
  - 0.197 | Add Economic Growth
    - 0.5 | Expand employment
    - 0.25 | Expand tax base
    - 0.25 | Increase Attractiveness to Industry
  - 0.164 | Enhance Safety: reduce risk / enhance security
    - 0.778 | Avoid Fatalities
    - 0.162 | Avoid Serious Injuries
    - 0.059 | Avoid Department/organizational losses ($)
  - 0.191 | Improve Resilience: enhance continuity of service
    - 0.443 | Avoid Overall Regional Economic Loss ($)
    - 0.169 | Avoid Service/Function Outages
    - 0.387 | Avoid Direct loss to the public
  - 0.125 | Enhance the Effectiveness & Efficient of Local Government
    - 0.4 | Increase Effectiveness: Net Benefits
    - 0.2 | Improve Efficiency: Benefit / Cost Ratio
    - 0.4 | Augment Tax Revenues

Figure 3.11 **Overall Priorities of Objectives and Criteria in Example (On-Screen "Tree" Format)**

Courtesy of Decision Lens Inc.

Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan area

- 0.125 Enhance Equity
- 0.2 Add Economic Growth
  - 0.1 Expand employment
  - 0.05 Expand tax base
  - 0.05 Increase Attractiveness to Industry
- 0.164 Enhance Safety: reduce risk / enhance security
  - 0.127 Avoid Fatalities
  - 0.027 Avoid Serious Injuries
  - 0.01 Avoid Department/organizational losses ($)
- 0.188 Improve Resilience: enhance continuity of service
  - 0.083 Avoid Overall Regional Economic Loss ($)
  - 0.032 Avoid Service/Function Outages
  - 0.073 Avoid Direct loss to the public
- 0.125 Enhance the Effectiveness & Efficient of Local Government
  - 0.05 Increase Effectiveness: Net Benefits
  - 0.025 Improve Efficiency: Benefit / Cost Ratio
  - 0.05 Augment Tax Revenues
- 0.111 Assure Infrastructure Adequacy
- 0.088 Enhance Environmental Sustainability

Figure *3.12* **Overall Priorities of Objectives and Criteria In Example (Report "Tree" Format)**

Courtesy of Decision Lens Inc.

often find that their initial assessments were in error.

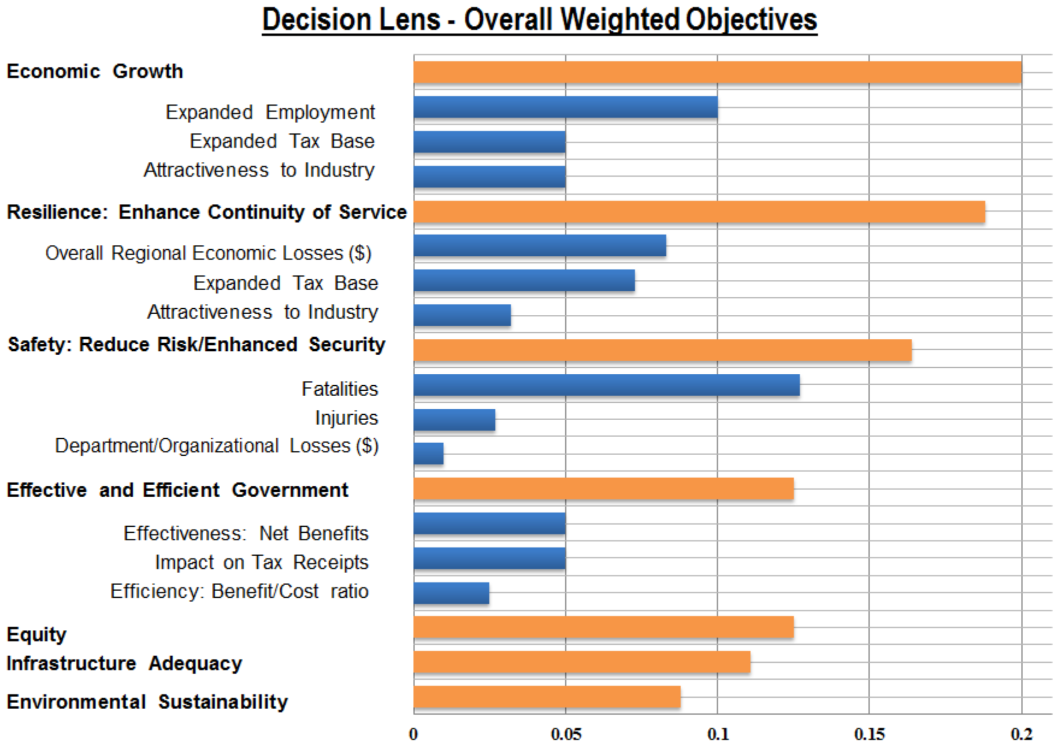
Figure 3.11 shows the priorities of both criteria and objectives in "tree" form.

The Decision Lens software provides the same information as a report, as shown in *Figure 3.12*. *Figure 3.13* displays the same information in graphical form, a figure that was prepared outside the software, but found to be more readily understood than the tree form by many decision-makers.

Step 5. Review weights and metrics; adjust. This step consists of stepping back and asking if the stated goal, objectives, criteria and metrics actually reflect the preferences of the decision-makers. This step is necessary to assure the decision-makers that the intrigue of the technology does not cause them to overlook desirable outcomes that are not captured in the goal hierarchy they have created. In the RR/SAP, these reconsiderations can be especially important to refine the objectives and criteria based on the findings of the Assessment Phase. If there are such concerns, they are accommodated by revisiting any or all the preceding steps.

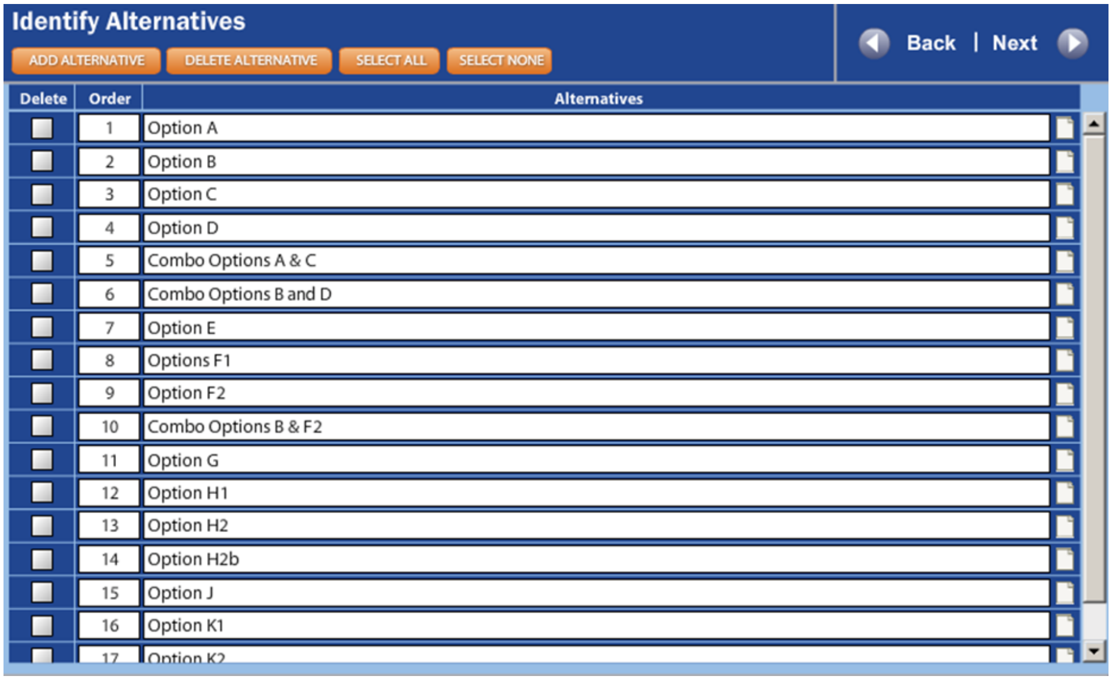
Steps 6 through 9 are not part of the initial goal-setting of RR/SAP Phase 1, but are discussed here because they use the same technology. Step 6 is the first activity of the Evaluation Cycle, the definition of options. Step 7 is the estimation of the metrics – the work of RR/SAP Phases 2 through 4. Many of these metrics are the difference between the situation without the option, as estimated in the Assessment Cycle and with the option implemented, as estimated in the Evaluation Cycle. In other words, many of the metrics describe the benefits of the option. Step

Figure 3.13 **Overall Priorities of Objectives and Criteria in Example (Bar Chart)**



Courtesy of Decision Lens Inc.

Figure 3.14 **Example Display of Options**



Delete	Order	Alternatives
☐	1	Option A
☐	2	Option B
☐	3	Option C
☐	4	Option D
☐	5	Combo Options A & C
☐	6	Combo Options B and D
☐	7	Option E
☐	8	Options F1
☐	9	Option F2
☐	10	Combo Options B & F2
☐	11	Option G
☐	12	Option H1
☐	13	Option H2
☐	14	Option H2b
☐	15	Option J
☐	16	Option K1
☐	17	Option K2

Courtesy of Decision Lens Inc.

8 ranks the options according to their estimates on the metrics defined above. And, Step 9 is the final selection of which options are to be included in the operating and capital budgets.

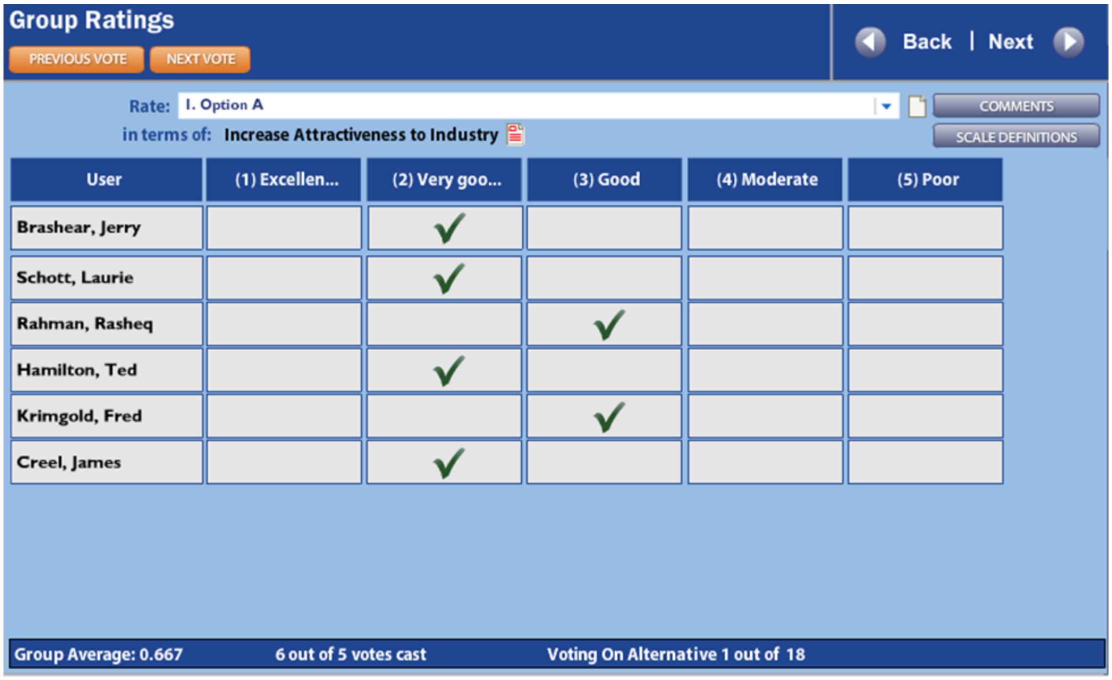
Step 6. Develop options to advance the goal and objectives.

Once the criteria have been determined, options for improvements are defined. In the case of RR/SAP, options must be well enough defined to allow estimation of specifically how and by how much they would change the situation and how much they would cost over their lifetimes and in the next year. *Figure 3.14* shows the set of options defined for this example.

Step 7. This step is RR/SAP Phases 2 through 5 to estimate the *quantitative* metrics, along with systematic judgments for the more *qualitative* (ordinal) metrics. *Figure 3.15* shows how the qualitative judgments are made, in this case, the impact on the attractiveness of the region to industry. For the quantitative metrics, the values as estimated in the other phases are simply substituted directly into the ratings sheets.

Step 8. This step calculates the overall weighted score on all the metrics and ranks the options by these weighted scores. This ranking is the value score as has been defined in this process. It can be treated as the "benefits" of the options, but in the RR/SAP, this term is reserved for a more specifically technical meaning as described in the next chapter. *Figure 3.16* displays the ranked options with their overall weighted scores and all

Figure 3.15 **Example of Group Judgments on an Example of the Qualitative Metrics**



Rate: I. Option A

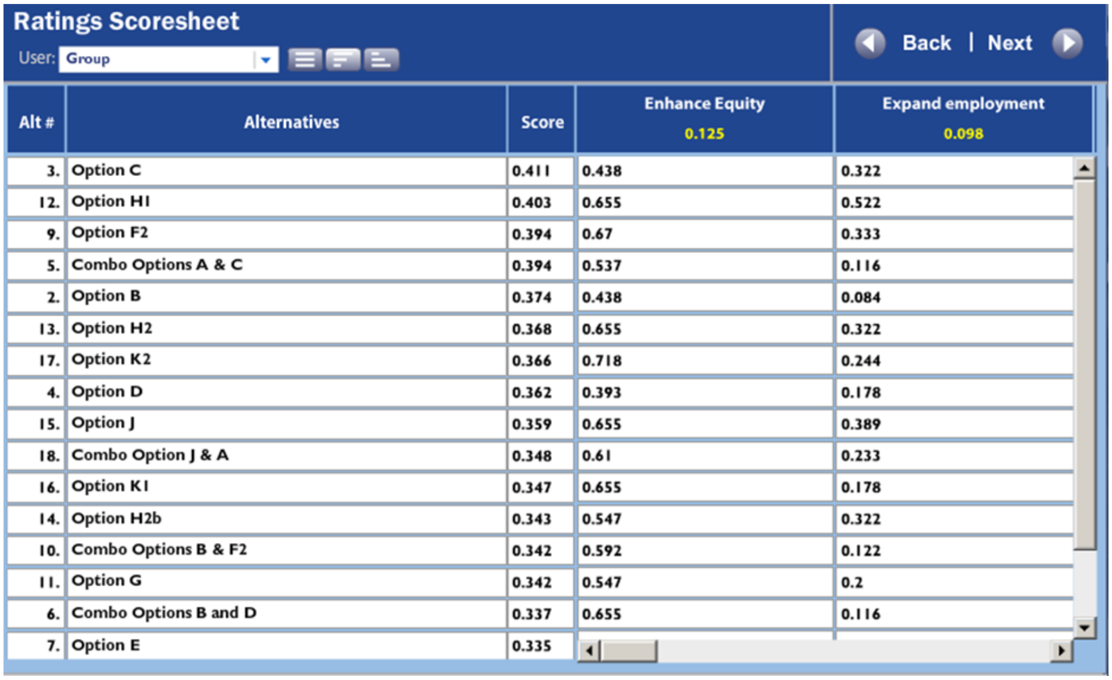
in terms of: Increase Attractiveness to Industry

User	(1) Excellen...	(2) Very goo...	(3) Good	(4) Moderate	(5) Poor
Brashear, Jerry		✓			
Schott, Laurie		✓			
Rahman, Rasheq			✓		
Hamilton, Ted		✓			
Krimgold, Fred			✓		
Creel, James		✓			

Group Average: 0.667 6 out of 5 votes cast Voting On Alternative 1 out of 18

Courtesy of Decision Lens Inc.

Figure 3.16 **Example Options Ranked by Score Based on Weighted Metrics**

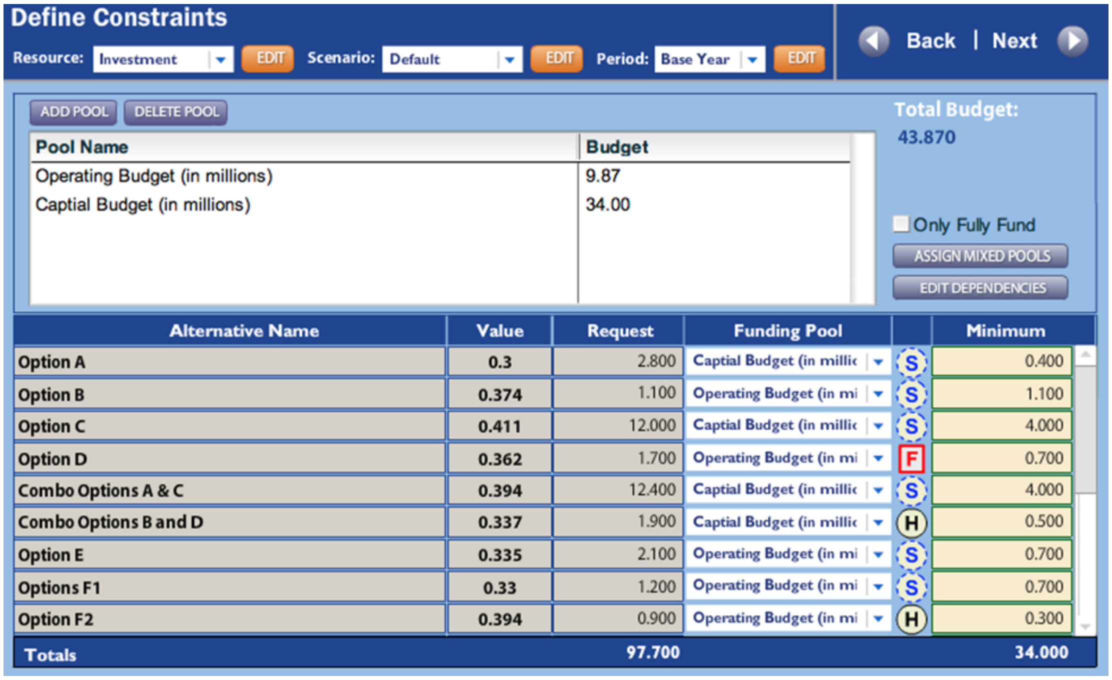


User: Group

Alt #	Alternatives	Score	Enhance Equity 0.125	Expand employment 0.098
3.	Option C	0.411	0.438	0.322
12.	Option H1	0.403	0.655	0.522
9.	Option F2	0.394	0.67	0.333
5.	Combo Options A & C	0.394	0.537	0.116
2.	Option B	0.374	0.438	0.084
13.	Option H2	0.368	0.655	0.322
17.	Option K2	0.366	0.718	0.244
4.	Option D	0.362	0.393	0.178
15.	Option J	0.359	0.655	0.389
18.	Combo Option J & A	0.348	0.61	0.233
16.	Option K1	0.347	0.655	0.178
14.	Option H2b	0.343	0.547	0.322
10.	Combo Options B & F2	0.342	0.592	0.122
11.	Option G	0.342	0.547	0.2
6.	Combo Options B and D	0.337	0.655	0.116
7.	Option E	0.335		

Courtesy of Decision Lens Inc.

Figure 3.17 **Entering Budgets and Costs of Options**



Resource: Investment

Scenario: Default

Period: Base Year

Total Budget: 43.870

☐ Only Fully Fund

Pool Name	Budget
Operating Budget (in millions)	9.87
Captial Budget (in millions)	34.00

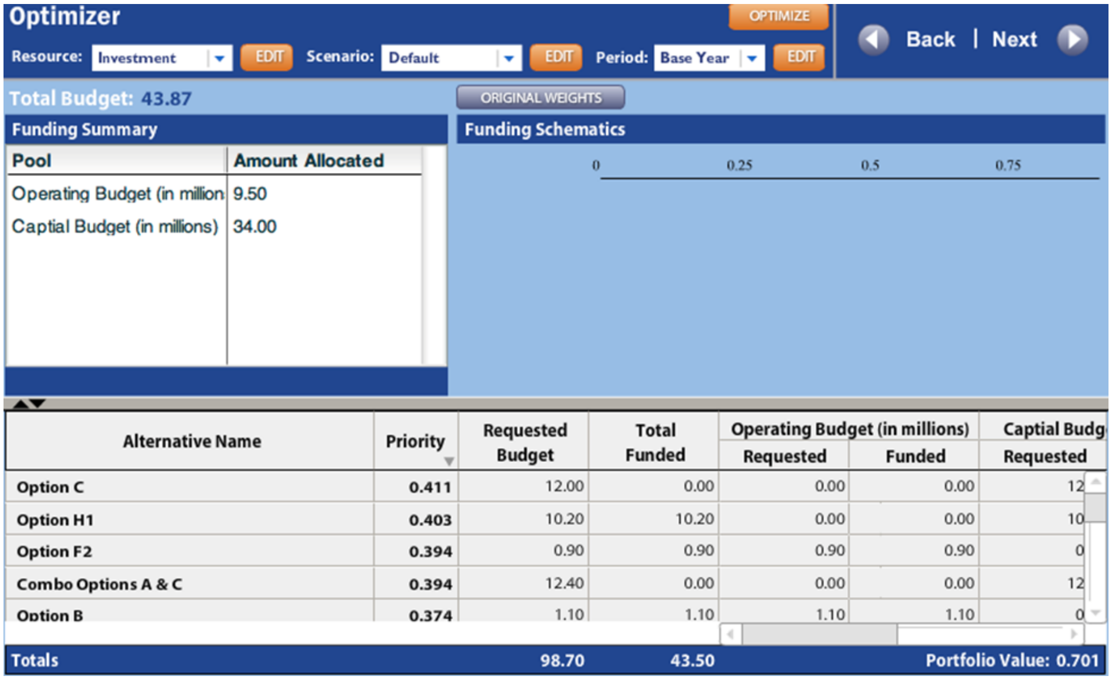
Alternative Name	Value	Request	Funding Pool		Minimum
Option A	0.3	2.800	Captial Budget (in millic	S	0.400
Option B	0.374	1.100	Operating Budget (in mi	S	1.100
Option C	0.411	12.000	Captial Budget (in millic	S	4.000
Option D	0.362	1.700	Operating Budget (in mi	F	0.700
Combo Options A & C	0.394	12.400	Captial Budget (in millic	S	4.000
Combo Options B and D	0.337	1.900	Captial Budget (in millic	H	0.500
Option E	0.335	2.100	Operating Budget (in mi	S	0.700
Options F1	0.33	1.200	Operating Budget (in mi	S	0.700
Option F2	0.394	0.900	Operating Budget (in mi	H	0.300
Totals		97.700			34.000

Courtesy of Decision Lens Inc.

the constituent metrics, arrayed to the right (only the first two show in the screen image, but all criteria are included for each option).

Figure 3.17 is the screen in which the costs of the options are entered. Multiple funding pools may be used, in this example, the operating and capital budgets. These are entered as the amount available for discretionary use. The total cost of each option is entered in the "request" column and from which budget it may be drawn in the "Funding Pool" column. The S, F, and H in the next column indicate constraints on the minimums that may be funded. A "Soft" minimum is amount that *may* be funded, *if* the project is funded based on its priority. A "Fixed" is the amount that *must* be allocated regardless of priority. A "Hard" minimum is the least amount that must be funded regardless of priorities. Other constraints may also be included to deal with consideration of alternatives (if select A, must

Figure 3.18 **The Optimized Option Selection**



Resource: Investment
Scenario: Default
Period: Base Year

Total Budget: 43.87

Funding Summary

Pool	Amount Allocated
Operating Budget (in million	9.50
Captial Budget (in millions)	34.00

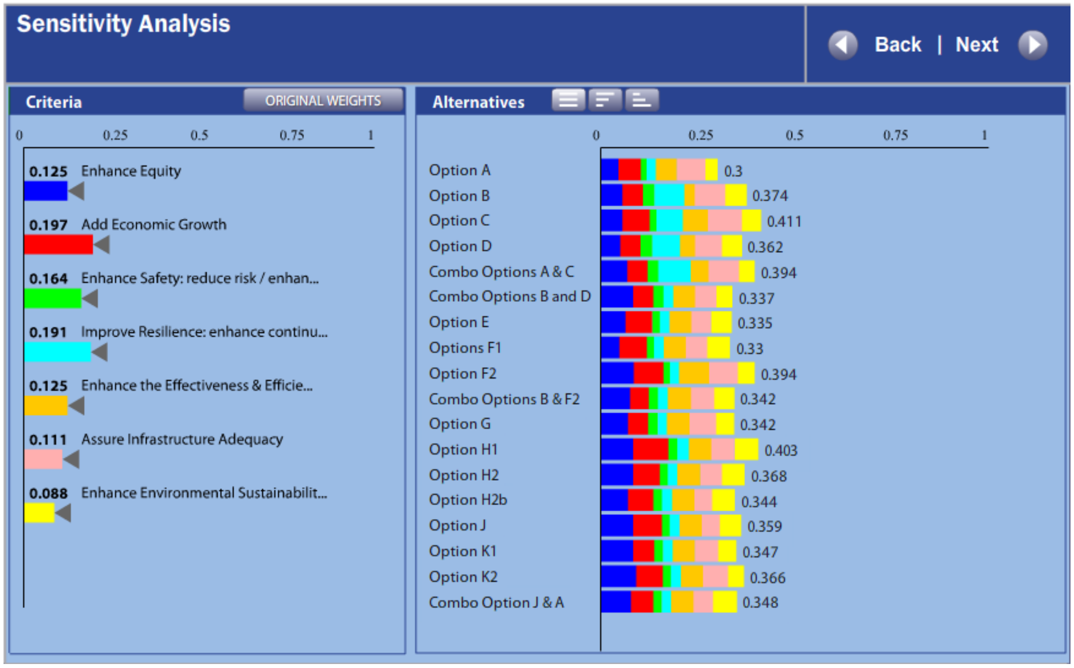
Alternative Name	Priority	Requested Budget	Total Funded	Operating Budget (in millions)		Captial Budg
				Requested	Funded	Requested
Option C	0.411	12.00	0.00	0.00	0.00	12
Option H1	0.403	10.20	10.20	0.00	0.00	10
Option F2	0.394	0.90	0.90	0.90	0.90	0
Combo Options A & C	0.394	12.40	0.00	0.00	0.00	12
Option B	0.374	1.10	1.10	1.10	1.10	0
Totals		98.70	43.50		Portfolio Value: 0.701	

Courtesy of Decision Lens Inc.

not select B), dependencies (if select A, then must select B), etc.

Figure 3.18 shows the selection of options that optimize the total portfolio score under the constraints of the total budgets available and the minimums as set for some options. In this example, the available funds were less than half of the total requested, but the optimized selection is able to produce 70% of the total possible priority if all the options were fully funded (the "portfolio value"). The software optimizes by value score per dollar of outlay within all the constraints. Some projects are partially funded, to be completed in later years, which is typical of multi-year construction. The optimizer found a solution that best fit the constraints by *not* selecting the alternative with the highest value score, but a lower value per investment dollar score.

Figure 3.19 **Ranked Projects with Original Objectives Priorities**



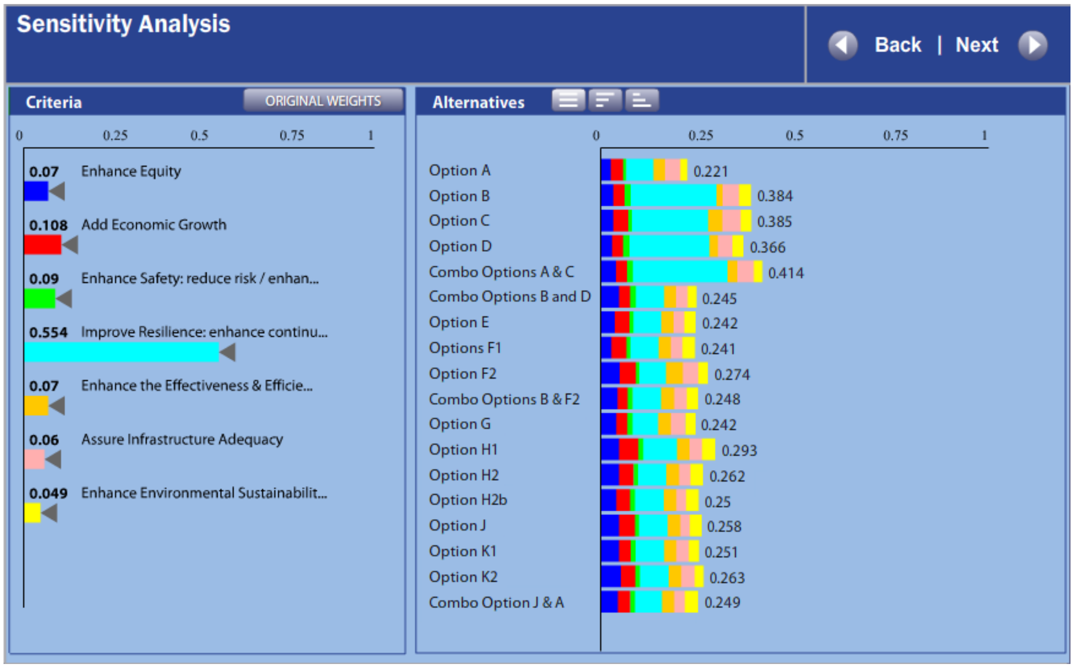
Weight	Criteria
0.125	Enhance Equity
0.197	Add Economic Growth
0.164	Enhance Safety: reduce risk / enhan...
0.191	Improve Resilience: enhance continu...
0.125	Enhance the Effectiveness & Efficie...
0.111	Assure Infrastructure Adequacy
0.088	Enhance Environmental Sustainabilit...

Alternatives	
Option A	0.3
Option B	0.374
Option C	0.411
Option D	0.362
Combo Options A & C	0.394
Combo Options B and D	0.337
Option E	0.335
Options F1	0.33
Option F2	0.394
Combo Options B & F2	0.342
Option G	0.342
Option H1	0.403
Option H2	0.368
Option H2b	0.344
Option J	0.359
Option K1	0.347
Option K2	0.366
Combo Option J & A	0.348

Courtesy of Decision Lens Inc.

*Step 9. Select Options***.** The final step is the one in which the decision-makers commit themselves to a specific selection of options and funding levels. If the objectives, criteria, metrics, weightings and constraints have successfully captured the full preferences and realities they face, the optimized selection may be simply accepted. Often, however, the decision-makers need to become comfortable with a specific selection. Decision Lens provides a sensitivity analysis feature that allows decision-makers to vary the weights assigned to the respective options and observe the impact on the ranking of the projects. *Figure 3.19* shows the objectives with their original weights beside the ranked options. *Figure 3.20* shows how increasing the weight of "Improve Resilience" would affect the rankings. In this example, the option with the highest original rank falls to second place, while the one with the fourth highest originally has climbed to the top. In addition, decision-makers may need to further adjust the optimal rankings, for example, to assure the political support for the whole program. This last step accommodates these issues.

Figure 3.20 **Ranked Projects with Objectives Priorities Revised to Emphasize Resilience**



	Criteria
0.07	Enhance Equity
0.108	Add Economic Growth
0.09	Enhance Safety: reduce risk / enhan...
0.554	Improve Resilience: enhance continu...
0.07	Enhance the Effectiveness & Efficie...
0.06	Assure Infrastructure Adequacy
0.049	Enhance Environmental Sustainabilit...

Alternatives	
Option A	0.221
Option B	0.384
Option C	0.385
Option D	0.366
Combo Options A & C	0.414
Combo Options B and D	0.245
Option E	0.242
Options F1	0.241
Option F2	0.274
Combo Options B & F2	0.248
Option G	0.242
Option H1	0.293
Option H2	0.262
Option H2b	0.25
Option J	0.258
Option K1	0.251
Option K2	0.263
Combo Option J & A	0.249

Courtesy of Decision Lens Inc.

Appendix 3A. Goal, Objectives, Criteria and Metrics

Overall Goal: Select projects and programs that contribute to a vibrant, resilient metropolitan area - Contributions to this goal are made by economic growth; environmental sustainability; public safety; resilient and adequate infrastructure; efficient, effective and equitable government.

Objective	Definition
Enhance Equity	This criterion will be used to assess the extent to which the initiative contributes to political, racial and economic balance among geographic and political groupings. The perception and fact of "fairness" and distributional justice are the primary issues. Metric: 5-point scale
Add Economic Growth	This criterion will be used to assess the extent to which the initiative provides jobs for citizens, enhances the tax base, and brings new industry into the area. Metrics: All quantitative.
Enhance Safety: Reduce Risk / Enhance Security	This criterion will be used to assess the extent to which the initiative reduces fatalities, injuries, department/ organizational loss ($). Metrics: Expected value of avoided or reduced fatalities, serious injuries and owner's financial loss.
Improve Resilience: Enhance Continuity of Service	The ability to withstand an undesired incident or, if not possible, to return to fully meeting demand for services quickly. Metrics: Expected values of avoided or reduced outages, regional economic losses and direct losses to the public.
Enhance the Effectiveness & Efficiency of Local Government	This criterion relates to the contribution of the option to the effectiveness and efficiency of the metro region's governments, as reflected in the net benefits, benefit/cost ratios and impact on the tax revenue. Metrics: Net benefits, benefit/cost ratio, and change in tax revenues.
Assure Infrastructure Adequacy	This criterion is the ability of the infrastructure to meet near- and longer-term demand for infrastructure services, without brown-outs, congestion, or service denials under normal (non-emergency) conditions. Metric: 5-point scale.
Enhance Environmental Sustainability	Enhances or avoids degradation of the natural environment, including conservation of natural resources, avoidance of pollution, etc. Metric: 5-point rating scale.

Add Economic Growth

This criterion will be used to assess the extent to which the initiative provides jobs for citizens, enhances the tax base, and brings new industry into the area.
Metrics: All quantitative.

Criterion	Definition
Expand employment	The percentage of jobs generated or sustained. Metric: percentage of current employment base.
Expand tax base	Incremental percentage additions to the taxable base. Metric: percentage of current tax base.
Increase Attractiveness to Industry	Increases the likelihood that new industry will locate in region and that current businesses will remain. Metric: 5-point scale.

Enhance Safety (reduce risk / enhance security)

This criterion will be used to assess the extent to which the initiative reduces fatalities, injuries, department/organizational loss ($), direct loss to public ($), indirect/regional loss

Criterion	Definition
Avoid Fatalities	Expected value of the number of people whose lives are saved by the option. Metric: Expected value of lives saved.
Avoid Serious Injuries	Expected value of the number of people saved from seriously injury in the incident. Metric: Expected value of serious injuries avoided.
Avoid Department & Organizational losses ($)	Expected value of the dollar amount in direct losses avoided to the owner's organization or department avoided because of the option. Metric: Expected value dollars saved.

Improve Resilience *(enhance continuity of service)*

The ability to withstand an undesired incident or, if not possible, to return to fully meeting demand for services quickly. Metrics: Expected values of avoided or reduced outages, regional economic losses and direct losses to the public.

Criterion	Definition
Avoid Overall Regional Economic Loss ($)	This is the expected value of the avoided loss in regional economic performance (input-output model). Metrics: Same, in dollars
Avoid Service/ Function Outages	This criterion will be used to assess the extent to which the initiative avoids or minimizes service outages to provide continuity of service (expected value of units/ day x days in $, or gross revenue, loss avoided). Metric: Same, in dollars.
Avoid Direct loss to the public	Expected value of reduction in direct economic losses to the public due to option. Metric: Avoided direct losses, in dollars.

Enhance the Effectiveness & Efficiency of Local Government

This criterion relates to the contribution of the option to then effectiveness and efficiency of the metro region's governments. as reflected in the net benefits, benefit/cost ratios and impact on the tax revenue. Metrics: Net benefits, benefit/cost ratio, and change in tax revenues.

Criterion	Definition
Increase Effectiveness: Net Benefits	Net benefits = gross benefits - cost Metric: net benefits of option, in dollars.
Improve Efficiency: Benefit / Cost Ratio	The ratio of expected value net benefits to costs. Metric: the ratio.
Augment Tax Revenues	Tax increases or decreases attributed to the option, based on input-output model. Metric: Tax revenues added or expected value losses avoided.

Annex 3B

Ratings Scale Definitions

Enhance Equity

Rating	Weight
Excellent	100.00% (1.00)
Very good	85.40% (0.85)
Good	58.20% (0.58)
Moderate	20.40% (0.20)
Poor	0.00% (0.00)

Increase Attractiveness to Industry

Rating	Weight
Excellent	100.00% (1.00)
Very good	75.00% (0.75)
Good	50.00% (0.50)
Moderate	25.00% (0.25)
Poor	0.00% (0.00)

Expand Employment

Rating (% net gain)	Weight
0.00	0.00% (0.00)
15.00	100.00% (1.00)

Avoid Fatalities

Rating (No. Lives Saved)	Weight
0.00	0.00% (0.00)
100.00	100.00% (1.00)

Expand Tax Base

Rating (% net gain)	Weight
0.00	0.00% (0.00)
15.00	100.00% (1.00)

Avoid Serious Injuries

Rating (No. Injuries Avoided)	Weight
0.00	0.00% (0.00)
500.00	100.00% (1.00)

Avoid Departmental/ Organizational Losses ($)

Rating ($ Loss Avoided)	Weight
0.00	0.00% (0.00)
10,000,000.00	100.00% (1.00)

Avoid Overall Regional Economic Losses ($)

Rating ($ Loss Avoided)	Weight
0.00	0.00% (0.00)
1,000,000,000.00	100.00% (1.00)

Avoid Service/Function Outages

Rating ($ Revenue Loss)	Weight
0.00	100.00% (1.00)
100,000,000.00	0.00% (0.00)

Avoid Direct Loss to the Public

Rating	Weight
0.00	0.00% (0.00)
1,000,000,000.00	100.00% (1.00)

Increase Effectiveness: Net Benefits ($)

Rating	Weight
0.00	0.00% (0.00)
100,000,000.00	100.00% (1.00)

Improve Efficiency: Benefit/Cost Ratio

Rating	Weight
0.00	0.00% (0.00)
10.00	100.00% (1.00)

Augment Tax Revenues (%)

Rating	Weight
0.00	0.00% (0.00)
7.00	100.00% (1.00)

Avoid Direct Loss to the Public

Rating	Weight
Fully meets present & future demand	100.00% (1.00)
Meets most of present & future demand	75.00% (0.75)
Meets present demand	50.00% (0.50)
Moderate under-supply	25.00% (0.25)
Serious under-supply	0.00% (0.00)

Avoid Direct Loss to the Public

Rating	Weight
Excellent	100.00% (1.00)
Very good	83.00% (0.83)
Good	62.30% (0.62)
Moderate	23.30% (0.23)
Poor	0.00% (0.00)

CHAPTER 4

Facility/Asset Resilience/Security Analysis:
The RAMCAP® Process

4.1 Origin and Evolution of RAMCAP®[6]

Risk Analysis and Management for Critical Asset Protection (RAMCAP) was selected as the basic component for Phase 2 of the Regional Resilience/Security Analysis Process (RR/SAP). As *Figure 4.1* illustrates, this phase is the beginning of the analytic work of both the Assessment Cycle and the Evaluation Cycle. RAMCAP consists of seven steps (defined later) that are practical and robust rather than esoteric or theoretical. The goal is an efficient, straightforward process that can be carried out by on-site professionals – within a reasonable amount of time, with a modicum of special training – to support decisions to allocate resources to enhance security and resilience.

Following the attacks of September 11, 2001, the American Society of Mechanical Engineers (ASME) convened more than one hundred industry leaders, at the request of the White House, to define and prioritize the requirements for protecting our nation's critical infrastructure. The leaders' primary recommendation was to create a risk analysis and management process to support decisions to allocate resources to initiatives that reduce risk and enhance resilience within *and across* industries. This would require a common and consistent process, terminology and metrics – tailored to the technologies, practices and cultures of the respective industries – to permit direct comparisons within and across industry sectors. Such direct comparisons were seen as essential to support rational decision-making in the allocation of limited private and public resources.

In response to this recommendation, ASME convened a team of distinguished risk assessment experts from industry and academia to develop a process that came to be named RAMCAP. ASME has been involved in probabilistic risk assessment for a number of years. Its many committees have developed a large body of knowledge and application, especially in the area of nuclear power, pressure vessels, and pipeline safety. The newly convened team defined a seven-step process that enables facility owners to

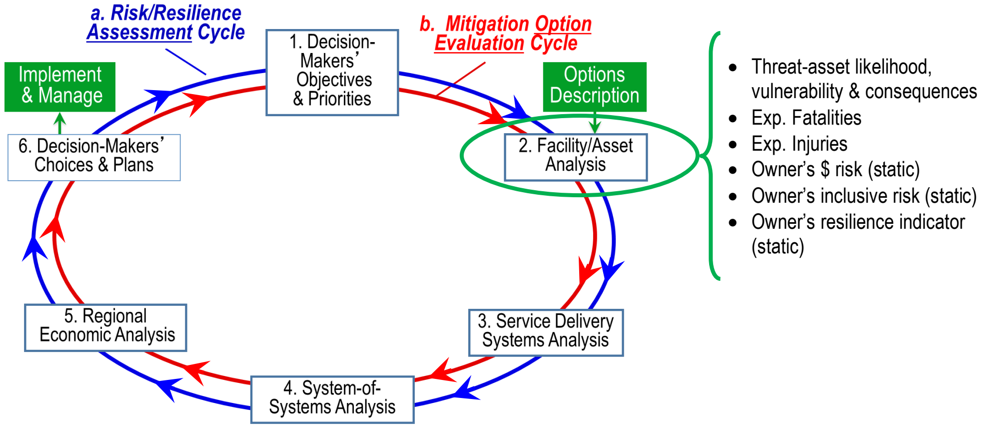


Figure 4.1 **RR/SAP Phase 2: Facility Risk/Resilience Analysis**

---

[6] RAMCAP® is a registered trademark of ASME Innovative Technologies Institute, LLC. The registered trademarks are implied in every use of "RAMCAP" in this volume.

perform assessments of their risks and evaluate risk-reduction options relative to specific attacks. Risk is defined as a function of the likelihood of specific attacks, the asset's vulnerability to these attacks and the consequences of the attack. With this information, alternative risk-reduction and resilience-enhancement initiatives are evaluated for their ability to reduce the vulnerability, likelihood and/or consequences (including outages, blackouts and revenue losses – key elements of resilience) related to risk. The reductions in risks and enhancements of resilience can be used in estimating the benefit/cost ratios to inform decisions allocating resources to specific initiatives.

Risk is defined as a function of the likelihood of specific attacks, the asset's vulnerability to these attacks and the consequences of the attack.

ASME Innovative Technologies Institute, LLC (ASME-ITI) was established in 2004 to continue the development of RAMCAP. The initial version of the RAMCAP approach was the draft *Risk Analysis and Management for Critical Asset Protection: General Guidance* (ASME-ITI, 2004), a generalized description.

The University Consortium for Infrastructure Protection recommended this version as the preferred tool for supporting asset and system resource allocation decisions in protecting the National Capital Region (McCarthy and Brashear, 2005). Based on an assessment of the majority of available tools (62 in number), the initial version of the RAMCAP process was the only application that offered universality, essential direct comparability and a practical synthesis of the leading methodologies available at the time.

To achieve the necessary consistency and comparability while recognizing the differences among industries, the RAMCAP approach was conceived as having three levels: (1) a high-level and general process description, periodically updated based on accumulated experience, and as (2) a series of sector-specific guidance (SSG) documents, expressly tailored to the technologies, issues and cultures of the respective sectors and subsectors; a subset of these would be converted to (3) a series of voluntary American National Standards if the respective industries so desired. Voluntary standards were seen as desirable as the basis for self-regulation, limited bureaucratic involvement and the eligibility criteria for various incentives such as direct subsidies, insurance premium discounts and financial rating enhancements. The SSGs and standards – and adaptations of other tools – would be "RAMCAP-consistent" if they met explicit criteria derived from the then-current approach. This assured that the results of applying SSGs would be directly comparable regardless of the industry to which they were applied.

The *General Guidance* was circulated in draft widely and reviewed extensively by panels of applied risk management and security experts. It was seen as a competent and comprehensive synthesis of the best available methods and highly appropriate for an academic or risk professional. It was not, however, as useful to security and operating personnel at the facilities of concern, who stated they found it too complex and difficult to understand. As the result, a key design criterion was added to encourage widespread application; the process should be appropriate for *self-assessment by on-site staff in a relatively short period of time*. In response to this feedback and the design requirement, the *General Guidance,* which was never published, was streamlined and simplified into two documents: the semi-technical *Introduction to Risk Analysis and Management for Critical Asset Protection* (ASME-ITI, 2005a), and a non-technical *Risk Analysis and Management for Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security* (ASME-ITI, 2005b)*,* written expressly for the intended audience.

The approach described in these three initial RAMCAP documents was referenced in the various drafts of the *National Infrastructure Protection Plan* (NIPP) in 2006 as the

"RAMCAP Framework." This framework met the NIPP requirements for a simple and efficient process to support consistent, quantitative assessments and provided results that could be systematically and directly compared. The 2006 version of the NIPP broadened the definition of the concerns from terrorism only to include natural hazards, which are included in later RAMCAP documents. In 2004-5, the U.S. Department of Homeland Security (DHS) funded a series of five SSGs including: (1) nuclear power plants; (2) spent fuel transportation and storage; (3) petroleum refining; (4) chemical manufacturing; and (5) liquefied natural gas off-loading ports (ASME-ITI, 2005c through 2005g). The next version was updated as the *RAMCAP Framework*©*, Version 2.0* (ASME-ITI, 2006), and is based on the experience of developing the first five SSGs. Version 2.0 was used to guide development of the next two DHS-sponsored SSGs, (6) dams and navigational locks and (7) water and wastewater systems (ASME-ITI, 2007a and 2007b), and (8) a privately funded SSG for higher education campuses (ASME-ITI 2008). ASME-ITI joined with the American Water Works Association (AWWA) to adapt the SSG for the water sector into a standard approved by the American National Standards Institute (ANSI) as an American National Standard (ANSI/ASME-ITI/AWWA J100-10, 2010).

As with the earlier *Framework*, prior experience and the latest three sectors informed the drafting of a new general statement of approach, *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach* (ASME-ITI, 2009). This new version of the refined *RAMCAP Plus* included the following revisions and additions:

- Likelihood, vulnerability and consequences of natural hazards (earthquakes, tornadoes, hurricanes and floods);
- Increased attention to immediate functional and location-based dependencies posed by supply chains and proximity;
- Explicit recognition of the role of resilience (the ability to withstand or rapidly restore function to critical assets after an attack or natural event), measured in duration and severity of denial and economic impact on the community;
- Dual-perspective economic impacts, estimating the impacts to both the owners of the infrastructures and the community they serve;
- Benefit-cost analysis at both owner and community levels;
- The general reference threat of product contamination (necessitated by the water sector, but applicable to food, pharmaceuticals, etc.); and
- Expanded discussions of several steps in the RAMCAP process.

At least three major research/engineering organizations are currently engaged in developing software to implement the RAMCAP process as defined through the standards.

The present project has further extended RAMCAP by applying it to public safety functions, for fire suppression, emergency medical services and emergency communications. Feasibility was also checked for applying the approach to selected police functions. In all these cases, no major changes in the process or metrics were needed to use RAMCAP. The current project also updated the analytic approaches for floods, earthquakes and tornadoes and added ice storms to the list of natural hazards.

4.2 Reasons for Selecting RAMCAP for RR/SAP Facilities Risk/ Resilience Analysis

The RAMCAP process was selected for use because it was designed expressly for the central issue of the present project – allocation of resources for enhanced security and resilience. Other attributes include ease of use by on-site personnel, inclusion of both risk and resilience analysis, dual-perspectives (owner and regional community), quantitative objectivity, transparency, repeatability, comparability at numerous scales and across time (for accountability and measuring progress and trends), the history of its applicability to a wide array of industries, and the fit with the other tools in the RR/SAP. RAMCAP generates benefits to the organization using it, the sector or industry that adopts it, the community it serves and the public policy-makers that focus on infrastructure security and resilience.

For organizations using the RAMCAP process, net benefit and benefit/cost ratios of options to enhance security and resilience can result in rational allocation of resources across sites, facility assets and lines of business. The benefits of making decisions on this basis are more efficient management of capital and human resources and enhanced reliability in performance of a system's mission. The ability to define risk and resilience levels quantitatively at the community level enables the firm to partner with other firms and public agencies. Individual organizations will incur additional benefits if its sector adopts the RAMCAP process. If adapted to be a voluntary consensus standard, it becomes the vehicle for incentives, such as preferred supplier status, lower insurance costs, higher credit ratings and lower liability exposure.

A sector adopting the RAMCAP process will be able to identify the components with the greatest need and potential for improvement by comparing the results of concrete, quantitative RAMCAP assessments. They will have concrete, repeatable descriptions of the current levels of risk and resilience, as well as the potential benefits and benefit/cost ratios of their sector. Adoption also permits direct comparison of the sector's risk and resilience level to other sectors for higher-level resource allocation and policy-making. If the sector decides to make its RAMCAP-consistent methods or SSG into a consensus standard, additional benefits can be gained, such as an affirmative defense in liability cases,[7] preferential treatment by insurers, financial rating services and customers, the ability to substitute bureaucratic regulation with self-regulation through standards, and direct participation in federal regulatory, procurement or other activity involving security and resilience of the sector.

RAMCAP generates benefits to the organization using it, the sector or industry that adopts it, the community it serves and the public policy-makers that focus on infrastructure security and resilience.

For the community and public policy, the facilities using the RAMCAP process will be routinely asked to estimate the potential for lost economic activity by the metropolitan region they serve, allowing that to become a salient criterion in both private and public decisions. Use of the RAMCAP process will allow cooperative decision-making by providing risk and resilience analysis on a comparable, consistent basis, which may also support rational trade-offs should the community, metropolitan region or public-private partnership determine to enhance the region's security and resilience. Further, if a RAMCAP consensus standard exists, a community might designate the standard as the local code of expected practice.

Finally, if state, multi-state regions or federal agencies seek to allocate resources rationally to maximize the security and resilience enhancement within a finite budget, widespread use of the RAMCAP process could provide the required method of consistency and direct comparability needed to perform the assessment. The methods used to estimate economic losses to metropolitan regions can be extended to states, multi-state regions or the national economy – whatever scales are relevant to the decisions to be made.

In summary, use of the RAMCAP process for facility- and asset-level analyses in the RR/SAP

---

[7] The ANSI/ASME-ITI/AWWA J100 standard is under review to be granted SAFETY Act recognition.

yields significant benefits to the asset owners who use it, the communities they serve and their role in local, regional and/or national economies. It exhibits all the necessary characteristics to fulfill the purposes of this level of analysis. No alternative to date has these specific characteristics.

4.3 The RAMCAP Process in Overview

The RAMCAP process has been developed to facilitate the analysis and management of risk and resilience of critical facilities, infrastructures and public safety functions. It is based on the fundamental definition that risk is the "expected value" of the consequences of specific adverse events, weighted by the likelihood of the event and the conditional likelihood that the event will lead to the estimated consequences. In its functional form, this is the definition of risk advanced by the U.S. Department of Homeland Security (DHS, 2009). The RAMCAP process provides a system of common terms, metrics, steps and tasks that allow any RAMCAP-based analysis to be compared with other RAMCAP-based analyses. The RAMCAP process can be applied to any asset, set of assets or system of assets.

> *… risk is the "expected value" of the consequences of specific adverse events, weighted by the likelihood of the event and the conditional likelihood that the event will lead to the estimated consequences.*

The RAMCAP process is a quantitative method that estimates numeric values of risk and resilience, as well as benefits of improving security, resilience and value based on estimates of vulnerability, threat likelihood and consequence (including service outages) made by on-site personnel, usually from operations, security, engineering and security units. RAMCAP also calls for descriptions of non-quantifiable consequences, such as psychological impacts, public confidence, and military preparedness.

The use of RAMCAP-based risk and resilience analysis provides decision-makers the ability to make informed judgments of the value of options to reduce risk and/or enhance resilience relative to threats of hurricane, flood, tornado, earthquake, ice storms, terrorism and dependencies on other systems.

4.3.1 Risk and Resilience Defined

There are many common, everyday terms which, when used by risk assessment professionals, take on very specific meanings. It is important to keep these specific definitions in mind and resist using the more colloquial terms. In the NIPP (DHS, 2009), *risk* is defined as a function of threat likelihood, vulnerability and consequences. In the earlier NIPP and the RAMCAP *Framework*, this function is defined as the product, or:

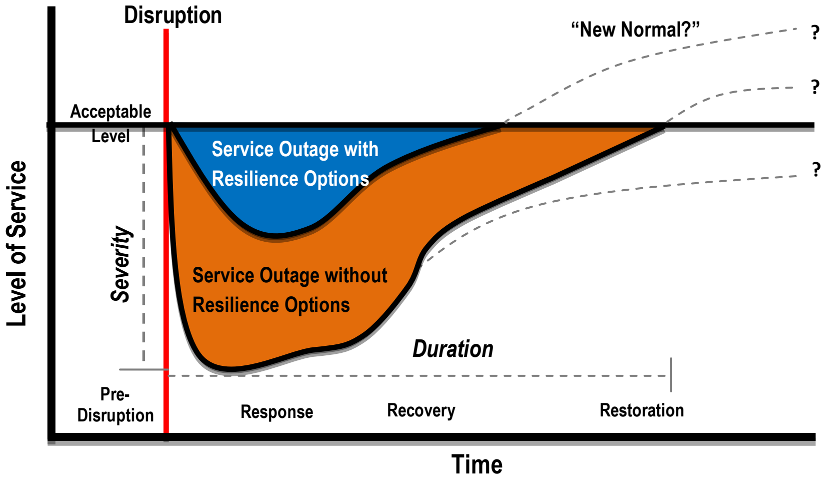
$$\textit{Risk} = (\textit{Threat Likelihood}) \times (\textit{Vulnerability}) \times (\textit{Consequence}) \text{ or } R = T \times V \times C \qquad \textit{Eq. 4.1}$$

Where:

Risk (R) – The potential for loss or harm due to an untoward event and its adverse consequences. It is measured as the combination of the probability and consequences of an adverse event. When the probability and consequences are expressed as numerical point estimates, the expected risk is computed as the product of those values. In the case of the RAMCAP process and many other risk and resilience processes, risk is the product of threat, vulnerability and consequence.

Threat Likelihood (T) – Any circumstance or event with the potential to cause the loss of, or damage to, an asset or population. In the case of terrorism risk, threat is based on the analysis of the intention and capability of an adversary to undertake actions detrimental to an asset or population and the attractiveness of the asset or population

Figure 4.2 **Resilience & Security Add Value by Reducing Service Outages & Losses, Respectively**



(Based on a slide by Dr. Mary Ellen Hynes)

relative to alternative assets or populations. In the case of natural hazards, threat refers to the historical frequency of the specific natural event to which the asset(s) at a specific location may be subjected. In both cases, threat is summarized as the likelihood the event will occur.

Vulnerability (V) – Any weakness in an asset or infrastructure's design, implementation or operation that can be exploited by an adversary or contribute to functional failure in a natural disaster. Such weaknesses can occur in building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings or operational and personnel practices. In security risk analysis, vulnerabilities are usually summarized as the conditional probability that, *given* an event, the estimated consequences will ensue, i.e., the attack will succeed or the natural event will cause the estimated damage.

Consequence (C) – The outcome of an event's occurrence, including immediate, short- and long-term, direct and indirect losses and effects. Loss may include human fatalities and injuries, financial losses to the owner and economic damages and environmental impacts to the whole community, which can generally be estimated in quantitative terms. Consequences may also include less tangible and less quantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness or other impacts.

Another key concept, resilience**,** is a very important subset of risk, but is central to the purposes of the RAMCAP process. Critical infrastructures and public safety functions are "critical" because denial of their services endangers the physical and economic health and well-being of whole regional communities, with consequences that can spill over into other critical service-delivery systems and other communities. Outages of the services provided by critical infrastructures and public safety functions have such profound consequences that resilience or continuity of service is an aspect of risk that is singled out for special attention.

Resilience is broadly defined as the ability to withstand an adverse event and maintain functioning (service delivery) or, if function is unavoidably compromised, the speed by which target levels service delivery and quality can be restored, or a substitute service provided to an acceptable level. Resilience as a concept is still being formalized; so many definitions and metrics have been suggested. Some prefer to measure resilience using time, from time of event until return to full function, but this ignores partial service denial, which is generally much more common than complete loss of function, and the value of the services denied. Virtually all formal definitions of resilience use some variation of the concept illustrated in *Figure 4.2*. A disruptive event causes a service outage which can be defined by its *severity* – units per day of unmet demand – and *duration* – the time in days that the outage lasts. Improving resilience is reducing the severity, duration or both. Perfect resilience is the ability to withstand the event with no service outage.

For the asset owner, the *resilience indicator* for a particular threat to a particular asset is expressed as:

Owner's Resilience Indicator =
***(Duration x Severity)* × *Vulnerability* ×**
Threat Likelihood

Eq. 4.2

Where:

Duration – the length of time, in days, that service delivery falls below the minimum acceptable level.

Severity – the amount of service per day that is denied, in natural units.

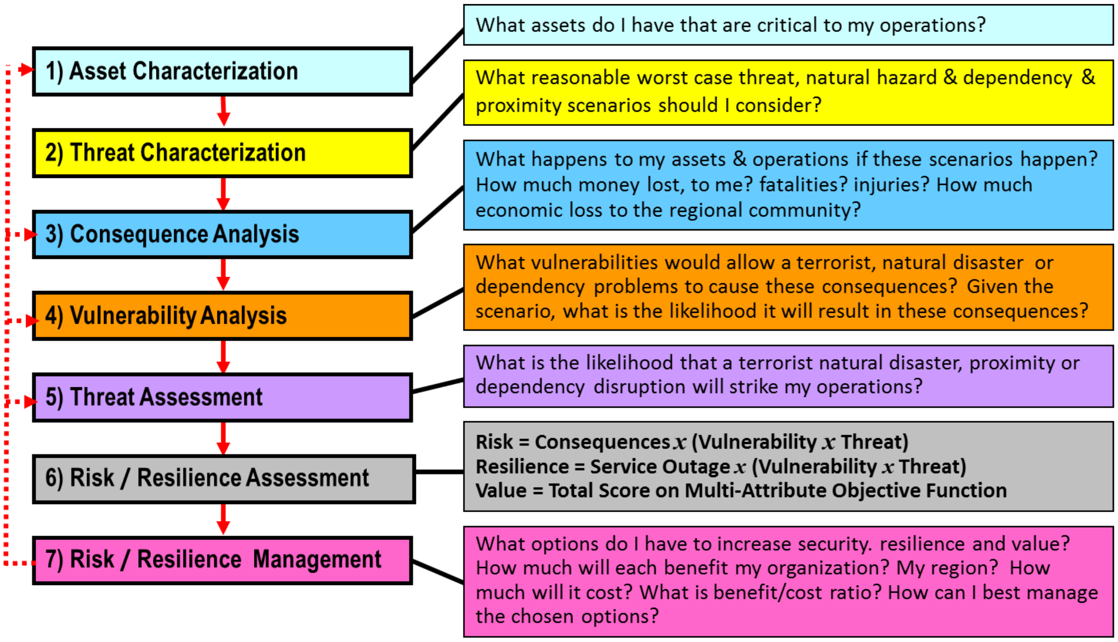
Vulnerability and **Threat Likelihood** are the same as in the risk equation.

This index results in expected outage in units of service. When comparability outside a single industry is desired for decision-making, the resilience indicator is multiplied by the prevailing unit price before the initiating event. This quantity, of course, is gross revenue lost, a component of financial risk. As risk is a measure of the imperfections in security, the resilience indictor is the measure of imperfections in resilience. In both cases, the higher the indicator, the lower the valued condition.

4.3.2 Summary of the RAMCAP Process

RAMCAP uses a seven-step approach to risk analysis and management (*Figure 4.3*), of which the first six steps are fundamental to developing the baseline state of risk and resilience for an organization, facility or system. These are all parts of the RR/SAP Assessment Cycle. For risk and resilience levels that are unacceptable to the decision-makers, the RR/SAP Evaluation Cycle is initiated by refining the objectives and defining a series of options that will enhance security and resilience. These options are defined in enough detail to estimate their impacts and costs. Then, Steps 3 through 6 are repeated under the assumption that the options have been implemented. The difference between the baseline risk and resilience metrics (from the

Figure 4.3 **Steps in the RAMCAP Process**



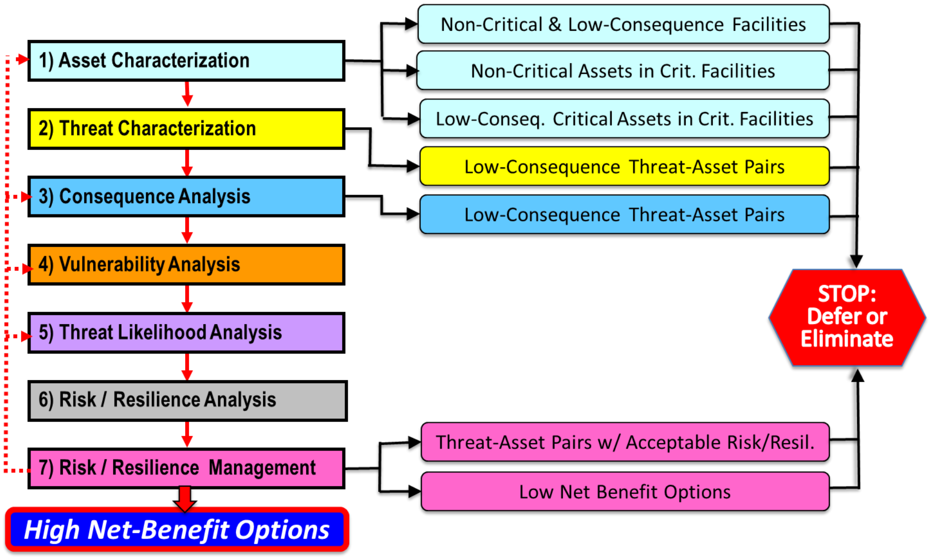
Assessment Cycle) and the same metrics with the options (from the Evaluation Cycle) are the benefits of the options. Net benefits (gross benefits minus costs), benefit/cost ratios, and value added relative to the objectives from Phase 1 are considered by decision-makers in allocating their budgets.

Each step is discussed in more detail in later sections, but is summarized here to show the overall logic. Taken as a whole, these steps provide a rigorous, objective and transparent foundation for data-collection, interpretation, analysis, and decision-making.

In summary, the seven steps are:

1. *Asset Characterization* – defining which facilities and which assets are critical to the performance of the mission or function of the organization and prioritizing them based on very rough initial estimates of the consequences of their functions being disrupted;
2. *Threat Characterization* – defining what specific threats to consider for each asset, defining the threat-asset pairs that are the subject of the next five steps and prioritizing them, again, based on rough estimates of consequences of disruption;
3. *Consequence Analysis* – estimating in detail the worst reasonable outcomes of each high-priority threat-asset pair, including fatalities, serious injuries, financial losses to the owner, economic losses to the region and less quantifiable dimensions identified as important in Phase 1 of the Assessment Cycle, Decision-Makers' Goals, Criteria and Priorities;
4. *Vulnerability Analysis* – estimating the probability that each threat to each asset will in fact result in the estimated consequences, given that the event occurs and considering the effectiveness of available security measures;
5. *Threat Likelihood Assessment* – estimating the probability or likelihood that the initiating event will occur;
6. *Risk and Resilience Assessment* – estimating the risk and resilience associated with each event on each asset;
7. *Risk and Resilience Management* – evaluating risk-reduction and resilience enhancement options for their value (usually net benefits, benefit/cost ratios and value added relative to the objectives developed in Phase 1) and selecting, implementing and managing those that are selected.

Figure 4.4 **The RAMCAP *Plus* Process is Selective**



While some risk and resilience analysis approaches encourage the user to analyze every aspect of their operations, RAMCAP is explicitly selective. The reason for this is the recognition that the time of the people needed to carry out the analysis is valuable to their organizations and also that the level of tedium in trying to look at everything may compromise the quality of looking at the most important things. In several RAMCAP steps, the user is encouraged to rank or prioritize facilities, assets, and/or threat-asset pairs for the amount of attention they will receive. *Figure 4.4* shows where in the process these rankings should occur.

In each of these, the criteria for ranking are based on the relevance to the decision-making to follow. Knowing that resources are limited assures that only the more important – that is, more consequential – elements will be considered. It is wise to prune out and defer the less consequential elements. In Step 1, facilities that are not critical or have relatively low consequences are deferred or eliminated, then assets within critical facilities that are non-critical or low-consequence are set aside. In Step 2, low consequence threat-asset pairs are identified and deferred, as they are at the end of Step 3. In Step 6, threat-asset pairs that have expected consequences and resilience levels that the owner and the public can accept are set aside as are options with low net benefits or benefit/cost ratios. This selectivity, illustrated in *Figure 4.4*, is central to keeping the amount of time and the level of attention focused on the most important elements in the decision.

In a RAMCAP analysis, a suite of specific threat scenarios is provided. The use of common threat and hazard definitions is central to the comparability of the results of the analyses. The majority of the terrorism scenarios in this publication were specified by DHS.[8] Naturally, the owner/operator user of RAMCAP may also want to add threats other than those provided for its local use, but not included in the scenario set that is used in comparisons with other assets. Users may also delete threats that are not feasible (e.g., water-borne attacks in a desert or hurricanes on the west coast of the U.S.).

With the consistent threats used in a RAMCAP analysis, the consequence analysis estimates potential fatalities, injuries and financial losses to the owner of the facility. In prior versions of RAMCAP, economic losses to the community were also estimated. In RR/SAP, they are estimated in Phase 5. In addition to the usual elements of risk, other dimensions of consequences, e.g., psychological, environmental, military readiness, are noted if they might have significance in decision-making.

Vulnerabilities of critical assets to specific threats are estimated using tools such as failure trees, event trees, and path analysis and expressed as conditional probabilities that assume the occurrence of the threat event.

Team-based assessment and evaluation raises the awareness of the system's vulnerabilities and resilience.

Threat likelihood (or probability) is estimated in different ways for each type of threat. For naturally occurring events, the likelihoods are estimated directly from historical data compiled by federal agencies, the weather service and commercial forecasting services. The likelihood of dependency hazards uses historical outage rates as a baseline and adjusts them to reflect their resilience levels. Proximity hazard likelihood is directly estimated, but in a regional scale assessment that includes all utilities and major economic drivers. Many of the facilities near the one being analyzed will have been analyzed independently. This is one of the reasons a region-wide assessment can be more

---

[8] The only scenarios that have not appeared previously in one or more SSGs are the dependency and proximity hazards, both of which are included in the most recent NIPP (DHS, 2009).

effective – it explicitly analyzes the risks and resilience of the utilities, major economic drivers, first responders and their interdependencies. For accidents and crime, historical statistics are used as a baseline, but can be adjusted in various scenarios.

For terrorism threats, a more complicated approach is needed. It starts with consultation with intelligence and law enforcement officials so that any actionable intelligence of tendencies of known terrorist organizations can be incorporated into the estimates of the likelihood of an attack on the subject facility. Occasionally an intelligence agency may be able to provide quantitative estimates of the likelihood of attack. These are treated very seriously and can be used directly. More often, however, no such quantitative estimates can be provided, so a "proxy" method is employed. The proxy method assumes the terrorist is a rational decision-maker seeking to maximize the damage and fatalities in selecting the asset to attack and the mode of that attack. The process takes into account the available understanding of the terrorist's capabilities, historical trends and broad intelligence interpretations, all conditioned to the individual asset and based on local considerations (e.g., number of similar targets in the region, target attractiveness relative to alternative targets, deterrence). From this, a proxy or surrogate estimate can be calculated. This number is not a true probability because there are significant unknowns that cannot be included, but the proxy indicator is believed to capture major elements of terrorist decision-making and to correlate with the true probability.

... results are directly comparable from asset to asset within the system, between firms in the same sector, and to other critical infrastructures.

The execution of a RAMCAP assessment, whether for the first time or as an update on previously completed security analyses, engages the leaders and staff of the facility and their partners who respond to emergencies, such as fire and emergency medical personnel. Team-based assessment and evaluation raises the awareness of the system's vulnerabilities and resilience. The results of a structured and rigorous risk assessment such as RAMCAP are risk reduction and resilience enhancement. These results are directly comparable from asset to asset within the system, between firms in the same sector, and to other critical infrastructures. This direct comparability frequently results in the emergence of best practices and improved system practices. Quantification of both risks and benefits, in terms of fatalities, injuries, facility recovery costs and economic losses to the community, can provide a powerful foundation upon which to base resource allocation decisions. Because the RAMCAP process is designed for quick self-assessment without outside expertise, it is best used to identify specific assets, threats and vulnerabilities that require more in-depth engineering risk assessment before directing major investments. The user-friendliness and efficiency of the RAMCAP process makes it appropriate for periodic re-application to measure progress in reducing risks, enhancing resilience and to note changes in the threat environment.

4.4 Preparing to Use the RAMCAP Process

4.4.1 Composition of the Evaluation Team

A RAMCAP risk assessment is a multi-disciplinary evaluation exercise that typically requires a risk assessment team composed of individuals with specialized expertise. *Table 4.1* suggests the composition of the RAMCAP assessment team. During the assessment, all team members will not be needed on a full-time basis, so it is useful to differentiate the "core" team members, listed at the top of the table, from members who will be needed on an "on-call" basis.

While it is entirely possible to use RAMCAP with no specific training, it usually increases the efficiency of the process if at least two members of the core team take training. Currently, such training is offered by the American Water Works Association.[9] Their training program is specifically referenced to the ANSI/ASME-ITI/AWWA J100-10 standard. It is general enough to use RAMCAP in any environment.

The RAMCAP risk/resilience assessment focuses on potential adversarial, natural and dependency hazards that could cause severe impacts on supporting systems at the facility. The shipment, storage, and handling of any form of flammable and/or toxic substances could pose a vulnerability concern that may not be integrally associated with the asset, but should be part of the risk assessment. Therefore, the security risk assessment studies should be conducted by a team with skills in both the security and safety procedures as well as the operational and reliability concerns of the facility. The team will evaluate traditional asset security, safety-related

Table 4.1 **Suggested Composition of a RAMCAP Assessment Team**

Role	Expertise
Core Team	
Team Leader	Knowledge of and experience with the RAMCAP risk assessment process and familiarity with configurations and operations of facilities being evaluated. This individual generally has taken specific training in the RAMCAP process.
Security Specialist	Knowledge of and experience with the application of facility security procedures, technologies, methods and systems, including law enforcement issues.
Safety Specialist	Knowledge of potential natural hazards and their resulting consequences to the asset, safety design requirements, procedures, methods, and safety systems analysis results.
Risk Analyst	Knowledge in the analysis of security risk application and procedures, data collection formats for important information analysis and evaluation, and documentation of security risk factors and results. RAMCAP process training would be beneficial for this individual.
Operations Manager/ Design Engineer	Knowledge of the full-asset operations and equipment management and system criticalities.
Maintenance Manager	Knowledge of critical operating equipment, its initial and replacement costs, identification of "critical spares," work-around procedures, and preventive maintenance programs.
Others, as Needed	
Facility Manager	Knowledge of the design of the asset and related systems under study including mission, customers served, asset value, functionality, critical assets, customer base and expectations, key suppliers, and operations and emergency action procedures.
Information Technologist	Knowledge of information systems technologies (including Supervisory Control and Data Acquisition (SCADA) and cyber security provisions. Knowledge of facility manual and remote control systems, business cyber and security systems, and security and emergency operations plans.
Regulatory Compliance Specialist	Knowledge about state and federal regulatory requirements and status.
First Responders	Knowledge of the security program and its systems to include policies and procedures, emergency response plans, and evacuation procedures. May include representatives of local law enforcement, fire protection and emergency medical personnel.
Financial Specialist	Knowledge of asset's billing and financial accounting systems, enterprise asset management systems and databases, cost accounting and tax principles for the specific asset.

---

[9] For more information on training offered by AWWA, please see http://www.awwa.org/Conferences/learning.cfm?ItemNumber=3413&navItemNumber=1519.

Table 4.2 **Checklist of Documents to be Assembled Prior to or Early in a RAMCAP Assessment**

A. Before on-site work or early in on-site work

1. Plot, schematic and/or aerial photo of each facility with defined dimensions, providing details of locations of major components and critical elements for further evaluation (at least a Google™ map or Google™ Earth image, with scale)
2. Schematic of the major process flows in each facility or system
3. Dates and citation of building codes in effect at time of original construction or major rehab
4. Replacement cost data on facilities construction or major equipment
5. Identify the source and point of entry/egress for key infrastructures, e.g., power, water and wastewater services, telecommunications, key suppliers, major customers, employees
6. Description of direct, remote and manual control systems, including SCADA systems
7. Insurance coverage for capital and business interruption expenses, including potential loss of revenue, impacts on user rates, and critical customer base
8. Previous risk assessment(s), SVA(s), or other security risk analysis reports completed for the facility (if available), Buffer Zone Protection Plan (BZPP) description and application for facilities
9. Most recent annual report
10. After-action reports on any major disruptions

B. Called for During On-Site Work

1. Physical security systems and resilience preparedness
    a. Existing and planned operator and asset security operations systems, procedures, countermeasures, and physical security plans that describe security systems in-place, including: barriers, closed-circuit television (CCTV), access controls, intrusion detection system (IDS), as well as protective measures
    b. Emergency preparedness and/or continuity protocols and action plans, studies and maps, drills or exercises conducted with law enforcement authorities, and response procedures and agreements (those of the facility and of off-site responders), including on-site consequence mitigation systems and response times for local or state law enforcement and fire-rescue
    c. Security incident reports
2. Cyber security policies, plans, and procedures, including password controls
    a. SCADA system design and operational characteristics (e.g., how systems are connected, use of data historian reports, remote access capability, etc.)
    b. Information systems, including flow diagrams and management policies
3. Personnel identification system – employees, contractors, visitors – areas of restricted access, ID badges, ID verification (automated and manual)
4. [Only if available and permissible, for use on-site at NES] System map or GIS representation of the distribution, collection, service or patrol areas or networks network

consequences and vulnerabilities, and subsequently implemented countermeasures. Input from other specialized engineering and safety organizations at the facility or from outside should be solicited as needed for certain portions of the RAMCAP risk assessment.

4.4.2 Documents to Be Assembled Prior to the Assessment

Compiling documents and databases needed in the RAMCAP assessment ahead of time can save valuable time and avoid frustrating breaks in the continuity of the process while data are retrieved. *Table 4.2* provides a checklist of documents usually needed for a RAMCAP assessment. The list is illustrative, not definitive. The team leader should define which of these items or others are likely to be required based on his or her knowledge of the facility.

4.5 The First Six Steps of the RAMCAP Process

As seen earlier, *Figure 4.3 (above)* shows the seven steps and the iterative nature of the RAMCAP process. The feedback arrows imply that the assessment of benefits is a reiteration and modification of some or all of the same logical steps as the initial risk estimate. Reducing risks and enhancing resilience require that the options being considered reduce consequences (including duration or severity of service denial), vulnerability and/or the likelihood of occurrence. The process estimates the changes attributed to a countermeasure or mitigation option. Thus, the benefits are defined as the change in risk and/or resilience indicator, and the costs include the investment and operating costs of the option. This benefit/cost ratio can be used to rank the options by the risk reduction per dollar of cost. If the decision-maker prefers other measures of marginal merit (e.g., return on investment), the RAMCAP quantitative assessments can be summarized to produce the other metrics.

… benefits are defined as the change in risk and/or resilience indicator, and the costs include the investment and operating costs of the option.

The feedback arrows also imply that the process is reiterated for three additional concepts: (1) for each relevant threat for a given asset; (2) for each asset critical to the mission of the organization; and (3) over time as part of continuous improvement and periodic evaluation of progress (e.g., annually as part of budget development) or as needed based on changing threat circumstances.

Before beginning, it is useful to review the nature of scales of measurement. Stevens (1946) defined four scales of measurement: (1) *nominal*, or the ability to discriminate and name items, e.g., categories or genus and species names; (2) *ordinal*, or the ability to order or rank items in a meaningful series, e.g., college football team ratings, or good-better-best survey categories; (3) *interval*, or the ability to describe a quantity in terms where the intervals between any two are the same but lacks a true zero point, e.g., temperature in Celsius; and (4) ratio scales, or interval scales with a natural zero, e.g., items that are counted or measured by rulers.

All arithmetic functions may be used with ratio scales, but only addition and subtraction may be used with interval data and no arithmetic functions can be used with the ordinal or nominal scales. This is important in a RAMCAP analysis because it is often useful to make rough initial estimates using temporary, informal ordinal scales to focus attention on high-priority items. The final estimates, however, are all in ratio scales. Having the basic metrics in ratio scales allows calculation of absolute (as opposed to relative) risk and resilience, net benefits, benefit/cost ratios, value on the multi-attribute scale developed in RR/SAP Phase 1, and the value-cost ratio. Estimates made using any scale less than ratio cannot be calculated meaningfully, so cannot be compared or used in resource allocation decisions.

4.5.1 Step 1 – Asset Characterization

This step analyzes the organization's mission and operational requirements to determine which facilities and assets within them, if damaged or destroyed, would diminish the facility's ability to meet its mission or carry out its function. Because the number of facilities and assets in a region owned by an organization can be substantial, it is imperative that the assessment team identifies the high-priority facilities and assets from an initial ranking and screening. High-priority assets are typically addressed first and in the greatest detail.

Critical facilities and assets are identified based on very preliminary estimates of the amount of disruption to mission or function or gross potential losses of dollars or lives that would result if the facility or asset were removed from service. The facilities and assets evaluated include the offices, plants, the infrastructures and supplies on which they depend, and the distribution and/or collection systems. These assets may include physical plant, cyber systems, knowledge base, human resources, customers or critical off-site suppliers.

This step consists of seven tasks:

Task 1.1. Identify the critical missions, functions and services provided by the organization in the region. This usually has been debated and refined previously as the organization has developed plans of various sorts. The point is to get a very simple definition of what the organization produces, why it might be critical, and to whom.

Task 1.2. List all the facilities involved in the operations of the organization in the region and identify the specific facilities that are *necessary* to performing the missions and functions of the organization. Of those that are necessary, identify all that are critical to the organization's performing its missions, the withdrawal of which would impede the organization's mission in serious ways. Defer consideration of all facilities that are not both necessary and critical.

Task 1.3. List the potentially critical assets in each of the remaining facilities. It is often useful to lay out the workflow by which the organization converts its inputs (raw materials, labor, utilities, etc.) to outputs (products and services, e.g., kilo-Watt-hours or gallons of potable water delivered, fires avoided or suppressed, etc.). Assets that are necessary and critical to accomplishing this flow are potentially critical.

Task 1.4. Identify and document existing protective countermeasures and mitigation measures/features that would limit the amount of damage or loss that each asset would incur.

Task 1.5. Identify and list any necessary internal or external infrastructures, utilities or supplies that are necessary and critical to sustaining the workflow that carries out the organization's missions. Add to the asset list any of these that are necessary and potentially critical.

Task 1.6. Estimate the *potential* worst-reasonable-case consequences if each asset or supporting element were to be abruptly withdrawn from performing its role in the organization's mission, regardless of the reason. The point of the worst-reasonable-case assumption is to tie the analysis to the reasonably possible, even if highly improbable, events. The worst-reasonable-case assumption for adversarial threats is to assume the adversary is goal-oriented, outcome-maximizing, rational and adaptive to the conditions as encountered, e.g., moving from the prime target that cannot be reached to a second target that can. It means that the adversary has detailed understanding of the facility and its processed. It does *not* assume unreasonable capabilities, luck or anything else. For natural hazards, it means attending to hazards for which there is reasonable possibility of occurring at the site, but does *not* assume that unlikely events occur in combinations that are not causally related. The consequences to be considered are gross losses to the owner of the asset, gross losses to the regional economy or human casualties (fatalities and injuries serious

Table 4.3 **Example of Initial Consequence Estimates**

	Group A Very Bad	Group B Bad	Group C Moderately Bad	Group D Moderate	Group E OK
Fatalities	Any	None	None	None	None
Serious Injuries	Any offsite	No off-site; some on	None	None	None
Regional Econ. Loss	≥ $500 M	$200-500 M	$50-200 M	$1-50 M	Negligible
Utility Econ. Loss	≥ $50 M	$20-50 M	$5-20 M	$1-5 M	Negligible
Environmental Damage	Irreparable	Very Severe	Severe	Moderate	Negligible
Service Denial	≥ 300 %-days	200-300 %-days	100-200 %-days	10-100 %-days	≤ 10 %-days

enough to require hospital treatment or loss of work for more than a week), major environmental impacts, etc. Completely disregard the likelihood that a disruptive event would occur.

Some users have found it helpful to set up an informal table such as shown in *Table 4.3*, which shows thresholds one group uses to decide the level of potential consequences. The purpose here is to eliminate or defer those with a minimal or tolerable worst-case consequence, not to make a refined estimate. This estimation process should not take much time or deliberation because the estimates will be refined considerably in later steps; this is the reason for using the rough ordinal scale. If a disagreement arises, after a small amount of discussion, accept the higher estimate for the moment and move on.

Task 1.7. Rank or rate the assets based on these rough estimates and defer or eliminate those below a specific cut-off defined by the analysis team. One way to do this is to use the example and simply define all assets having any category of consequences in, say Groups A, B and C, as critical and defer the rest. The retained assets are defined as critical for the analysis. Any assets that are set aside in this task can be moved back into the core analysis if it is realized later that it is in fact critical.

4.5.2 Step 2 – Threat Characterization

In this step, the threat scenarios to be used are identified and described in enough detail to estimate vulnerability and consequences. These are then considered as occurring to the higher priority critical assets identified in Step 1. Consequences of these threat-asset pairs are then roughly estimated, and the threat-asset pairs are ranked for priority. Lower ranked threat-asset pairs are deferred or eliminated from the analysis, while higher-priority pairs are passed to Step 3. Threat scenarios may be potential malevolent attacks, natural hazards, interrupted dependencies, or potentially hazardous neighbors. Organizations that complete a RAMCAP analysis strictly for their own internal decision-making may define threat scenarios as they choose, but should use a common set across all relevant organizational units so that the benefits will be comparable and rational resource allocations can be made. However, for risk knowledge to be useful and meaningful to other organizations, regional decision-makers, sectors, and possible grant donors, state agencies, etc., direct comparisons must be made based on a common set of defined reference threat scenarios.

The original set of RAMCAP reference threat scenarios, suggested by DHS, relied on characterizations by law enforcement and intelligence organizations and focused on terrorism exclusively. The list has been enlarged

Table 4.4 **RAMCAP Reference Threats**

Event Type	Event Description			
Natural Hazards	Hurricanes	Earthquakes	Tornadoes	Floods
Dependency & Proximity	Loss of Utilities	Loss of Suppliers	Loss of Employees	Loss of Customers
Wear & Aging: Major Accidents	Loss of Transportation		Proximity to other targets	
Product Contamination	Chemical	Radionuclide	Biotoxin	Pathogen
	Weaponization of waste disposal system			
Sabotage	Physical-insider	Physical-outsider	Cyber-insider	Cyber-outsider
Theft or Diversion	Physical-insider	Physical-outsider	Cyber-insider	Cyber-outsider
Attack: Marine	Small boat	Fast boat	Barge	Ocean ship
Attack: Aircraft	Helicopter	Small plane	Regional jet	Long-flight jet
Attack: Automotive	Car	Van	Mid-size truck	18-wheeler
Attack: Assault Team	1 assailant	2-4 assailants	5-8 assailants	9-16 assailants

to include the other types of risks primarily to infrastructures as suggested by events (e.g., natural hazards) and improved understanding (e.g., dependencies and proximity hazards). It is important to include the asset-level threats or events that are to be included in systems or system-of-systems scenarios because these will be activated in the later analyses.

Table 4.4 summarizes the current suite of reference threats. DHS, in consultation with the RAMCAP process developers, provided the terrorism reference threat scenarios. These specified scenarios are not "design basis threats," which would imply that the organization should take steps to withstand the threat to continue operations. Rather, these are "benchmark" or "reference" threats that span a range of possible threats across all critical infrastructure sectors. These reference threat scenarios can be used to assess total risk to the nation and guide investments for risk reduction and resilience enhancement.[10] The natural hazard threats are derived from data compiled over many years by several federal agencies and are based on the physical location of the analyzed facility. Product contamination was added for sectors whose product is physically consumed by people, e.g., water, food, pharmaceuticals. Dependency and proximity hazards address the issue of being critically dependent on elements of the supply chain, especially basic infrastructures, and being located close to other assets posing the risk of collateral damage. RAMCAP reference threats may be considered in three categories, malevolent, natural and dependency/proximity.

Natural hazards. The hurricanes of 2005 caused the inclusion of natural hazards, including hurricanes, tornadoes, floods and earthquakes. All of these have been updated and ice storms have been added in the present project. All that are possible should be included. If the organization is located in an area where other natural hazards are precedented or considered possible (e.g., wild fires, mud slides), they should be added to the list of natural hazards following the same general logic for the organization's and region's purposes, but not included if comparisons are to be made with RAMCAP analyses from other organizations or regions that did not include them. A special class of "natural" hazards is wear and aging. Generic methods for analyzing these await further development. As with local natural hazards, organizations should

---

[10] While in some cases, the severity of a specific type of threat attack is expected to increase from left to right on *Table 4.4* (e.g. marine, aircraft, land-based vehicles and assault), no such severity continuum is implied in others or their relative location of the threat in the table.

add these using the standard methods in their industry.

Interdependencies and proximity threats. A second set of hazards was added to include risks due to supply chain breakdowns (including utilities) and collateral damage from adverse events on nearby facilities. For example, as a result of the attack on the World Trade Center, the damage to the buildings, a primary target, also severely damaged the systems providing transportation, power, water and sanitation, telecommunications, banking, etc. One result was that 500,000 people stranded in Manhattan were boat lifted to transportation upstate and in New Jersey and Long Island – an operation half-again larger than the evacuation of Dunkirk (CNP, 2011). Dependency and proximity hazards focus only on the facility's direct relationships with suppliers, utilities, customers and neighbors, of which the facility's management would have direct knowledge. Other dependency hazards that are the product of cascading failures across indirectly connected infrastructures require a more regional approach described in the next two chapters, because the individual owner cannot be expected to know about these remote linkages. Proximity hazards are a "dependency" that results from being located near potentially hazardous sites (e.g., a rail yard where numerous cars containing toxic and explosive chemicals) or could become the target of a malevolent attack.

The identification of dependency threats within and between infrastructure systems can be difficult and time consuming. As initial identification of dependencies, it has proven to be efficient and effective to use a facilitated discussion by representatives of two systems at a time. These discussions are supported by large-scale Geographic Information System (GIS) maps that depict the geographic disposition of the systems under considerations. The facilitators of these paired system reviews are able to document the points of dependency, up-stream vulnerabilities and down-stream consequences. Potential solutions to reduce cascading failure may be noted for further analysis. Cascading failures in and across critical infrastructure systems are a primary mechanism for the propagation of failure and the magnification of impacts. The process of facilitated, pair-wise assessment of inter-system dependencies and interdependencies is found in Annex 4A.

Threat characterization requires that the assessors assume an attempt to maximize the consequences of the worst reasonable case.

Malevolent threats. The set of specific malevolent threat scenarios was suggested by DHS, based on their characterizations of the collective activities of law enforcement and intelligence organizations. DHS and other organizations have developed an understanding of the means, methods, motivations, and capacities of adversarial threats to include various modes of attack with explosives, shown in blue (e.g., air, land, and water), various sizes of attacks (e.g., small, medium, large, and extra large), and attacks *not* involving explosives, shown in white (e.g., contamination, sabotage, theft, and cyber attacks).

The work of this step consists of six tasks.

Task 2.1 Decide which of the standard reference threats in *Table 4.4* will be included in the analysis. The organization must decide which of the defined scenarios represent real, physically possible threats for the facility being assessed; some, such as a major marine attack in Arizona, for instance, can be deleted. If the assessment team believes the likelihood of attack using explosives is so small that the time to analyze the number of such attacks is not justified, the analysis team may assume that the perpetrator will select the most cost-effective transport solution from among these for each asset. The users are advised to retain the four levels of magnitude for whatever transport mode is selected.

Task 2.2 Determine whether local threats not included in the standard threat table pose a danger roughly as likely as the least likely of the standard reference treats. If so, they should be added to the reference threat list for all assessments in this same general vicinity. These are most likely to be local natural hazards, but could be threats of any sort.

Task 2.3 Define all material (non-financial) inputs to the functions performed by the facility. These include personnel, raw materials, utilities (including communications), equipment, transportation, etc. Of these, define which are critical inputs in the sense that their absence would cause the functions to fail and could not be replaced in a timely fashion. Any that are critical but either inventoried at the facility or quickly replaceable are deleted. It can be extremely useful in this task to meet with the utilities that support the facility and determine which of their assets are critical to the facility's mission and whether there are alternative sources of supply, either within the facility (e.g., emergency power generation) of from the utility (e.g., switching routines that route power to the facility even if the usual substation is compromised). These are the first-order dependency threats to the facility. See Annex 4A.

Consequence analysis identifies and estimates the worst reasonable consequences generated by each *specific threat-asset combination…*

Task 2.4 Identify any structures, circumstances or conditions outside the boundaries of the facility that could cause harm or loss to the facility. These might include railroads or highways that carry explosive or highly toxic materials that could reach the facility being assessed in the event of an accident.

Task 2.5 Array a matrix of the threats identified in Tasks 2.1 through 2.4 against the assets defined as critical and high priority in Step 1. For each threat-asset pair, quickly estimate whether the particular threat is possible with the particular assets. For those that are possible, make a rough estimate of the magnitude of consequences for human and dollar losses to the facility owner or to the regional economy, or other major impacts. These rough estimates should be made using an ordinal scale, which may be stated in either numerical (e.g., a 10-point scale) or verbal (e.g., major disaster, serious disaster, crisis, manageable crisis, disruptive but not major). As in Step 1, completely disregard the likelihood of the initiating event, but do consider the effects of the existing protective or mitigation measures.

Task 2.6 Select the threat-asset pairs that have the most severe levels of consequences and defer all others. This high-priority list of threat-asset pairs is the focus of the next three steps of the RAMCAP process.

Threat characterization involves more than assuming the specific threat is applied to a specific target or asset. It requires that the assessment team consider each threat scenario and its potential to cause the maximum credible consequences, i.e., the worst reasonable case. If a threat scenario can result in an asset causing consequences beyond the destruction of the asset or facility, then this combined scenario should be considered. For example, the destruction of a dam could release water downstream and inundate property below the dam. If this event were to occur at a time when the inundated area would be highly populated, for example on a holiday weekend, the water becomes a weapon to cause additional consequences. Threat characterization requires that the assessors assume an attempt to maximize the consequences of the worst reasonable case.

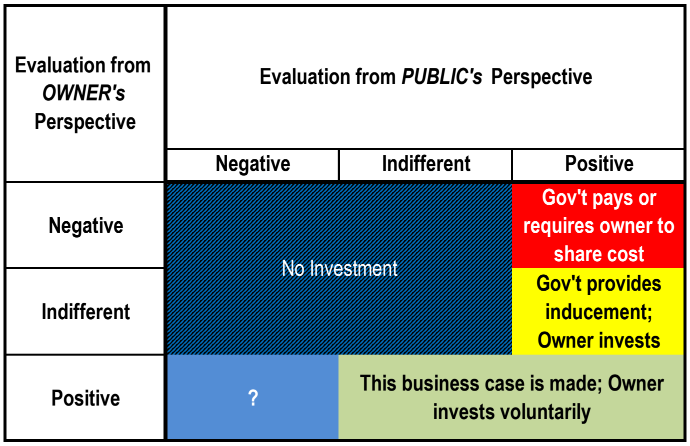
4.5.3 Step 3 – Consequence Analysis

Consequences in a RAMCAP analysis include all impacts of the initiating event. Consequence analysis identifies and estimates the worst reasonable consequences generated by *each* specific threat-asset combination, refining the previous rough, ordinal estimates into more thoroughly considered estimates stated in natural terms – numbers of fatalities and serious injuries, economic and financial losses in dollars, value scores on the multi-attribute objective – all ratio scales that can be used in decision-making. This step reviews facility design, layout and operation to identify the types of consequences that might result.

Fatalities and serious injuries include harm to employees, customers and bystanders. Many organizations choose to keep these estimates separate from economic estimates, while others prefer to convert them to dollar terms and include them with the financial and economic terms discussed below. Regardless of this preference, it is correct to include all direct financial liabilities attributed to these casualties in the financial losses. Moreover, some organizations find it useful to differentiate employees from others who are harmed, so maintaining separate metrics for each group is recommended.

Economic impacts are almost universally recognized as key indicators of consequences in analyzing risks from terrorism, natural disasters and dependencies. Specifically defining the meaning of "economic impacts" is necessary for a risk management methodology to maintain consistency of terms and metrics. The RAMCAP process defines "economic impacts" as appropriate for risk management decision-making at two levels: (1) the financial losses to the organization owning the asset; and (2) the economic losses to the regional metropolitan community the organization serves in both direct and indirect consequences. The logic for this dual analysis is illustrated in *Figure 4.5*.

Figure 4.5 **Economic/Financial Consequence Analysis: Two Perspectives Needed**



Evaluation from *OWNER's* Perspective	Evaluation from *PUBLIC's* Perspective		
	Negative	Indifferent	Positive
Negative	No Investment		Gov't pays or requires owner to share cost
Indifferent			Gov't provides inducement; Owner invests
Positive	?	This business case is made; Owner invests voluntarily	

Assume an analysis of a risk/resilience situation is undertaken from the perspectives of the owning organization (either a public agency or a private organization) and the general public, respectively, to decide whether to invest in an option to enhance security and resilience. To keep it simple, from both perspectives, the results of the analysis can be negative (i.e., a benefit/cost ratio (B/C) less than 1.0 or a rate of return (ROR) less than the cost of capital), indifferent (i.e., B/C of 1.0 or an ROR of about the cost of capital), or positive (i.e., B/C greater than 1.0 or ROR exceeding the cost of capital).

If the investment is evaluated as negative or indifferent from both perspectives, there is no investment. If it is positive from the owner's perspective, and either indifferent or positive from the public's, the owner will make the investment – the "business case" for the investment is made. If the owner's evaluation is positive, but negative from the public's, the outcome depends on whether the public's view can be imposed, e.g., by legal prohibition or regulation, the owner can be made to compensate the public (e.g., fees, special assessments) or the owner's view will prevail. Many environmental issues are of this nature. If the owner's evaluation is indifferent or negative and the public's is positive, the public, through government, either requires the owner to make the investment (again, as in many regulations) or provides incentives to induce the owner to make the investment by raising its value to the owner to an acceptable level. The circumstances either a negative public evaluation with a positive owner's assessment or of a positive public evaluation with an indifferent or negative owner's evaluation arises in cases economists call "externalities" – when there are costs or benefits that are not captured by the owner, so are not considered in his evaluation – or "public goods" – valuable goods or services for which

… economic consequences “ripple” through the regional economy, with the total impacts being some multiple of the direct impacts...

the owner cannot exclude some while including others, so cannot charge for the service.

Conducting the analysis from both perspectives allows the analysts to see whether the owner can be expected to make the investment without incentives or the public’s participation is required to either avoid negative options or stimulate positive ones. Looking at the situation in these terms also suggests new forms or partnerships between owners or between public and private organizations.

Losses from the owners’ perspective (or investments to avoid them) are the usual framework for conventional risk analysis, while losses from the public’s perspective (or investments to avoid them) are the usual framework for public policy analysis. Looking at both in the same analysis is unique to the RAMCAP process. The point of the dual assessment is to identify where the benefits and losses fall and, therefore, who should pay the costs. By doing the analysis together, the potential for communications leading to the correct decisions and cost-sharing are facilitated.

We will call losses to the owner organization “financial” losses, because they will be reflected in the organizations financial operations, whereas we will call losses to the regional public “regional economic” losses. The portion of these losses that are actual lost economic activity will be reflected in the regional income accounts, but the portion that relates to human casualties will not, so must be added when considering total losses and total benefits to the public.

Losses to the regional economy, estimated in RR/SAP Phase 4, demonstrate the severity of lost organization functionality to its served community and serves as the principal measure of fragility and resilience on the metropolitan region. (Note: Economic consequences for communities larger than the metropolitan area, e.g., the state, multi-state region or the nation may also be of interest to the decision-makers and can be addressed using the same methods as used at the metropolitan level.)

Financial losses to the organization include all “forward cash” costs to repair or replace damaged buildings and equipment, abandonment and decommissioning costs, site and environmental cleanup, revenue losses (including fines and penalties for failing to meet contractual production levels) while service is reduced, direct liabilities for casualties on and off the property, and environmental damages that cannot be fully mitigated. These costs are reduced by applicable insurance or restoration grants and must be corrected to account for tax effects for tax-paying organizations. Financial losses do *not* include non-cash charges like depreciation, depletion, good will, etc.

Regional economic losses are the reduction in regional economic activity due to the disruption of the asset by the threat. The primary concern for the public or community is the length of time, quantity and sometimes quality of service denied, and the economic consequences of service denial to the organization’s direct suppliers and customers. In addition to these “direct” losses, the community suffers “indirect” losses through reduced economic activity in general, i.e., to the suppliers’ suppliers and customers’ customers, and so on. The economic consequences “ripple” through the regional economy, with the total impacts being some multiple of the direct impacts, hence the term “multiplier effect.” When service denial is of short duration and/or customers cope through conservation, substitution, redundancies, making up lost production later through overtime or added shifts, the region is said to be “resilient” (Rose, 2004 and 2006; Rose and Liao, 2005; Rose et al., 2007). The public’s objective is to enhance the resilience of critical infrastructures on which they depend.

Assessment of direct and indirect business interruption losses resulting from damage to an infrastructure asset is the purpose of the infrastructure Inoperability Input-output Model (IIM), which is discussed in Chapter Nine, The implications for RAMCAP are that both sets of dollar estimates will be available for use in the overall evaluation.

Other consequences of the threat-asset pair are identified and described qualitatively. These include impact on iconic structures, governmental ability to operate, military readiness, citizen confidence in the organization, product, and/or the government.

The work of Step 3 consists of five tasks, the first four of which are repeated for each threat-asset pair. The last step is completed only when the first four have been completed for all threat-asset pairs. The tasks are:

Task 3.1 Estimate the number of human fatalities and serious injuries under worst-reasonable-case assumptions and document.

Task 3.2 Estimate the financial losses to the owner under worst-reasonable-case assumptions and document.

Task 3.3 Estimate the service denial or outage as the number of units per day and the number of days under worst-reasonable-case assumptions and document. Pass these to the IIM (RR/SAP Phase 4), described in Chapter Nine , where the regional economic losses will be calculated.

Task 3.4 Describe any other consequences of significance in words and numbers as appropriate.

Task 3.5 Rank the threat-asset pairs by their estimated consequences to the owner and to the regional economy, *disregarding* the likelihood of the threat or hazards. If some of these have materially less impact than the others, they should be deferred to keep the analytic focus on those with the greatest consequences.

In making these estimates, it is often useful to bring other tools to bear. Many of these may already be in use by the organization. For example, EPA requires organizations that use toxic gases to file a Risk Management Report based on a standard approach called RMP*COMP^{TM} (www.epa.gov/emergencies/rmp) part of which is the estimation of the population potentially at risk of a gas release (in a circle based on a radius estimated from the specific gas, the amount released, the local terrain and the U.S. Census population in the specific radius. A subset of this population (that which falls in the specific plume, not the whole circle) would be affected by an actual release.

4.5.4 Step 4 – Vulnerability Analysis

Step 4 analyzes the ability of the asset – in its setting of all existing countermeasures and protective systems – to withstand the specific threat, provided that the threat or hazard happens. Specifically, it estimates the conditional likelihood of each specific threat or hazard to overcome the defenses of the asset to the level identified in the consequence estimate from Step 3 for that threat-asset combination, *given that the initiating event occurs*. In the case of a terrorist attack, this means the probability that the attack would be successful, resulting in the estimated consequences. For other hazards, it means the probability that the estimated consequences would result if the specific hazard occurs. Vulnerability analysis involves an examination of existing security capabilities and structural components, as well as countermeasures and their effectiveness in reducing damages from threats and hazards.

The work of Step 4 consists of only three tasks, but can take a considerable amount of time on the second, critical task. For *each* threat-asset pair:

Task 4.1 Review all *existing* countermeasures and protective systems and procedures to thoroughly understand how they would or would not protect the specific asset from the specific threat. These would include active and passive systems, but would also include such things as natural protection from the local terrain, structure design, and local police or security response.

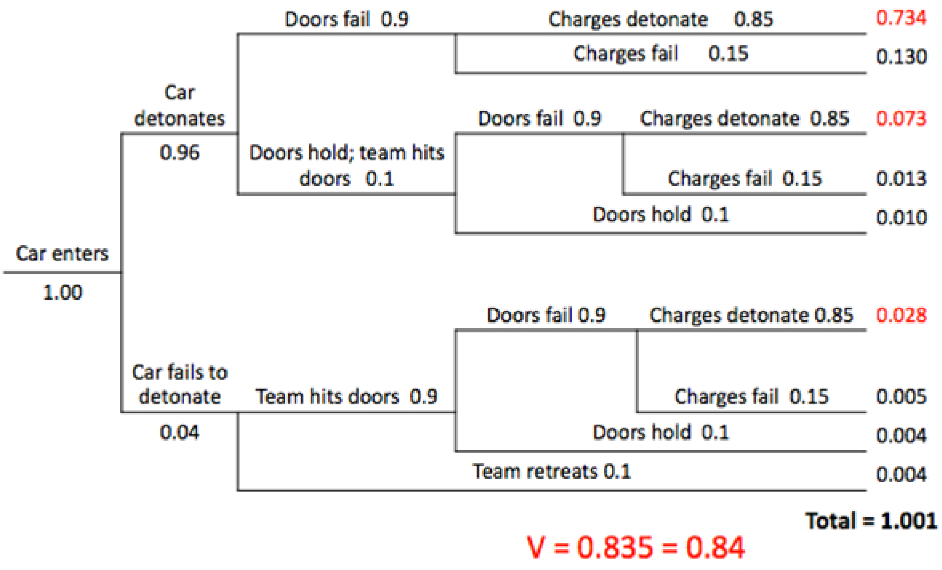


Figure 4.6 **Example of an Event Tree**

Task 4.2 Analyze the vulnerability of the specific asset to the specific threat or hazard using any one of four methods:

1. *Direct expert elicitation* – members of the evaluation team familiar with a facility's layout and workflows and knowledgeable about the asset discuss the likelihood of success and their reasoning for their estimates. Sometimes trained facilitators, on staff or under contract, are used to elicit the judgments. In its more elaborate form, a statistical "Delphi" or Analytical Hierarchy Process can be used to establish a consensus estimate of vulnerability.
2. *Vulnerability logic diagrams (VLDs, also called "path analysis")* – the flow of events from the time an adversary approaches the facility to the terminal event in which the attack is foiled or succeeds, considering obstacles and countermeasures that must be surmounted, with each terminal event associated with a specific likelihood estimate. This is frequently complemented by time estimates for each segment and compared with an estimate of the reaction time of a counterforce once the attack has been detected.
3. *Event trees* (also called "failure trees") – the sequence of events between the initiation of the attack and the terminal event is described as a branching tree, where each "branch" represents the possible outcomes at that junction, e.g., a car bomb may detonate or not (two possible events), as in the first branch of the example in *Figure 4.6*. The evaluation team estimates the probability of each outcome. Multiplying the probabilities along each branch, from the initiating event to each terminal event, calculates the probability of each unique branch, while all branches together sum to unity (1.0). *The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate.* These are the end points in red on the figure; they sum to 0.835, which is rounded to 0.84.
4. *Hybrids* of these – often used by more sophisticated assessment teams.

Direct elicitation often seems to be easier and less time-consuming, but the time to reason through each threat-asset pair can lead to long discussions and thus, it is difficult to maintain logical consistency across a number of such judgments. VLDs have the virtue of being pre-defined and are able to guide discussions and estimates along relevant paths efficiently and consistently. The same can be said for event or failure trees, with the added advantage that a true conditional probability is estimated and the evaluation team is exposed to the uncertainties in their estimates.

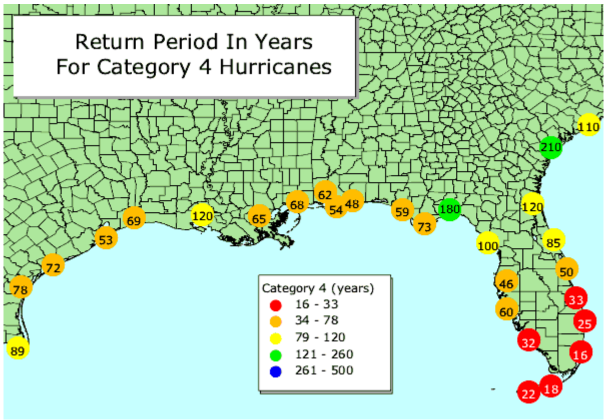
Either of the more structured methods (or the hybrids) produces a more reliable estimate in the sense that a different evaluation team (or the same team at another time) is more likely to make the same or very similar estimates, given the same threat-asset scenarios and the reasoning is documented in detail. This greatly increases the consistency and direct comparability of the assessments and permits them to be used over time to measure progress of security programs or assess evolving conditions.

Task 4.3 Document the approach used, all assumptions, and the results – the conditional probabilities – for each threat-asset pair. It is useful to identify which assumptions are the most uncertain, so they can be subjected to sensitivity analysis later. Usually, these are the ones that involve the most in-depth discussions by the analysis team.

4.5.5 Step 5 – Threat Likelihood Analysis

Threat assessment estimates the likelihood of the initiating adverse event for each threat-asset pair, whether a terrorist attack, dependency/proximity hazard or natural hazard. The threat assessment produces the probability that a particular threat – terrorist, dependency, proximity or natural – will occur in a given timeframe (usually one year).[11] It is a “true” probability (expressed as a specific positive value between 0.0 and 1.0), *not* an ordinal estimate (“very low”, “low”, etc.). Slightly different approaches are used for the respective hazards – malevolent attack, natural hazards, supply chain dependency and proximity hazards. The work of Step 5 consists of six tasks:

Figure 4.7 **Example of Federal Agency Frequency Data (Courtesy of NOAA.gov)**



Task 5.1 Estimate the likelihood of natural hazards. These estimates draw on the historical record for the specific location of the asset. Federal and some state agencies collect and publish records for hurricanes, earthquakes, tornadoes, floods, ice storms and other natural phenomena which can be used, often directly, as the required frequencies for various levels of severity of natural hazards at the facility’s specific location.

Figure 4.7 is an example of the type of natural hazard information available from federal agencies, in this case, the National Oceanographic and Atmospheric Administration (NOAA). It shows the “return period” in years for Category 4 hurricanes, or the average number of years between them. To convert these to the frequencies needed, this number of years is simply divided into 1.0. Thus, in New Orleans, the return period is 65 years, so the frequency is 1/65 or 0.015 or 1.5% likelihood.

---

[11] It may be possible to combine the threats into a comprehensive probability set using Bayes’ theorem. This would require that the events are mutually exclusive, collectively exhaustive, with likelihoods that sum to one. The applicability of Bayes’ theorem to terrorist events is currently being explored. It is not clear that the events can be considered mutually exclusive or collectively exhaustive. The set of reference threats used in RAMCAP are clearly not exhaustive and may not be mutually exclusive. For example, since terrorist attacks may be performed at an opportunistic time to inflict the most damage, the possibility of an attack at the same time as a natural hazard, such as a flood, is a distinct possibility. Research is ongoing to determine if threat probabilities can be combined in the same manner as other probabilistic events, such as games of chance involving inanimate objects, such as cards or dice.

Task 5.2 Estimate the likelihood of malevolent attack. This is universally considered the most difficult task in any risk analysis where terrorism is to be included. It would seem to require information that the user is unlikely to be able to acquire. The worst-reasonable-case assumption provides some guidance for this estimate. The perpetrator is assumed to be a rational person (or organization) who seeks to maximize gains relative to the likelihood of success from among the available alternatives. For each threat-asset pair, this task estimates the likelihood that this pair is selected from among the alternative threats, assets and locations. Estimates of the likelihood of terrorist attacks are based on the terrorists' objectives and capabilities and the attractiveness of the facility relative to alternative targets. Information on terrorists' capabilities and intentions can be informed by intelligence and law enforcement agencies. The asset owner should estimate the relative attractiveness of the target by evaluating alternative target options, considering the terrorists' objectives, the asset's level of vulnerability, the likelihood of success and the cost-effectiveness of the attack.

To the authors' knowledge, no satisfactory method has been proposed to estimate terrorism risks at the level of specific threat-asset pairs or even threat-facility pairs. Some argue that only detailed, current intelligence in the hands of an experienced intelligence analyst can make such estimates, and then, they cannot be widely disseminated for a variety of reasons. This is little help to the regional infrastructure owner or agency. Others have suggested highly sophisticated approaches such as game theory (Cox, 2009; Bier et al., 2009) based on apparent success with "toy problems" made up of hypothetical information – that is virtually never available – and computational facility scaled to the toy dimensions. Taking such methods to full scale would require intelligence information and expertise beyond the assumed users of this methodology possess. As a design issue, RAMCAP seeks a simpler, more practical way. Earlier versions of RAMCAP allowed various "soft" alternatives such as so-called "conditional" risk method, which assumed the threat likelihood to be 1.0, and various ordinal scale substitutes. Neither of these is currently seen as acceptable because the former distorts the decision-making and the latter requires calculations that are mathematically undefined. At present, two alternative approaches are offered to gain insight into the issues and use judgment to approximate threat frequency:

1. *Expert elicitation* – genuinely qualified experts discuss the likelihood of each threat -asset pair based on independent analyses of intelligence information and in-depth understanding of the adversaries' objectives. These discussions can be structured in several ways, but the end result must be a specific quantitative estimate of the probability of the threat-asset pair.
2. *"Proxy" estimate* – a new approach based on the assumed decision process a rational terrorist would use in selecting a facility, an asset and an attack mode – the threat-asset pair of the RAMCAP analysis. This approach draws heavily on work by Risk Management Solutions (RMS, 2008), advisors to the insurance and reinsurance industries on risk issues, the RAND Corporation analysis of global terrorism activity in the seven years following 9/11 (Willis et al., 2007) and on the results of Steps 3 and 4 just discussed.[12]

The proxy estimation process (*Figure 4.8*) seeks to emulate the decision process of rational terrorists as they narrow their choices in selecting target assets and modes of attack (threat-asset pairs):

---

[12] Most risk analysts stipulate that risk is best understood as a function of threat likelihood, vulnerability and consequences because (1) ideally each is treated as uncertainty distributions to be combined and (2) there are expectations of interactions among the three variables. This procedure addresses the latter at least in part, by making threat likelihood a function of vulnerability and consequences. This is consistent with the worst-reasonable-case assumption that they seek to maximize their expected consequences.

1. How *many attacks* to launch on the U.S. this year? The average number of attacks on the United States per year – based on the frequency in the seven years following 9/11.
2. What *metropolitan region* to attack? The likelihood of an attack on the metro region in which the facility is located – based on RMS target type analysis.
3. What *general type of target* to attack? The likelihood to an attack on the general target type of facility being analyzed – based on RMS target type analysis.
4. What *specific type of facility* to attack? The likelihood of the attack being on a facility in the sector being analyzed within the broader target type is proportional to the ratio of the analyzed type of facilities in the target type to all assets in the region *within* the target type (local data).
5. What *specific facility* to attack? The likelihood of the terrorist selecting the specific facility being analyzed is proportional to the ratio of capacity of the facility to total capacity in the metro region (local data).
6. What specific asset and attack mode to use? The likelihood of the terrorist selecting the specific asset–threat pair in question – proportional to the previously estimated product of consequences and vulnerability for the threat-asset pair to the sum of all

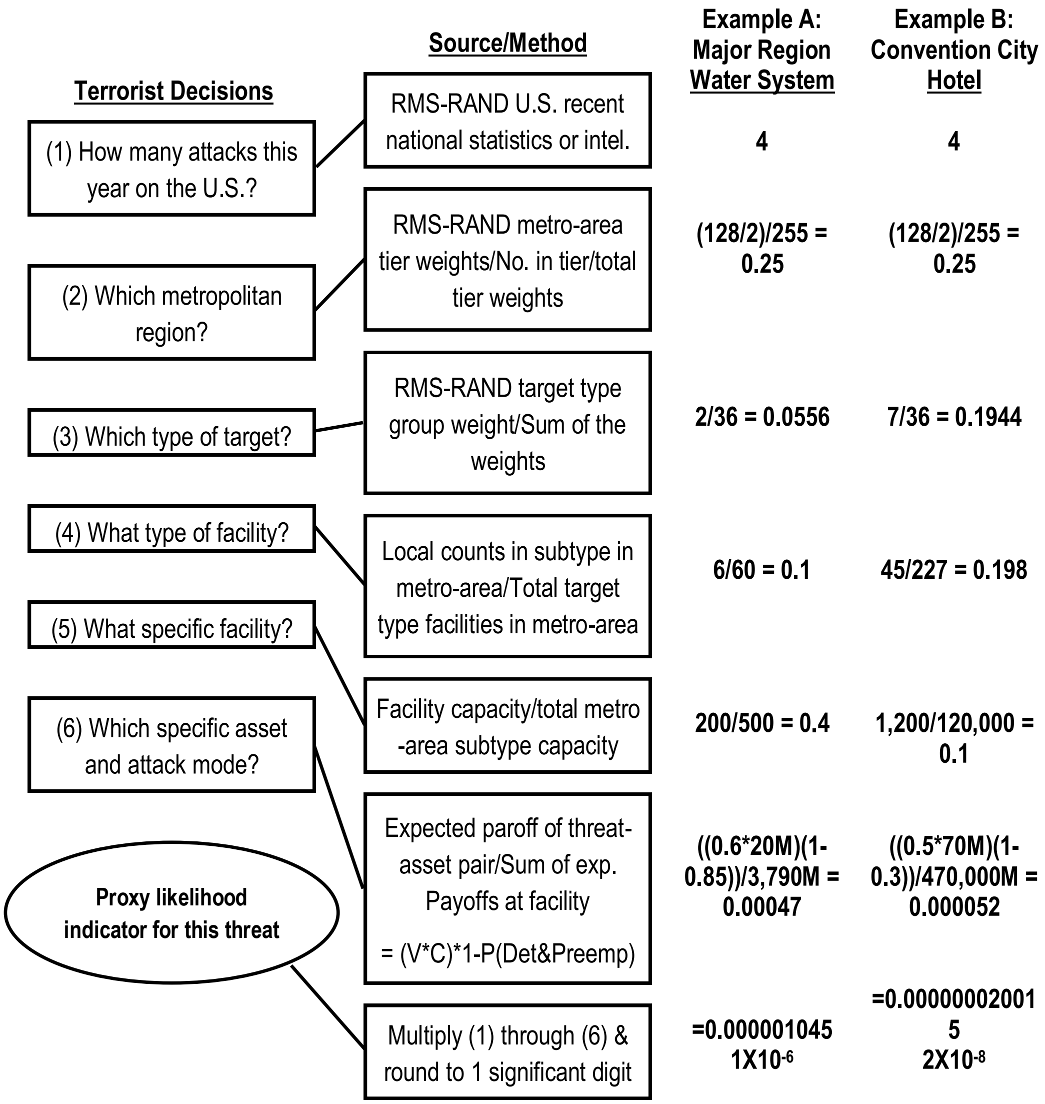


Figure 4.8 **Proxy Estimation Process**

such products at the facility, as adjusted for the probability the attack is detected and preempted before being mounted.

Collectively, these estimates go from the global decision to selecting the threat-asset pair in specificity to provide the likelihood proxy sought. Each of these is conditional on the preceding likelihood, so they can be multiplied together to estimate the overall likelihood of the selection of the facility, asset, and threat of interest. The results are very small numbers – so small that one is tempted to ignore them. They are aggregated, however, to the facility level, in examining the total risk and the basis for considering protective and resilience options. This process is described more fully in Annex 4B.

Task 5.3 Estimate threat likelihood for dependency hazards. Initial estimates of the likelihood of dependency hazards are based upon local historical records for the frequency, severity and duration of service outages. These estimates serve as a baseline estimate of “business as usual,” and may be incrementally increased if, based on the systems and system-of-systems analyses in RR/SAP Phase 3, discussed in the next chapter, the analyst believes they may be higher due to disruptions to the required utilities or supply chain elements. One of the values of using common threat sets in the analysis of all infrastructures, first responders and major economic drivers is that these analyses can examine the effects and likelihood of disruptions to the systems on which the subject systems depends. Confidential conversations with local organizations, utilities and suppliers of critical materials may inform these estimates. As other systems on which the facility depends are included in the analysis, these estimates may be updated to correspond to the suppliers’ estimates of vulnerability and threat likelihood, coordinated in a manner that maintains confidentiality of both systems.

Risk and resilience assessments tell decision-makers where their greatest concerns lie and create the foundation for defining and selecting strategies and tactics to defend against disabling events

Task 5.4 Estimate the threat likelihood of proximity hazards. If the neighboring facility has been assessed using RAMCAP in the overall RR/SAP, the sum of the probabilities of all events that would inflict significant collateral damage on the present facility would be the desired likelihood. If it has not been assessed, the analysis team should conduct its own analysis using the proxy method for the neighboring facility as a whole and all threats that could impose significant harm. The likelihood of incurring damage from an attack on a nearby asset is estimated based on the local situation and using the same logic in estimating terrorist risks (above) to the facility or its hazardous components of the assets to be analyzed. For threats of accidents or damage from natural hazards, analogies from the present analysis, informed by confidential conversations with the nearby facility, will suffice.

Task 5.5 Document all assumptions and input information, intermediate calculations and results clearly.

4.5.6 Step 6 – Risk and Resilience Assessment

Risk and resilience assessments tell decision-makers where their greatest concerns lie and create the foundation for defining and selecting strategies and tactics to defend against disabling events by establishing priorities based on this level of risk. The risk/resilience assessment step is the integration of the estimates made in the previous steps to calculate the major indicators of risk and resilience. It consists of five tasks:

Task 6.1 Estimate the risks for each threat-asset pair. The risk for each threat-asset pair (ta) is calculated from the risk relationship:

$$\mathbf{Risk}_{ta} = \mathbf{Consequences}_{ta} \times \mathbf{Vulnerability}_{ta} \times \mathbf{Threat\ Likelihood}_{ta} = \mathbf{C}_{ta} \times \mathbf{V}_{ta} \times \mathbf{T}_{ta} \qquad \text{Eq. 4.3a}$$

The decomposition of risk into consequences, vulnerability, and threat likelihood is compatible with the classic definition of risk as a measure of the probability and severity of adverse effects (Lowrance, 1987). Consequences are those estimated in Step 3, vulnerability is the conditional probability estimated in Step 4, and threat likelihood is the absolute probability estimated in Step 5. Risk estimates may be calculated for each of the individual key consequences if the decision-makers wish to use them all, thus:

$$\boldsymbol{Risk}_{\boldsymbol{Fatalities,\ ta}} = \boldsymbol{Consequences}_{\boldsymbol{Fatalities,ta}} \times \boldsymbol{V}_{\boldsymbol{ta}} \times \boldsymbol{T}_{\boldsymbol{ta}} \qquad \text{Eq. 4.3b}$$

$$\boldsymbol{Risk}_{\boldsymbol{Injuries,ta}} = \boldsymbol{Consequences}_{\boldsymbol{Injuries}} \times \boldsymbol{V}_{\boldsymbol{ta}} \times \boldsymbol{T}_{\boldsymbol{ta}} \qquad \text{Eq. 4.3c}$$

$$\boldsymbol{Risk}_{\boldsymbol{Owner\ Financia,tal}} = \boldsymbol{Consequences}_{\boldsymbol{Owner\ Financial,ta}} \times \boldsymbol{V}_{\boldsymbol{ta}} \times \boldsymbol{T}_{\boldsymbol{ta}} \qquad \text{Eq. 4.3d}$$

If the decision-makers have defined all of these as decision criteria in RR/SAP Phase 1, they may be used directly as the baseline for analysis of benefits in the Evaluation Cycle.

For the region, they may also be integrated into a single regional risk indicator by placing a monetary value on the fatalities and injuries and adding it to the regional economic loss. There is no exact parallel from the owner's perspective because the liabilities for casualties were included as part of the owner's financial loss.

When a single estimate of regional risk, resilience or benefit of improvements is needed for decision-making (e.g., when allocating budget resources to a large portfolio of improvements), organizations estimate the monetary equivalent of fatalities and serious injuries and add this to the financial or economic losses. For the total metropolitan region's impact, the "value of a statistical life" (VSL) is added to the estimated regional economic impacts. Estimating this value is based on the economic concept of how much society is willing to pay to preserve the life of an unknown or random individual. Details of this calculation continue to be a highly controversial topic of debate among economists and agencies.

Table 4.5 **Injury Severity Factors**

Abbrev. Injury Scale	Severity	Fraction of VSL
1	Minor	0.003
2	Moderate	0.047
3	Serious	0.105
4	Severe	0.266
5	Critical	0.593
6	Unsurvivable	1.000

The Office of Management and Budget (OMB) found that estimates of VSL range from one million to ten million dollars but does not state which to use (OMB, 2003). Recent federal agency estimates include the U.S. Department of Transportation's (DOT) $6.2 million (DOT, 2011), the U.S. Food and Drug Administration's $7.9 million (FDA, 2011) and the U.S. Environmental Protection Agency's $9.1 million (EPA, 2010). EPA recommends that the VSL be updated to the base year of the analysis and be used in all benefits analyses that seek to quantify mortality risk reduction benefits regardless of the age, income, or other population characteristics of the affected population. The user of this process should make a clear statement of the value being used and all analyses in the same set of decisions should use the same value. For example, a default value can be assumed as the average of the above three VSL estimates, or $7.7 million. In addition, sensitivity analysis of this assumption is strongly recommended. If the investments selected in RR/SAP Phase 5 would change significantly with relatively small changes in the assumed VSL, the decision-makers should be made aware of this and alternative solutions should be provided, as well as the original one.

DOT (2009) also supplies an approach to valuing serious injuries, shown in *Table 4.5*. For various severity levels, it provides the proportion of the VSL that should be used. In a RAMCAP analysis, the concern is for serious injuries defined as those requiring hospitalization or causing more than one week's absence from work. We assume these would encompass levels 3-5 and that the less serious would outnumber the more serious in a roughly lognormal distribution, for an assumed overall factor of 0.22 of the VSL, or in the default, $ 1.7 million.

The inclusive loss indicators for the owner using these default values would be:

$$\textit{Inclusive Owner's Loss}_{ta} = \textit{Consequences}_{Owner,\ Financial,ta} + (7.0 \text{ mill.} \times \textit{Fatalities} + (1.7 \text{ mill.} \times \textit{Injuries}) \quad \textit{Eq. 4.4}$$

The loss indicator is then used to calculate the owner's inclusive risk metric:

$$\textit{Risk}_{Owners,Inclusive,ta} = \textit{Inclusive Owner's Loss}_{ta} \times V_{ta} \times T_{ta} \quad \textit{Eq. 4.5}$$

Task 6.2 Calculate total risk to owner. All the forgoing calculations apply to the individual threat-asset pair. *Total* risk across all threat-asset pairs to the owning organization is the aggregation of these risks (using owner's loss, fatalities and injuries, respectively) for all individual threat-asset pairs being analyzed, i.e.:

$$\textit{Total Owner's Economic Risk} = \Sigma \textit{Risk}_{Owner,Economic,\ ta} \quad \textit{Eq. 4.6a}$$

$$\textit{Total Owner's Inclusive Risk} = \Sigma \textit{Risk}_{Owner,Inclusive,\ ta} \quad \textit{Eq. 4.6b}$$

This assumes that the set of scenarios (including "no incident") is mutually exclusive, represents all possible scenarios (i.e., collectively exhaustive), and the estimated probabilities sum to one (essentially assuming the likelihood of the "no incident" scenario is the complement of the sum of all the incident scenarios (i.e., 1.0 minus the sum of the probabilities of all incident scenarios).

The equations just presented understate the respective risks when based only on the losses estimated in RR/SAP Phase 2 because they fail to account for the risks this system poses to other systems and their derivative losses. These systems effects are estimated in RR/SAP Phases 3 through 5.

Useful subtotals can also be calculated in this way. It is meaningful to aggregate all terrorist risks, natural hazard risks, tornado risks, etc., especially when one is considering whether to develop options to manage whole classes of risk in the RR/SAP Evaluation Cycle.

Task 6.3 Estimate owner's and regional resilience for the threat-asset pairs. Resilience is the ability of an organization, facility or asset to function despite and during an attack, natural event or dependency failure or to restore functionality in very short time. The opposite of resilience is brittleness, or the tendency to break down and cease to function during a traumatic event. The central issue in resilience is the outage or service denial, defined either in the natural units provided or dollars:

$$\textit{Service Denial}_{Units,ta} = \textit{Severity}_{ta} \times \textit{Duration of Outage}_{ta} \quad \textit{Eq. 4.7a}$$

Or

$$\textit{Service Denial}_{\$,ta} = \textit{Severity}_{ta} \times \textit{Duration of Outage}_{ta} \times \textit{Average Unit Price} \quad \textit{Eq. 4.7b}$$

Where:

Service Denial – amount of service or products denied due to a disruptive event.
Severity – the number of units denied per day, usually measured from expected or "acceptable" level of demand.
Duration of Outage – the number of days the outage lasts.

Average Unit Price – the average price paid by customers in the affected area before the disruption.

The monetary version of the equation is, of course, the gross revenue loss to the owner, which has been estimated as part of the owner's financial losses. Where the analysis is limited to a single enterprise with one primary product (e.g., a water or power utility), either the units or dollar form can be used depending on which is more meaningful to decision-makers. If the analysis includes enterprises with multiple products or multiple enterprises, the dollar form should be used to allow comparability.
To reflect its uncertain, potential nature similar to risk, the resilience metric is the service outage multiplied by the likelihood of the threat event and the vulnerability of the asset, or, for the owner:

$$\textit{Resilience Indicator}_{Owner,ta} = \textit{Service Denial}_{ta} \times \textit{Vulnerability}_{ta} \times \textit{Threat Likelihood}_{ta} \qquad \text{Eq. 4.8}$$

This quantity is the number of "expected" (i.e., probability weighted) units not provided. For a perfectly resilient threat-asset pair, this index would be zero because there would be no service outage. Either resilience in units or percentages can be used. Reduction in this index directly measures the enhancement of resilience.

Task 6.4 Calculate total resilience indicator for owners and the region. Because the threat-asset pair metrics of resilience are both expected values, they may be totaled and subtotaled just as the risk metrics above, so:

$$\textit{Total Owner's Resilience Indicator} = \Sigma \textit{Resilience}_{\$,Owner,\ threat\text{-}asset} \qquad \text{Eq. 4.9}$$

Task 6.5 Document the risk and resilience estimates for all threat-asset pairs and relevant subtotals and totals. Document any assumptions made during this step.

At this point, the analysis from this Phase 2, the RAMCAP facility/asset analysis of the RR/SAP Assessment Cycle, passes to Phase 3 (analysis of individual distributed systems), Phase 4 (system-of-systems analyses) and Phase 5 (regional economic analysis) as input to their analyses. Phases 3 and 4 "feed back" to Phase 2 with information that can cause revisions to the initial analysis or new analyses altogether.

After the baseline risk and resilience levels have been established in the RR/SAP Assessment Cycle, optional new methods to reduce risk and/or increase resilience are defined for the areas of highest priority to the decision-makers.

Phase 3 receives the estimates of potential service outages of specific assets and traces them through the distributed service delivery model to capture the full impacts on the system being assessed. This may discover additional high-priority threat-asset pairs for analysis in Phase 2. Additional losses (financial or human) as the initial failure causes other parts of the system to fail, adding to loss estimates in Phase 2, or new causes of service denial give rise to additional threat-asset pairs to be analyzed. Conversely, the systems analysis may show that ability to route and re-route service delivery to work around damaged assets reduces the amount of service denial that the more static analysis in Phase 2 suggests. These findings are then analyzed through the Phase 2 RAMCAP assessment and the earlier results are updated or adjusted as needed.

Once the service delivery system impacts have been assessed, the full set of service outage estimates are imposed on *other* systems through the system-of-systems model and the impacts on the other systems are estimated and traced through *their* dependencies until they run their course. For example, a failure in the power system is assessed for its impact on the water service and then on the fire suppression system. These analyses generate additional information on dependency hazards for the *impacted* systems as well as capture the full set of outages and losses (both dollar and human) of all systems together through the full cascade of events.

Some of the outages in other systems may add to losses of the owner if there are delivery contracts that impose penalties for non-delivery. If this is the case, these losses are added to the owner's loss and the Phase 2 results are again updated.

The impacted systems and their customers, however, incur most of these derived losses and outages, without additional loss to the organization being analyzed. That is, they affect the immediate regional losses and service delivery, but not the owner's losses. This is one of the reasons that RAMCAP uses the dual-perspective analysis. These losses are very real and can have devastating impact on the organizations and individuals in the region, but using conventional risk analyses do *not* enter into the decision-making of the organization whose disruption caused them. The losses to the impacted systems are direct consequences of the initial event that often call for cooperative solutions from the respective systems.

4.6 RAMCAP Step 7 – Risk and Resilience Management – The Core of the RR/SAP Evaluation Cycle

Step 7 lies entirely in the RR/SAP Option Evaluation Cycle, so it is discussed in more detail in Chapter Ten. It is the most important step in improving the security, resilience and reliability of the organization or region. Through the intelligent and informed management of risk, the organization can improve its level of resilience, service reliability and security to its customers and the regional community.

This step makes the decisions that actually reduce risk and increase resilience. It supports the decisions to select and commit resources to specific options to enhance overall security. Risk and resilience management is the deliberate course of deciding upon and implementing options (e.g., establishing or improving security countermeasures, improving consequence mitigation tactics, building in redundancy, entering into mutual aid pacts, creating emergency response and continuity plans, and developing training and exercises) to achieve an acceptable level of risk and resilience at an acceptable cost to the organization and the community.

After the baseline risk and resilience levels have been established in the RR/SAP Assessment Cycle, optional new methods to reduce risk and/or increase resilience are defined for the areas of highest priority to the decision-makers. These options are well enough defined to estimate their effects on the terms of risk and resilience – consequences, vulnerabilities, threat likelihood and/or service denial – and their costs of acquisition/implementation and maintenance through their useful lives. The value or benefit of the options is their ability to improve security and resilience – to reduce the risk and resilience indicators. These benefits are estimated by revisiting RAMCAP steps 2, 3 and/or 4 as well as RR/SAP Phases 3 and 4 to re-estimate the (reduced) threat likelihood, vulnerability, consequences and/or service denial and recalculate a new risk and resilience with the option in place. The reduction in risk and the increase in resilience (reduction in the resilience indicators) are the benefits or overall value of the option, which can be compared to the cost of implementing it and the benefits and costs of other options. The options may include countermeasures (directed toward reducing threat likelihood or vulnerability), or consequence-mitigating actions (intended to reduce the economic and public health consequences of an adverse event and hasten a return to full functionality). Taking no action, i.e., accepting the current level of risk, is always a baseline option against which all others are compared.

The major tasks in risk management are:

Task 7.1 Decide what risk and resilience levels are unacceptable by examining the estimated results of the first six steps for each threat-asset pair, considering the risks and resilience to the owner, the regional direct systems' risk/resilience and the overall regional risk/resilience. Provide guidance in the form of a ranked list and any refined evaluation criteria of value.

The decisions made based on RAMCAP information create a prioritized plan to enhance security and resilience integral to the organizations' overall investment and operating plans.

Task 7.2 Define countermeasure, mitigation and/or resilience options for the higher ranked threat-asset pairs that are not acceptable.

Task 7.3 Estimate the investment/acquisition, operating and maintenance costs of each option and calculate their time-discounted present value, including forward cash only.

Task 7.4 Assess each option by analyzing the threat-asset pair or subsystem under the assumption that the option has been implemented – revisiting all affected steps 3 through 6 to re-estimate the risk and resilience levels and calculate the estimated gross benefits of the option (the difference between the risk and resilience levels without the option and those with the option in place).

Task 7.5 Identify the options that have benefits that apply to multiple threat–asset pairs or might be redundant with other options (potentially causing "double-counting" of benefits). Adjust the benefit estimates to account for these situations.

Task 7.6 Calculate the net benefits (gross benefits less costs), net benefit/cost ratio and any other values or ratings needed to fully describe the option relative to the selection criteria (i.e., its value).

Task 7.7 *Review* the options considering their net benefits, benefit/cost ratios and value scores relative to the major indices − fatalities, serious injuries, owner's risk and resilience, total regional systems risk/resilience, total economic risk/resilience and score on the value criteria – and allocate resources to the selected options.

Task 7.8 Implement, monitor and evaluate the performance of the selected options. These are the actions that actually reduce risk, enhance resilience and add value to the community.

Task 7.9 Conduct periodic additional risk analyses to monitor progress and *adapt* to changing conditions.

4.7 Benefits of Using the RAMCAP Process

Many benefits are realized when an organization conducts a RAMCAP assessment. These include enhanced security and resilience, quantification of potential consequences and the benefits of their avoidance, and enhanced public policy. Each of these examples provides the organization and its decision-makers with critical information for the effective allocation of resources and is discussed further below.

4.7.1 Enhanced Security and Resilience

Upon completion of a RAMCAP assessment, the organization will have identified its most significant threats, its most important vulnerabilities and the potential consequences and outages it may face if confronted by an adverse event. The organization will also have developed a prioritized set of options for risk and resilience enhancements to component parts and to the organization overall. The result can be a significant improvement in the security of the system to prevent or repel an attack and manage natural events, as well as an increase in the system's resilience to continue operations and recover and restore full service to its customers rapidly afterwards.

4.7.2 Improved Decision-Making from Quantification of Potential Fatalities, Injuries and Losses

While many security or resilience improvements may require significant capital as well as operating and maintenance expenditures, substantial improvement can often be achieved through minimal investment. Unlike some other investments, an identifiable revenue stream does not immediately offset many security and resilience investments. Therefore, it can be difficult for an organization to place security investments in their proper perspective along with its other investment and operating demands. A significant output of a RAMCAP assessment is the quantification of possible negative consequences should the investment not be made in risk reduction or resilience enhancement, and the benefits of reduction in these consequences if they are made. This analysis includes complete and directly comparable estimates of gross and net benefits and costs and benefit/cost ratios (or other metric of marginal value per dollar of investment) that are directly comparable to other options. This information is necessary and sufficient for rational allocation of resources.

RAMCAP is able to contribute to more rational security and resilience investment selection because it:

- Maintains consistency and comparability of results within and across sectors of the economy and between public and private assets;
- Provides continuity through changing circumstances;
- Provides an accepted standard to be referenced by insurance agencies, credit agencies, major customers, etc., to specify and reward preparedness;
- Institutionalizes the consensus process of all relevant stakeholders, including, but not driven by, the federal government;
- Uses existing mechanisms for implementation – most decision-makers in industry and the public sector understand codes and standards;
- Supports effectiveness of the process through publications, training, certification, accreditation, conformance assurance, evaluation of effectiveness, regular updates, etc.; and
- Provides for continuous improvement – *while* maintaining consistency and comparability.

The decisions made based on RAMCAP information create a prioritized plan to enhance security and resilience integral to the organizations' overall investment and operating plans. The ability to provide credible benefit and benefit/cost ratios or similar metrics allows security and resilience concerns to enter the boardroom or council chambers to compete with other investments in a standard budget process. Over time, security and resilience considerations will take their place with health and safety, environmental protection, equal opportunity and even strategic profitability as investment criteria. To the extent that insurance companies, financial rating organizations, lenders and investors begin to place value on security and resilience (business continuity) concerns, these trends will accelerate.

4.7.3 Enhanced public policy

No organization can know all of the pertinent details of any *other* organization's relevant risk and resilience posture. Likewise, few organizations other than government agencies are in a position to understand the intentions and capabilities of a terrorist adversary and only the most sophisticated adequately plan for natural events or dependency hazards, even with historical statistics. The consistent terminology and process of RAMCAP provides the common language for organizations and government agencies to have a meaningful dialogue. By working together and sharing appropriate knowledge, the participants have an ability to achieve their goals. The common language used by a RAMCAP analysis, based on carefully defined and agreed-upon terminology, specific and focused threats and structured consequence metrics, provides the basis for an organization to compare itself with others similarly situated.

From a more aggregate perspective, the comparable results of the RAMCAP process permit rational resource allocation across all sectors – for the facility manager, the business or municipal agency executive with multiple facilities, the mayor or regional public-private partnership with municipal and metropolitan risks

Annex 4A

Process for Identifying Dependencies and Interdependencies and Estimating Mediated Impacts

The Challenge

A geographic information system (GIS) is often used to map spatial distributed systems and to "geo-tag" information with reference to geographic location. Geo-coding provides the basis for the organization of a wide variety of information by reference to spatial coordinates. Infrastructure systems as spatially-distributed network systems are ideally suited for the application of GIS descriptive and analytical tools. Most municipalities and metropolitan areas in the United States now have established a structure of GIS resources. Smaller jurisdictions may contract out for these services. Municipal GIS resources, however, typically focus on the major critical infrastructure systems including:

- Energy: electric power transmission and distribution systems;
- Water/Wastewater: reservoir, storage, treatment and distribution system and sewer collector and treatment facilities;
- Transportation: roads and highways, bridges and tunnels, rail, marine and air transport facilities; and
- Communications: emergency communications facilities, telephone central offices, broadcast facilities, microwave and cable facilities.

In many cases public access to these GIS maps for critical infrastructure systems is restricted for proprietary or security reasons. The restriction of access to system information can be attributed to the following:

- Electric power systems – a general policy by investor-owned utilities is to restrict public access to system plans and mapping of distribution lines. Some municipal systems are, on occasion, more willing to share specific information on system design.
- Water systems – the EPA, soon after 9/11, required detailed vulnerability assessments for all U.S. water systems of any material size and severely restricted access to the assessment. EPA also requested that water system managers restrict access to system plans for water systems.
- Road systems – because they are clearly visible, they are generally available to those studying system vulnerability and dependency.
- Communications systems – typically owned by private investors, communication systems are particularly reluctant to share system information because information on system deployment is considered to be highly proprietary and a key element of competitive position.

Access to electric power and water system maps may only be available on site at the offices of the system operator or in the presence of the system operator's staff. Access to communications systems GIS may not be available under any circumstances.

Approach to Solution

In light of these difficulties and the strong motivation to implement improvement measures as soon as possible, an alternative approach has been developed and piloted on an experimental basis. The objective of the alternative approach is to identify the specific assets that are critical to the operations of *other* infrastructures. These are the major points of dependency or interdependency in the region. The approach is to convene local systems experts – managers, engineers, planners and/or operating personnel to address key *pairs* of infrastructure systems. They are asked to discuss which of the "supplier" system's assets support which of the "receiver" system's critical nodes. The process requires each system's local expert team to access their own GIS system map without disclosing this information to either the other system's team or the facilitating analysts.

This simplification makes possible the visual evaluation of mapped intersections, co-locations and functional dependencies, while stimulating focused consultation and discussion between two infrastructure teams at a time in a mutually beneficial manner. The analysis team works directly with the two teams to capture the key dependencies between the systems for use in constructing the system-of-systems model in Phase 4.

The first step in the process of identifying system interactions and interdependencies is to identify system pairs of elevated interest. In general, the heavy dependency on electric power of most modern infrastructure systems suggests proceeding in the following order:

Dependency pairs based on electric power:

1. Electric Power/ Emergency Services
2. Electric Power/Communications
3. Electric Power/Water
4. Electric Power/ Energy Systems

Dependency pairs based on communications:

1. Communications/Emergency Services
2. Communications/SCADA

Dependency pairs based on transportation:

1. Transportation/Emergency Services
2. Transportation/Fuel Distribution
3. Transportation/Evacuation

Dependency pairs based on water:

1. Water/Fire Suppression
2. Water/Cooling and Industrial Processes
3. Water/Sanitation

The pair of GIS system maps are superimposed (literally or figuratively) to clearly indicate the geographic disposition of the two systems under consideration and the location of their key facilities or assets. The overlay of the system maps provides immediate indication of where the systems intersect in space and where they are collocated. Proximity may also indicate functional dependency, e.g., the nearest substation most likely provides the pumping station with power. These functional relationships are discussed, especially around the issue of back-up systems should the primary supplier asset be compromised and under what conditions the supplier is unable to meet the requirements of the receiver asset.

Actual Process as Used in Metro City

Personnel. In the Metro City prototype application of the participatory dependency assessment methodology three principal groups were involved:

1. Electric power utility operations and planning personnel;
2. Water utility operations and planning personnel; and
3. Facilitating resiliency assessment team.

Background materials prepared for the "bilateral dependency assessment" session included the following large scale maps:

1. System map for the electric power system, including transmission lines, substations, and distribution system;
2. System maps for the water system, including water source point, water treatment plants, and water distribution and storage system; and
3. Overlay of electric power and water system maps.

Participatory process

1. The process is initiated by the resilience assessment team with the requested identification of recognized points of dependency of the water system on electric power. This information was

simultaneously recorded on the overlay system map and the detailed context and conditions of the dependency were documented in writing with associated quantitative data.

2. Each of the dependency points is ranked in terms of importance to the functioning of the water system – in terms of potential service interruption – and evaluated in regards to potential consequences of decreased water supply in the relevant service area. This estimate is based on knowledge of specific "down-stream" customers and functions.
3. Each identified dependency point of the water system is then examined by the electric power team to determine which of its assets services each water system node and available back-ups, as well as determine the vulnerability to interruption of electric power service to the water system element.
4. The electric power team then traces the source of electric power to the point of delivery to the water system to identify points of potential service interruption. This "up-stream" vulnerability investigation is documented as the potential path of cascading failure within the electric power system that would influence the functioning of the initial asset in the water system. Power system assets that support the water system's critical nodes are conditionally defined as critical power system assets and treated in the power system's analysis.
5. The process is repeated until each pair of infrastructure systems has been completed.

Major outputs of the process:

1. First cut identification and prioritization of key points of intersystem dependency;
2. Initial recognition of up-stream and down-stream vulnerabilities;
3. Initial prioritization of points of potential resilience investment;
4. Establishment of common reference and basis for mutually acceptable solutions for relevant system operators; and
5. Initial prioritized list of multi-system interface conditions that require more detailed analysis.

Communications between the respective systems among planning, engineering and operating personnel are established, often for the first time. The perception of shared interests and common issues allows more in-depth exchanges of information – and actual mutual assistance in crises – over time.

Discussion

Discussion of intersystem dependencies based on GIS system map overlays and moderated by the regional resilience reference team provides the opportunity for common identification and prioritization of issues relevant to both respective systems and for direct confrontation of these issues in implementing a collaborative resolution. In many cases where emergency curtailment of service is necessary for system survival, operators lack adequate knowledge of the consequences of such curtailments outside of their own system. Downstream consequences are not systematically documented or taken in to account in emergency situations or in system planning. Key customers with large demand and special customer service representation may be offered preferential treatment, but this does not extend to vulnerable populations or to the extended consequences of intersystem disruptions.

In the case of the bilateral consideration of the electric power and water systems, there are several examples of the GIS overlay approach. First, in the relationship of power to critical facilities, it is possible for the water system to assess the vulnerability and reliability of the sources of electric power for treatment plants. The option of dual feeds from independently-sourced substations is often available at a premium rate. On-site, back-up generation may also be considered for particularly critical functions. This type of analysis has led to the purchase of on-site generating capacity at a number of water treatment plants in areas subject to hurricane disruption of electric power.

Beyond the key assets of the water system, the GIS overlay allows for the investigation of consequences of power outages on the water distribution system. Specific feeds from specific substations to specific water distribution pumps can be identified. The consequences of pump failure at that point can be assessed from the perspective of the water system. This can include impacts on fire suppression, critical facility cooling, manufacturing and public health. All of these factors are relevant in evaluating the appropriate level of investment in the reliability of the power source to any pump in the water system.

Benefits of the Approach

1. Confidential system data does not leave the control of the system owner/operator, but critical dependencies are defined in terms of specific assets and back-ups.
2. Operator knowledge and experience of the system are fully incorporated in the analysis. This is important because the complexities of system interaction are critical to the overall system-of-systems performance and are not generalized from one case to another.
3. The direct interaction of the assessment team with the manager/operator teams allows for the application of expert knowledge of intersystem dependencies and regional resilience issues in the context of specific local system knowledge and experience. This interactive approach provides a valuable synthesis of general knowledge of failure patterns with specific local experience.
4. In the course of this interaction, with reference to the specifics of the local systems, the recommendations of the assessment team can be weighed against the constraints of the available resource base and trade-offs offered by the specific local conditions.
5. This process ends with an output that is based on accurate understanding of specific local conditions, concerns and capabilities. At the same time, the necessary implementers of the results of the analysis are satisfied that they have had a critical role in the process and accept the rationale for proposed actions.

Annex 4B

Proxy Indicator of Terrorism Threat

Note: This material is adapted from work originally developed for use by ANSI/ASME-ITI/AWWA J100-10 (2010).

The Difficulty in Estimating Terrorism Threat Likelihood

Risk, as defined in the RR/SAP (and many other sources, including the National Infrastructure Protection Plan, 2006 and 2009), requires estimation of threat likelihood. For most major natural hazards, likelihood can be estimated from the location-specific historical frequencies (perhaps extended with empirical trends). Estimating terrorism threat likelihood, however, is more complicated because of the lack of a solid historical statistical base – and more important – the knowledge that terrorists are rational decision-makers, fully capable of developing strategies that counter historical trends. For these reasons, terrorism threat likelihood is generally acknowledged to be the most difficult task in terrorism risk analysis – the estimation of the likelihood of a terrorist attack on a *specific* facility and *specific* asset within that facility, using a *specific* attack mode or scenario.

Some argue that only in-depth intelligence information of the specific plans of the adversary can enable useful estimates of likelihood. This information, however, cannot be released publicly for a variety of security reasons.

Others argue that terrorism likelihood can be estimated, but that an intelligent, adaptive, and knowledgeable adversary an confound any straightforward estimation, so more sophisticated methods are required, such as game theory (Cox 2009, Bier et al. 2009). Such approaches, however, require restricted, in-depth intelligence information and sophisticated risk and probability expertise, which is scarce in the user community for RR/SAP.

In light of this, some have suggested using simplified alternatives. One is the use of "conditional risk," i.e., the product of vulnerability and consequences, *assuming* that the attack occurs (i.e., assuming the Threat Likelihood is 1.0, certainty). A variation on the conditional risk approach, recommended by some in the water sector, is using the "tiers" used in ranking water systems by the U.S. Department of Homeland Security be used as a proxy, with Tier 1 having a likelihood of 1.0, Tier 2 of 0.75, Tier 3 of 0.50, and Tier 4 of 0.25. These approaches suffer from the same limitations. For instance:

- If risk analysis is to contribute to decision-making, the practice of using the same likelihood for all threat-asset pairs distorts the magnitude of the true risk and the benefits of risk-reduction measures, so distorts decision-making. The problem is that the conditional and tier-based risks mask the fact that threat likelihood can vary by several orders of magnitude – substantially more than can generally be appreciated at an intuitive level.
- No one would argue that all utilities, or even just Tier 1 systems, *will* be attacked with certainty every year; nor would anyone suggest they make decisions that assume this – but certainty is, of course, the definition of a likelihood of 1.0.
- Natural hazards, for most of which we have historical frequency data, should generally be considered in the same analyses as terrorist threats. If the "conditional" or "tiered" threat assumes certainty, it will make natural hazards appear *less* likely than terrorist attacks – to which no one would agree.
- Conditional and tier-based approaches fail to differentiate among threat–asset pairs, assigning the *same* likelihood of attack to

all threat-asset pairs in the facility. But this seriously distorts the estimates given to the decision-makers. The reference threats differ greatly in the cost and are difficult to mount with a strong likelihood to be detected and preempted before being launched. Just as with conditional risk, using these approaches distorts the apparent relative magnitude of the risk because it would assign highest risk systematically to the threat-asset pairs with the greatest consequences – which are very often the *least likely* due to cost and most readily detected and interdicted.

- If the magnitude of terrorism likelihood is not indicated in the analysis, the decision-maker, who knows intuitively that a terrorist attack on utilities is improbable, will regard the results of a risk analysis as irrelevant at best and ridiculous at worst. The risk analysis will simply become an empty "paper exercise," conducted only when mandated, completely disconnected from real decision-making.

Thus, using conditional risk and the "tier" system and similar approaches result in vast overstatement of the risks, significant distortions of the relative likelihood of specific threat-asset pairs and can distort decision-making.

A "Proxy" Threat Likelihood Indicator

If a true and precise estimate of terrorism likelihood is too difficult to provide in this context, the need is not for gross assumptions that could distort decisions or reduce risk analysis to a paper exercise, but for an alternative approximation that can be used with minimal decision distortion.

The present approach stipulates that estimation of true terrorism threat likelihood is extraordinarily difficult and that estimation of the correct quantity *with precision* is beyond the resources of the risk analysis process as applied in most real-world municipal and corporate settings. The approach does not, however, accept that nothing useful can be done. On the contrary, this approach suggests that it is possible within reasonable informational and expertise resources to develop a *proxy* threat likelihood – an approximation that logically corresponds to the actual threat likelihood (in order-of-magnitude sense and correlation with accepted notions of terrorist behavior) and differentiates among threat-asset pairs in ways that also correspond with differences in terrorism likelihood. That is, we accept that true terrorism threat likelihood estimation is beyond the scope of most risk analysis, but that estimating a proxy indicator useful in decisions is not. If the proxy indicator overcomes the obvious shortcomings of the alternatives so far proposed, it can be used as though it were a true likelihood while recognizing its limitations.

The approach conceives the problem as the adversary choosing a target facility, a specific target asset within the facility, and the specific mode of attack. In making these decisions, some elements of the decision are based on the location and properties of the facility, some based on the nature of the specific attack mode and some in the characteristics of the threat-asset pair being considered. All the information needed to complete the method has been estimated in previous RAMCAP steps, is provided by this annex, or can be readily accumulated by the utility.

Recent studies by Risk Management Solutions, Inc. (RMS, 2008), a leading risk analysis consulting firm to the insurance and reinsurance industries, and the RAND Corporation (RAND, 2007), based on an assessment of global terrorism activity in the seven years after September 2001, provide a solid basis for starting the approach. This information can be combined with local data, information in this appendix, and estimates calculated earlier in the Standard RAMCAP process can be interpreted as the basis for estimating:

1. The number of attacks on the United States per year – based on the frequency in the seven years following 9/11, as interpreted by RMS.

2. The likelihood of an attack on the metro area in which the facility is located – based on RMS metro area classes.
3. The likelihood of an attack on the general target type of facility being analyzed – based on RMS target type analysis.
4. The likelihood of the attack being on a given type of facility within the broader target type – based on the ratio of the present facility type in the target type to all assets in the region within the target type (local data).
5. The likelihood of the terrorist selecting the specific facility of interest – based on the ratio of capacity of the facility to total capacity in the metro area (local data).
6. The likelihood of the terrorist selecting the specific threat-asset pair in question – based on the previously estimated consequences and vulnerability for the threat-asset pair and the characteristics of the threat – specifically the probability the attack is detected and preempted before being mounted (provided in this annex).

Collectively, these estimates go from the global to the threat-asset pair in specificity to provide the likelihood proxy sought. Each of these is conditional on the preceding likelihood, so they can be multiplied together to estimate the overall likelihood of the selection of the facility, asset, and threat of interest.

Steps for Estimating the Likelihood Proxy

The approach can be visualized as a sequential series of the six decisions a terrorist would need to make to choose a specific attack on a specific asset in a particular facility. *Figure 4.8* illustrates the decision sequence and contains two examples of its use to calculate terrorism threat likelihood. The sequence a terrorist would use is to choose the specific facility (nodes 1–5) and then the specific threat-asset pair from among the following alternatives:

Decision 1. **Choose the Number U.S. Attacks –** *Estimate the number of attacks in the United States.* In the seven years after 9/11, 30 plots to attack the United States were discovered, although none was successful (RMS, 2008) or slightly more than four per year on average, ranging from three to seven in a single year. If intelligence information is available, it should be used, but if none is available, assume default of four per year. The probability of detection and preemption is included below.

Decision 2. **Choose the Metro Region to Attack** – *Estimate the likelihood of an attack on this specific metro area.*[13] RMS (2008) found a strong tendency to focus on the “premier city” of each country attacked and that 12 of 22 plots on the United States with known cities targeted New York City or Washington, D.C., and seven more in Los Angeles, Chicago, Miami, and Las Vegas. These rankings were based on the expert judgment of a panel of terrorism risk experts and are used by the insurance and reinsurance industries. Numerous attributes of the metro areas contribute to attractiveness as a target. Population, however, is a major attribute along with symbolic or iconic stature. RAND (2007) cites slightly earlier but more detailed RMS data that define “tiers” of metro areas based on relative likelihood of attack, where the relative rank of each next lower tier is one-half the next higher, as shown in *Figure 4B.1.*

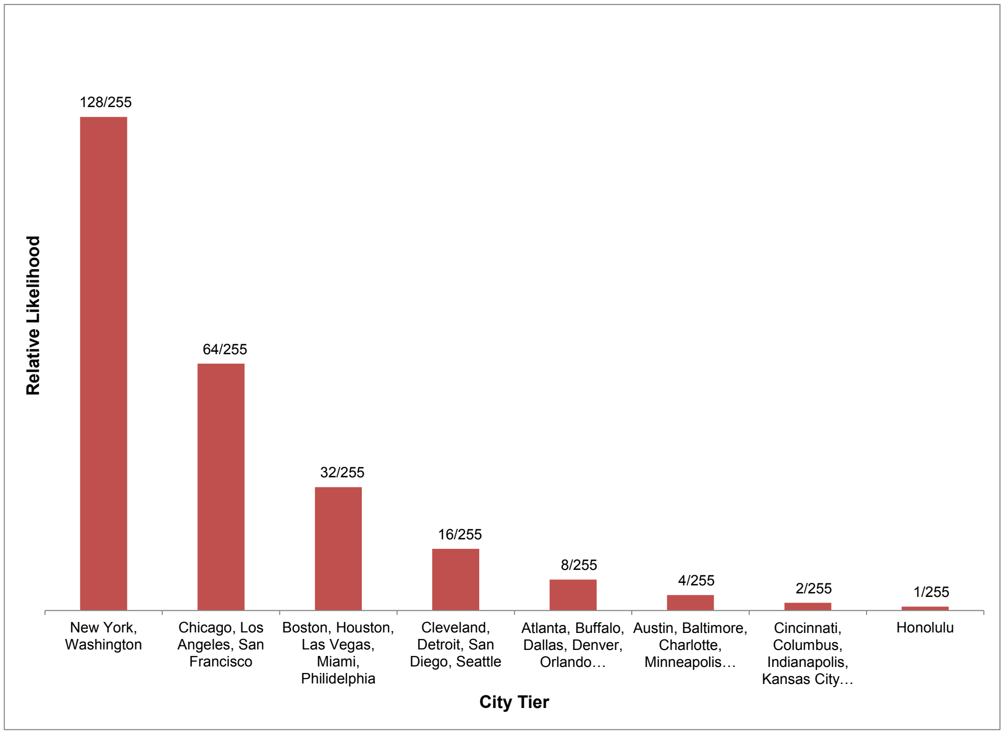
Using this scale, one can estimate the relative likelihood of each tier as the ratio of the height of the tier bar to the sum of their heights, assuming the smallest is one, as illustrated. The sum of the ranks is 255. To estimate the risk of attack in a particular metro area, take the ratio for its tier and divide that by the number of cities in the tier, e.g., for Las Vegas, use 32/5/255 = 0.025.

For metro areas that do not appear in the figure, compare population with those enumerated and select the most similar tier. Then, use the

---

[13] For smaller cities and towns, the U.S. Census has coined the phrase “micropolitan areas” as the complement to metropolitan areas in defining all urban areas. These are implied when “metropolitan areas” are mentioned in the text

Figure 4B.1 **Relative Likelihood of Terrorist Attack in Different City Tiers**
Source: (RAND, 2007)



following numbers as the denominator in the above calculation e.g., for Tier 5, use 8; Tier 6, 8; Tier 7, 12; Tier 8 and all others, 50. These are roughly interpreted by the author based on population as judged from the U.S. Census Bureau. Population is used because it is one of the largest elements of attractiveness to terrorists in the experts' views and the one with the most uniformly available data. If users believe that their area has special attraction (e.g., iconic value), they may raise the category (and the denominator) by one.

Decision 3. **Choose Which Target Type** – *Estimate the likelihood of this target type being chosen.* The RAND study ranks "target types" of facilities using ordinal numbers or ranks (RAND, 2007), which might be converted to ratio numbers by making simple assumptions, as illustrated in *Table 4B.1*

Table 4B.1 **RMS Target Type Groups**
Source: (RAND 2006)

Target	Type Group	Target Types in Group
1	8/36	Government buildings
2	7/36	Business districts, skyscrapers, stock exchanges, hotels and casinos, airports, nuclear power plants
3	6/36	Military, train and subway stations, stadiums, bridges and tunnels
4	5/36	Industrial facilities, oil and gas processing facilities, tourist attractions, shopping malls, restaurants, ports and ship
5	4/36	Media HQ, Fortune 100 HQ, theaters, major entertainment center, gas stations
6	3/36	Cruise ships, apartment buildings, foerign consulates, United Nations
7	2/36	Water reserviors and distribution, passenger trains, airspace zones
8	1/36	Power plants, dams, railway networks
	Sum = 36	

A very simple approach to convert ranks (ordinal scales) to ratio numbers is to assume the intervals between ranks are equal across the range illustrated and that there is a "zero" rank, indicating no value to the terrorist decision-maker. This permits the simple assumption that the likelihood of each type is proportional to the ratio of its rank to the total ranks. To preserve the table's ranking while using it this way requires the ranks be reversed so the higher the rank, the larger, not smaller, the number: top-ranked number 1 becomes top-ranked 8, second-ranked number 2 becomes second-ranked 7, and so forth to lowest-ranked number 8 becoming the lowest 1. The sum of these ranks is 36, so all the ratios are the new (reversed) rank number divided by 36, as shown in the table.

A refinement by the J100 ASME-ITI/AWWA Water Standard RAMCAP Committee was to agree that water and wastewater treatment plants should be treated as most similar to "industrial facilities" in Class 4, whereas reservoirs and distribution systems should be treated as shown in the table.

***Decision 4.* Choose Which Facility Type** – *Estimate the likelihood of this facility type being chosen from the target type.* The likelihood of this facility type being selected from the target type is assumed to be proportional to the number of such facilities in the region to the total number of facilities in the target type. Estimate the number of this type facility of in the region (e.g., water reservoirs) in the region and the number of all facilities in the target type of all kinds in the region (e.g., water reservoirs, passenger trains at any given time, and airspace zones). For example, if there were six major stadiums in a metro area that contained 60 Class 3 facilities, the likelihood of selection would be 6/60, or 0.10.

***Decision 5.* Choose Which Specific Facility** – *Estimate the likelihood of this facility being selected from among all members of its subclass in the region.* The likelihood is assumed to be proportional to the facility's capacity as a proportion of the total region's capacity. Estimate the ratio of the capacity of the facility in question to the total capacity in the region. For example, if a stadium had 22% of the region's total stadium capacity, use 0.22 as the likelihood.

***Decision 6.* Choose Which Threat –Asset Pair** – *Estimate the likelihood of this threat-asset pair being chosen from among all threat-asset pairs at this facility.* Assuming the terrorist is a rational decision-maker, he will employ some sort of an expected benefit approach in selecting specific assets and specific attack modes. Assuming also that the terrorist has the same knowledge as the risk analysis team about the facility's configuration and operations (consistent with the worst-reasonable-case assumption), he will estimate the *expected benefit* of each specific attack on each specific asset (threat-asset pair) as the previously estimated product of:

- Vulnerability – the likelihood of success, given the specific attack is mounted (which he is choosing); and
- Consequences – the human and financial/ economic losses that result from a successful attack.

This is the same conditional risk criticized above, but it is used differently in the present approach. It is the core element of expected *benefit to the terrorist* of an attack on this specific asset, using that specific attack mode.

It is, however, incomplete as an expected benefit to the terrorist because *pre-attack terrorist success likelihood* – the vulnerability term – is the estimated likelihood of success, *given* that the attack is mounted and *from the point in time* when it is mounted. The likelihood of detection and preemption *before* the attack must be accounted for as well.

The likelihood of a specific threat-asset pair being selected, *given* that the subject facility is selected, is assumed to be proportional to that threat-asset pair's expected benefit to the total expected benefit of all the threat-asset pairs. This can be estimated by the ratio of the expected benefits of this specific threat-asset to the sum of the expected benefits of all the threat-asset pairs:

$$
\begin{gathered}
\mathit{Pr(selection)}_{\mathit{asset\text{-}threat}} = \\
((V_{\mathit{asset\text{-}threat}} \times C_{\mathit{asset\text{-}threat}}) \times \\
(1 - \mathit{Pr(det\ \&\ preempt)})_{\mathit{threat}}) \div \\
(\Sigma_{\mathit{All\text{-}asset\text{-}threat\text{-}pairs}}(V_{\mathit{asset\text{-}threat}} \times C_{\mathit{asset\text{-}threat}}) \times \\
(1 - \mathit{Pr(det\ \&\ preempt)})_{\mathit{threat}})
\end{gathered}
\qquad \textit{Eq. 4B.1}
$$

Where:

$\mathbf{Pr}(\mathit{selection})_{\mathit{threat\text{-}asset}}$ = Likelihood proxy for the specific threat-asset pair.

$V_{\mathit{threat\text{-}asset}}$ = Vulnerability of the specific threat-asset pair, previously estimated.

$C_{\mathit{threat\text{-}asset}}$ = Consequences of the specific threat-asset pair, previously estimated, expressed as a singular, monetary number including all consequences.

$\mathbf{Pr}(\mathit{det\&preempt})_{\mathit{threat}}$ = Probability of detection and preemption of the specific threat, drawn for *Table 4B.2*.

The product $((V_{\mathit{threat\text{-}asset}} \times C_{\mathit{threat\text{-}asset}}) \times (1 - \mathrm{Pr}(\mathit{det\&preempt})_{\mathit{threat}})$ is the expected value of the benefit to the terrorist. The probability of the selection of any specific threat-asset pair is assumed to be the ratio of its expected benefit to the sum of all the expected benefits for all threat-asset pairs. The vulnerability and consequences were estimated in previous steps, so only the probability of detection and preemption of the attack must be estimated.

$\mathrm{Pr}(\mathit{det\&peempt})_{\mathit{threat}}$ is a property of the specific threat, regardless of the asset to be attacked. The risk analysis in this standard is based on a set of reference threats (scenarios) for which a panel of intelligence experts could make reasonable judgments of these variables. *Table 4B.2* shows the reference threats in summary description and a set of *illustrative example estimates* of the likelihood of detection and preemption before mounting the specific attack.

The success of the authorities in preempting 30 attacks on American soil (RMS, 2008) suggests that the likelihood of detection and preemption is relatively high but varies inversely with the number of participants (the amount of communications needed for coordination increases more than linearly with the number of participants) and the difficulty in acquiring the vehicles (high-jacking an 18-wheeler will attract more attention than renting a car), and magnitude of explosives (purchasing large quantities is more likely to attract attention than smaller quantities).

Table 4B.2 **Detection Likelihood and Cost for Each Threat**
(Entries below the hazard titles are likelihood of detection and preemption before the attack is initiated)
Note: Natural Hazards are not applicable

Hazard Type	Hazard Description with Detection and Preemption Likelihood			
Product Contamination	C(C)Chemical 0.85	C(R) Radionuclide 0.95	C(B) Biotoxin 0.95	C(P) Pathogen 0.85
	C(W) Weaponization of waste disposal system 0.8			
Sabatoge	S(PI) Physical-insider 0.75	S(PU) Physical-outsider 0.8	S(CI) Cyber-insider 0.5	S(CU) Cyber-outsider 0.90
Theft or Diversion	T(PI) Physical-insider 0.75	T(PU)Physical-outsider 0.9	T(CI) Cyber-insider 0.5	T(CU) Cyber-outsider 0.9
Attack: Marine	(M1) Small boat 0.8	(M2) Fast boat 0.9	(M3) Barge 0.95	(M4) Ocean ship 0.99
Attack: Aircraft	(A1) Helicopter 0.75	(A2) Small plane 0.8	(A3) Regional jet 0.9	(A4) Long-flight jet 0.95
Attack: Automotive	(V1) Car 0.65	(V2) Van 0.75	(V3) Mid-size truck 0.8	(V4) 18-wheeler 0.9
Attack: Assault Team	(AT1) 1 assailant 0.5	(AT2) 2-4 assailants 0.65	(AT3) 5-8 assailants 0.85	(AT4) 9-16 assailants 0.95

***Decision 7.* Calculate Proxy Terrorist Threat Likelihood *– Determine the value of proxy threat likelihood* –** Because each of the above elements (except the first, the number of attacks in the United States) is conditional on the preceding element(s), their joint probability is their product, as exemplified in *Figure 4.8*. Because this is a very rough proxy for the more preferable "threat likelihood," it is important to avoid an appearance of precision. For this reason, the proxy likelihood is rounded off to one significant digit, as shown in *Figure 4.8*.

Discussion

RAND's approach may be used to estimate a proxy terrorism risk in RAMCAP Step 5 to estimate both risk and resilience at the threat-asset pair level in the initial pass through the RAMCAP process. As shown in the example, it yields a very small number, as would be expected on a specific threat-asst pair on a specific facility in a specific facility type and target type in a specific metropolitan region. These small numbers are aggregated as the risks of a facility are added together, but even then are a small number. Terrorism remains a threat to U.S. infrastructure, but its likelihood is still very much smaller than the likelihood of natural or non-terrorist human threats. The proxy estimate reflects this.

The proxy can also be used in Step 7 in estimating the benefits of risk-reduction and resilience-enhancement options. Most of these options operate on the consequences or vulnerabilities, but improving either of these also makes the threat-asset pair less attractive to terrorists. The proxy captures that effect. As security or resilience options reduce consequences and/or vulnerabilities, these automatically reduce the threat likelihood proxy because the (C × V) term is used in both the numerator and denominator of the estimate for the threat-asset pair. This seems an appropriate way to capture this interaction among the three variables.

In a sense, this proxy method crudely approximates the much more complex game theory approach. It approximates a two-player, four-step game:

1. The defender assesses the consequences and vulnerability of the initial condition for each threat-asset pair (RAMCAP Steps 3 and 4); then
2. In estimating threat likelihood, the attacker's choice of facility, asset, and threat is modeled, expressed as a probability (RAMCAP Step 5); followed by
3. The defender's decision to protect certain assets against specific threats by changing the consequences or vulnerability (RAMCAP Step 7, in updating Steps 3 and 4 when re-estimating consequences and vulnerability with changed conditions due to the defender's program); and finally
4. The attacker's revised choices, based on the more protected situation, are modeled in the revised threat likelihood term (RAMCAP Step 7 when re-estimating Step 5 for the changed conditions).

As in game theory, this proxy for threat likelihood is an output of the analysis, not an autonomous input to it. Of course, neither player is optimizing and the game could continue through more steps, but with the large number of threat-asset pairs using limited computing capability, the RAMCAP process stops before the defender's third-round decisions.

The proxy measure is *not*, of course, the true threat likelihood, but a number believed to roughly approximate true likelihood. It recognizes major differences in order of magnitude among threats and differentiates facilities and threat-asset pairs within facilities enough to avoid major decision errors, while maintaining consistency and comparability by constraining users to a limited number of options. The proxy measure is built on a collection of assumptions about the objectives, decision processes, and information available to terrorists, any of which could be in error. Reasonable sensitivity analyses could explore alternative assumptions.

It is tempting to include all man-made threats and hazards in this approach, but that stretches the source data too far. The RMS data and the elements estimated above refer to *terrorism* alone. In considering the information available, the objectives, etc., it is not wise to assume that common criminals, disgruntled employees, or vandals would behave in the same way. Local crime and industry statistics should be consulted to estimate the likelihood of these events.

CHAPTER 5

Service Delivery Systems Analysis

5.1 Purpose of Distributed Service Systems Analysis in RR/SAP

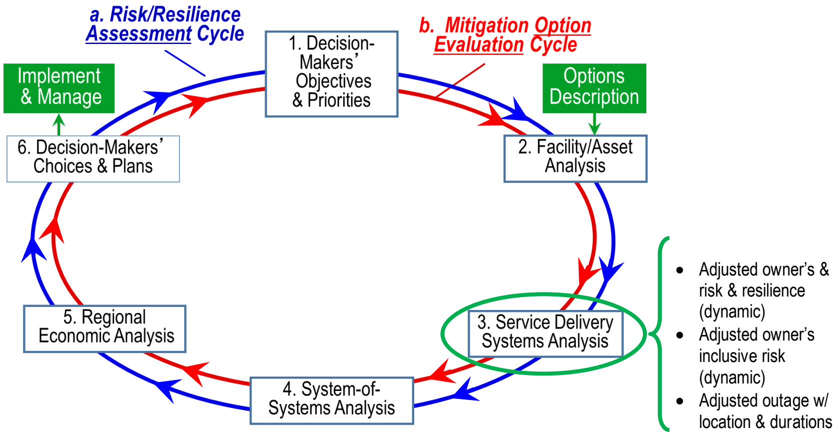
Most infrastructures deliver goods and services over an extended geographic service area. Interruption of these services causes direct disruptions to other parts of the infrastructure's extended service delivery system and to their customers. These disruptions have direct consequences on both the infrastructure and customers, ranging from inconvenience, to loss of income or production, physical losses, and even casualties. Conversely, in many infrastructures, modern SCADA and distribution management systems have the capacity to route around compromised assets to maintain service that otherwise might be disrupted. These consequences incurred by the infrastructure should be used to adjust the static consequence estimates made in the previous phase to account for the dynamics of the systems in operation. The revised estimates will adjust the owner's risk and resilience indicators and identify the specific geographic areas of service outage (*Figure 5.1*).

The purpose of distributed systems analysis is to trace these connected disruptions, estimate their immediate consequences to the owner and to identify the specific geographic areas of service denial. To do that, a distributed service model is constructed for each infrastructure to build on, complement and update the RAMCAP results. These models are also components of the system-of-systems analysis model described in the next chapter.

Distributed service models, by definition, are geographical in nature. The present project considered using GIS information to build these models, but decided that a simpler approach based on a grid pattern would be more useful in this prototype. This allows the development of the relationships and functions to be isolated for assessment. In future development of the overall approach, using GIS data will be considered.

Most infrastructures can be characterized as a system of fixed facilities and assets connected in space to fixed points of service delivery. This concept is useful for electricity, water and wastewater, emergency communications, banking, etc. It is substantially less useful in modeling the surface transportation network of highways, roads and bridges because of their ubiquity and high redundancy. For that reason, two different approaches were taken. The first,

Figure 5.1 **RR/SAP Phase 3: Service Delivery System Analysis**



described in this chapter, covers water, wastewater, electric power and emergency communications. Its concepts will be extended to other infrastructures in the future. Transportation is addressed in the next chapter, and the system-of-systems analysis is discussed in Chapter Seven.

5.2 Selection of Systems Model

For the non-transportation infrastructures, the modeling tool used was SmartMoves™, developed by Alion Science and Technology Corporation. SmartMoves is a network analysis tool that allows analysts to generate a representation of system behavior using link and node methods that establish influence paths representing the performance of distributed infrastructure systems. Nodes representing key infrastructures are connected together in a network diagram in which flows of energy, material, funds, and information are depicted as connecting arrows representing dependencies.

The need for a system-of-systems modeling environment led to development of requirements for a multi-disciplinary environment linking individual system models into a framework that recognizes interaction between systems. The requirements also indicated the need for a methodology and tool capable of operating across a wide range of data environments encountered such as those encountered in the real world. Finally, the methodology and tool selected were required to generate visually significant outputs as well as digital data.

Alion's SmartMoves technology was evaluated and selected to fulfill the project requirements. It is a methodology and tool for use in evaluating highly interconnected systems. It uses a link and node methodology to represented interconnected systems as networks following the principles of Systems Dynamics developed by Jay Forrester (1961 and 1969). Assets of interest such as power sub-stations, water pumping stations, wastewater lift stations, and emergency communications repeater and broadcast towers are represented as nodes. Single or multiple pathways of influence representing the means service deliveries are represented as connecting links. Infrastructure services are modeled as flows from node to node via connecting link. The degree of service delivery to any geographical point of interest is considered the measure of interest within a time-step driven model. Damage or degradation of an infrastructure asset or service delivery medium is propagated through the network providing insight into cascading failure patterns and generating a forecast of the impact on level of service (LOS) for each critical infrastructure. Pathways within the model represent both primary service delivery paths and a control network represents the switching and routing functions performed by modern SCADA.

SmartMoves includes a capital budgeting prioritization module that conducts cost-benefit analysis of single action and bundled action investment strategies.

SmartMoves is built around an interactive tradespace function that supports spot "what-if" assessments for spot failures as well as full-scale, regional scenario evaluation. The product of assessments is a forecast of the LOS for each critical infrastructure over a defined geographic area over a defined time horizon.

SmartMoves includes a capital budgeting prioritization module that conducts cost-benefit analysis of single action and bundled action investment strategies. SmartMoves is compatible with commercially available decision support software applications that support group generation benefit mapping tables and project priority based on association with stated goals. SmartMoves supports rapid closure on the short-list of viable investment options and supports assessment of those options across a range of future environments. SmartMoves works in multi-year assessment environments providing visibility of cost and benefit impact over an investment horizon.

A key SmartMoves characteristic that proved critical to the project requirements is its ability to cut across institutional "stovepipes" and methodologies allowing the information elements generated in specialized domains to interact with each other producing an estimate of regional-level impacts. SmartMoves is flexible and agile enough to operate with existing enterprise information. It is capable of working in the real world where decision environments need to consider both data and subject matter expertise. Its core methodologies overcome the challenges associated with ambiguous or incomplete data that often derail other decision support tools. SmartMoves continuously incorporates institutional and program specific lessons reducing future dependency on "tribal knowledge." It can operate at a very high "sketch level" to help leadership quickly assess opportunities and challenges, see the solution space, and generate change guidance that will lead to the most agile enterprise possible in the least time, at the least cost. SmartMoves can operate across a range of data density minimizing the disruption of day-to-day staff activities.

SmartMoves allows the user to build credible models with empirical information as the basis for predicting system behavior under a wide range of conditions.

Interdependencies are modeled within the context of the unique metropolitan area or regional infrastructure complex. The network diagram allows a change at one node (representing damage to a physical asset) to be pulsed through the system providing insight into the cascade pattern and the magnitude of impact at any particular node within the system. As the nodes within the system are affected, the performance of the infrastructure sectors within the system is affected. A SmartMoves model is typically related to a geographical representation that displays the model results in terms of infrastructure performance in user designated analysis zones.

Underpinning SmartMoves is a time control function that allows the user to establish reference times and forecast periods. This function supports analysis of infrastructure system performance over time using user-defined time-steps as discrete event markers within the model. "Soft agents" provide logic elements to manage switching functions and generate conditional responses over time. Time series runs generate the impacts caused by the increase, cessation, reduction, or gradual decay of critical flows between infrastructure components that make up the system. This, coupled with the control system, allows for a refined estimate of the time and location of service outages.

SmartMoves allows the user to build credible models with empirical information as the basis for predicting system behavior under a wide range of conditions. SmartMoves methodologies simplify the network modeling process allowing an inference-based solution to be used as a means of representing the multitude of possible outcomes that are present in large network models.

In brief, SmartMoves was selected for the RR/SAP prototype because the methodology, developed over the past five years, provides a transferrable method to rapidly outline and model the performance of infrastructure systems that underpin regional activity and ranges from delivery of basic public safety services to expansion and development of the economic base.

5.3 Non-Transportation Infrastructures: Basic Concept

The methodology recognizes that the performance of infrastructure systems is directly related to regional activity and that stress related to natural or man-made events may cause a region to temporarily move down the Level of Regional Activity continuum illustrated in *Figure 5.2*.

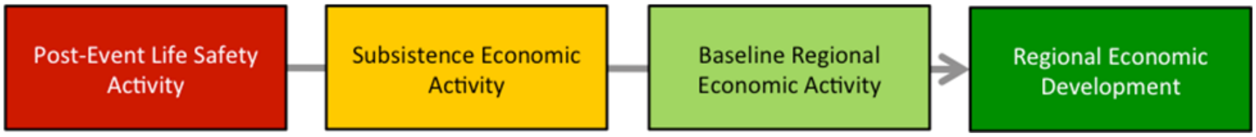


Figure 5.2 **The Level of Regional Activity Continuum Identifying Discrete Performance Levels**

The link between infrastructure performance and regional activity is the LOS across the foundational infrastructures. Electrical power, water, wastewater, emergency communications, and transportation infrastructures are considered in this study. Besides transportation, each infrastructure is addressed as independent systems in this chapter. The systems are evaluated in post-event environments to determine a LOS that indicates, on a scale of 0.0 to 1.0, the ability of the system to balance supply and demand. The objective in this chapter is to present the method used to evaluate the LOS for each infrastructure and to summarize the results of the assessment. This chapter is dedicated to a systems model – independently assessing each infrastructure.

The system model LOS estimate is generated considering the overall system capacity, individual asset contributions to capacity, the post-event recovery profile of individual assets, and the ability of system control functions to overcome asset degradation or destruction via implementation of alternate load distribution plans and delivery paths. The system model recognizes that post-event LOS may be unevenly distributed throughout the region and that the LOS and distribution patterns will change over time as assets are repaired and put back into service. It accounts for asset restoration profiles and for constraints in alternate path availability generating spatial and temporal LOS forecasts for the 30-day period following an event. LOS output values from the system model support economic impact assessment including lost revenue to the service provider and lost productivity to the customer.

The methodology views each of the distributed service infrastructures as systems of links, nodes, and control functions that are integrated to form a value stream. The physical aspects of the infrastructure system are defined as assets that possess qualities with respect to vulnerability to specific natural or man-made threats, as captured in the previous RR/SAP Phase (RAMCAP). The control aspects of the infrastructure system are defined as the ability to exercise load management and/or path management to accommodate routine asset maintenance, wear-based asset degradation, and event-based asset degradation or destruction. Control functions also possess qualities with respect to vulnerability to specific natural or man-made threats that were also assessed in the RAMCAP Phase.

A water system example is illustrated in *Figure 5.3* indicating that the LOS realized at each point of service (POS) is a function of the performance of physical assets and control functions leading to it from the original water source.

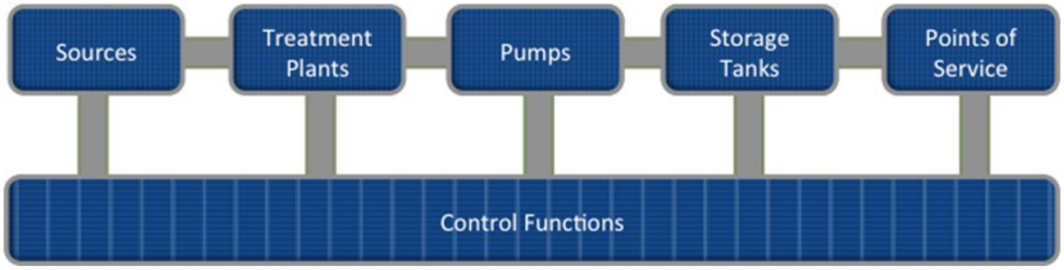


Figure 5.3 **Link - Node - Control Function Infrastructure Modeling Concept**

The methodology assumes that degradation of a physical asset will lead to system performance degradation and that control functions will be used to select alternative load distribution and delivery options to minimize impact and speed recovery.

5.4 Principles of the Methodology

The distributed system modeling and assessment methodology is a cause-and-effect-based approach. The method is based on the following principles:

- Principle One — Physical infrastructure assets are geographically distributed across a region.
- Principle Two — Natural and man-made events generate and emit damage and destruction mechanisms on a localized basis. Individual infrastructure asset performance is degraded based on the vulnerability of the individual asset to the specific damage and destruction mechanisms generated by the event within effective proximity.
- Principle Three — Infrastructure LOS is affected differentially across the region based on the footprint of the event, role of the specific damaged or destroyed asset, system subsystem, and asset excess capacity, path redundancy, system compartmentalization, and the agility of the system control function.
- Principle Four — Infrastructure LOS degradation for a specific damage profile may vary in spatial and temporal distribution based on asset recovery profiles and efforts to continuously manage capacity and demand.

5.5 Common Location Reference System

The approach uses a geo-reference system that can vary between coarse and fine. Within the methodology, finite elements can range in dimensions from 2 miles by 2 miles down to 60 feet by 60 feet. The finite element methodology can be supplemented with precise locations for specific points of interest using GIS information. Selection of the finite element dimensions and the inclusion of specific point locations of interest are subject to the precision of the available data, the scale of the region of interest, and the purpose of the assessment.

For the purpose of this study, a representative region was identified. *It was based on a map of Nashville, Tennessee, but all locational and functional information is purely hypothetical and for illustration of the method only.* The hypothetical region is approximately 150 square miles in area consisting of rolling hills that range in elevation from 1000 feet above mean sea level (MSL) to 1700 feet above MSL. The region is bisected by a major river that runs through a low elevation area at approximately 800 feet above MSL that skirts the northern boundary of the central business district. The business district hosts government and commercial areas including tourist attractions. The area directly to the south of the business district is a center of medical research and medical care facilities along with affiliated universities. The southeastern area is predominantly light industrial while the southwestern and northwestern areas are predominantly suburban with transitions to rural land use. The northeastern area is a mix between light industrial, suburban and rural land use. The study employs a finite element grid as illustrated in *Figure 5.4*.

5.6 Association of Events with Area Impacts

Alion Science and Technology's SmartMoves modeling system was used to generate a cause-and-effect modeling approach to asset damage and destruction based on the occurrence of a natural or man-made event within a zone of influence. The system employs grid system to record the area impact of an event. The area impact was modeled as a range from "no effect"

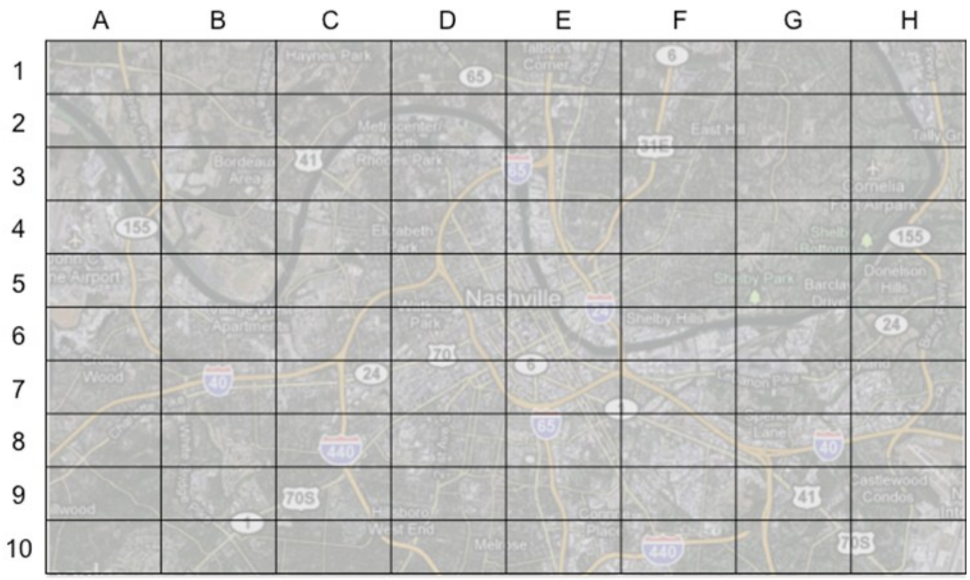
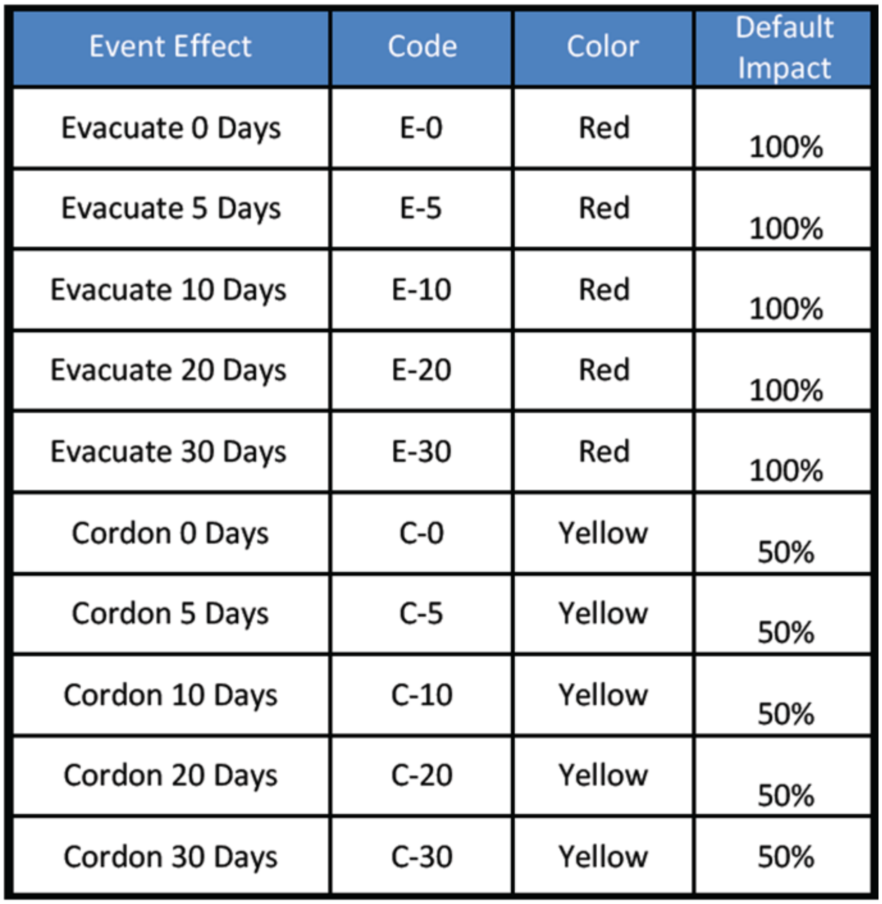


Figure 5.4 **Grid Location Concept Employed in the Modeling Methodology**

Table 5.1 **Area Impact Assessment Schema**



Event Effect	Code	Color	Default Impact
Evacuate 0 Days	E-0	Red	100%
Evacuate 5 Days	E-5	Red	100%
Evacuate 10 Days	E-10	Red	100%
Evacuate 20 Days	E-20	Red	100%
Evacuate 30 Days	E-30	Red	100%
Cordon 0 Days	C-0	Yellow	50%
Cordon 5 Days	C-5	Yellow	50%
Cordon 10 Days	C-10	Yellow	50%
Cordon 20 Days	C-20	Yellow	50%
Cordon 30 Days	C-30	Yellow	50%

to “evacuation required” for periods of time ranging from 0 to 30 days. An intermediate impact level is noted by the designation of a “cordon” for a particular area. The cordon designation is supplemented by a duration designation ranging from 0 to 30 days. *Table 5.1* shows the full range of possible area impacts.

Evacuation is defined as all people are ordered to leave the area for the designated time period. The only access allowed are emergency personnel including public safety and infrastructure repair crews. Cordon is defined access by emergency personnel including public safety and infrastructure repair crews as well as residents and business owners.

As an illustrative scenario to support the study, a HAZMAT event takes place at 9:00 AM on a Wednesday in the spring of the year. The case is a chlorine spill of approximately 8500 gallons in the southeastern corner of Grid C-4. The effects of the spill are carried by prevailing southwesterly winds generating an area impact pattern as shown in *Figure 5.5*.

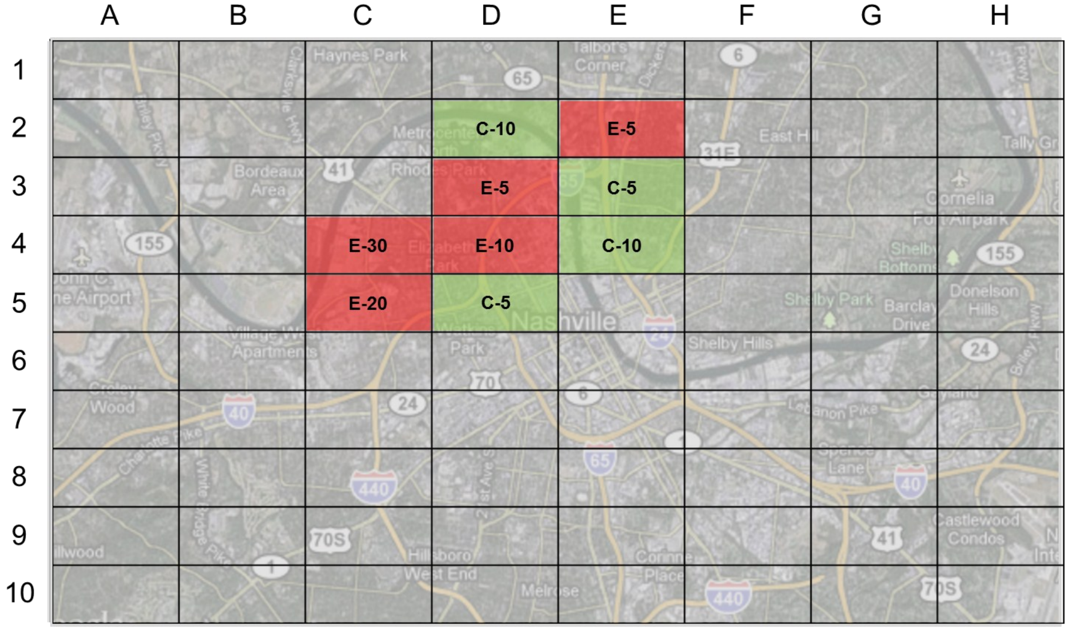
A total of nine zones covering approximately fifteen square miles are affected. Five grid zones comprising approximately eight square miles are evacuated and four grid zones comprising approximately seven square miles are cordoned.

5.7 Application of the Systems Model

5.7.1 Inventory and Locate Infrastructure Assets

Electrical Power. The electrical power system for the study consists of an independent electrical distribution service that purchases power from major power generation facilities outside the metro area through a multi-state grid. Power is delivered to the service provider via transmission lines that terminate at main power stations identified in *Figure 5.6* as Mains 1, 2, and 3. From the main power stations, power is distributed to substations via a combination of overhead, bridge-suspended, and underground lines. There are three subsystems differentiated by nominal operating voltage, 15 substations, two critical overhead line segments, and three critical bridge-suspended segments. Power is distributed via a system of closed loops that spur distribution lines. The central study area is characterized by significant path redundancy. The fringes of the area are served by dedicated service lines with little to no path redundancy. The system has a 20% excess capacity as a system, 20% excess

Figure 5.5 **Area Impact Tool Output for a Specific Event (Map Overlay)**



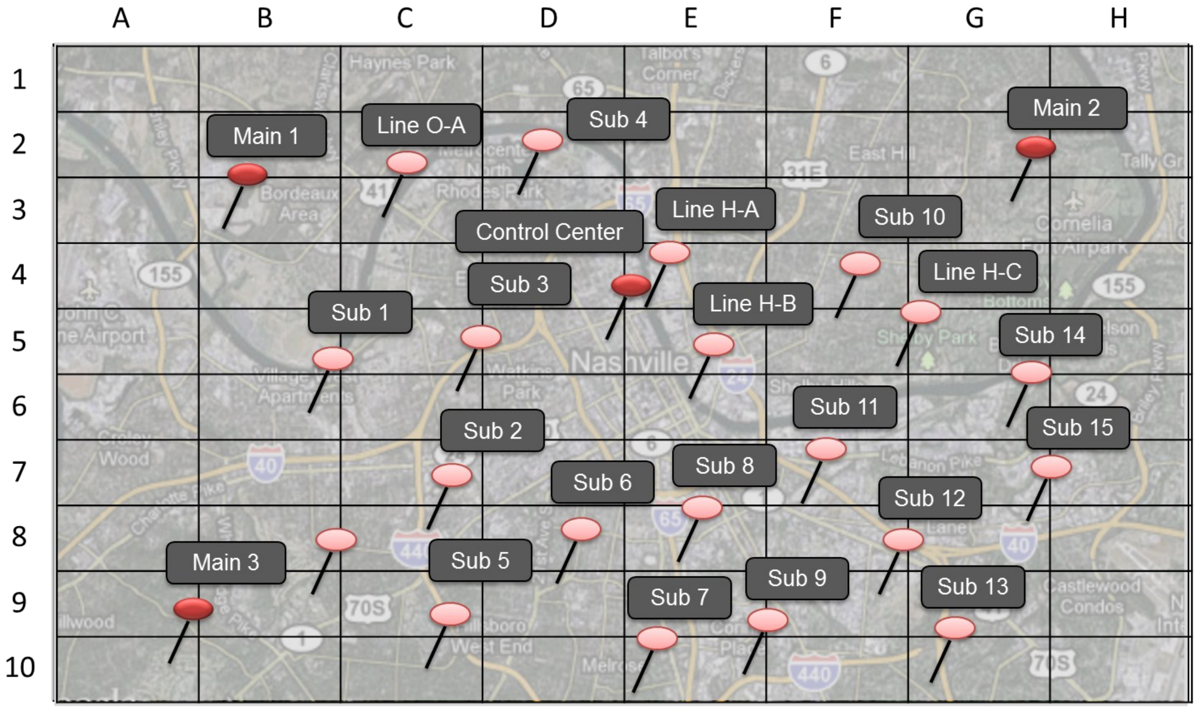


Figure 5.6 **Electrical Asset Inventory and Spatial Distribution (Map Overlay)**

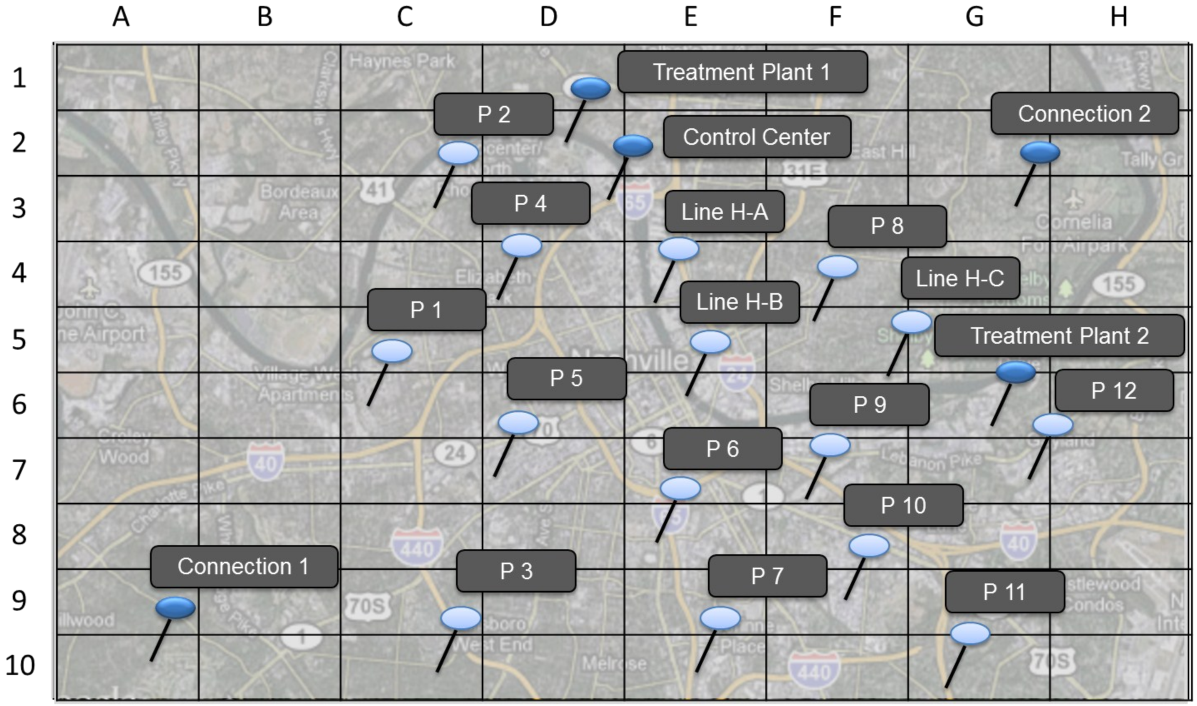


Figure 5.7 **Water Asset Inventory and Spatial Distribution (Map Overlay)**

capacity within each of the subsystems, and 20% excess capacity at each substation. Theoretically, the system can operate within an environment in which three substations are completely incapacitated.

Water Supply. The water and wastewater system for the study consists of a municipally-operated water and wastewater utility. Water is sourced from the major bisecting river at two points east and west of the downtown center. These source points are collocated with the two independent water treatment facilities identified in *Figure 5.7*. Each facility splits the capacity to serve 75% of the regional demand. Under normal circumstances the region is divided in half, with each half served by a single source and treatment facility. The control center is collocated with the western treatment plant. It is supported by a backup power generation system with a seven-day supply of fuel. The eastern treatment plan has a dual electrical service supported by two different substations. Under stress, several in-place connection points allow a single plant to serve the entire region albeit at a deficit supply to demand ratio. Under circumstances where supply is less than demand, the region can purchase water from neighboring districts via two existing cross-jurisdictional connection points totaling to 15% of the normal supply level. Water is delivered to the points of service via mechanically pressurized service lines. Pressure is maintained via twelve pump stations that are powered by the electrical service provider. From the water treatment stations, water is distributed via a combination of bridge-suspended and underground lines. The central study area is characterized by significant path redundancy. The fringes of the area are served by dedicated service lines with little to no path redundancy.

Wastewater. Wastewater is treated at two independent facilities identified in *Figure 5.8*. One is located in a complex near the western water treatment plant. The second is located in the southeastern quadrant of the region. The control center is collocated with the water control center. Although controlled by the same center, the plants are operated independently of each other. Both wastewater treatment plants are served by the municipal electric service provider

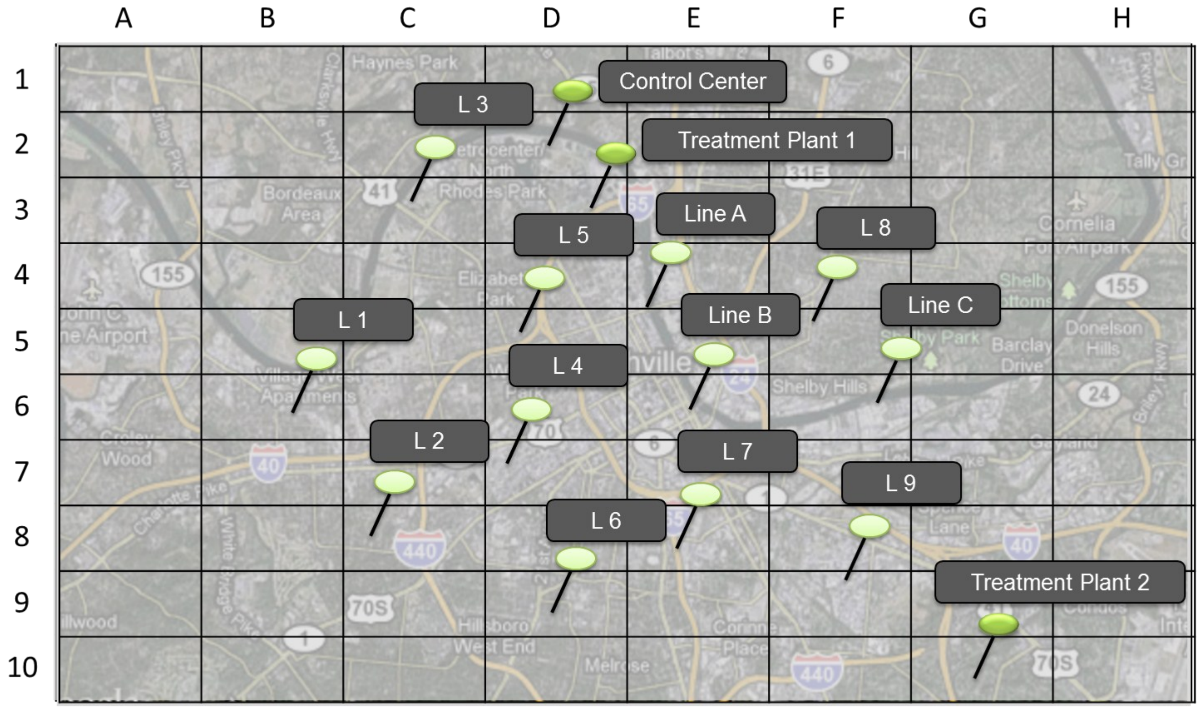


Figure 5.8 **Wastewater Asset Inventory and Spatial Distribution (Map Overlay)**

and have backup power sources with a five-day supply of fuel. The southeastern wastewater treatment plant has a dual electric service supported by two different substations. There are nine wastewater lift stations. Stations 1 through 5 serve the western district and stations 6 through 9 serve the eastern district. Each service district contains a bridge-suspended line segment. Within each service area, wastewater is distributed via a system of interconnected and spur-forced main collection lines. The central study area is characterized by significant path redundancy and the fringes of the area are served by dedicated service lines with little to no path redundancy.

Emergency Communications. The emergency communication system is an 800MHz radio system that is supported by a central transmission and dispatch center located in the south-central area of the region depicted in *Figure 5.9*. The system carries all dispatch communications for police, fire, and emergency medical service. The physical system is shared with the electric service provider during stress conditions supporting power service crew dispatch on an alternate channel set. This facility has a backup center capable of 100% duplication of function that is located in the southeastern area. The system is comprised of seven towers distributed over the region to provide full area coverage. There is significant overlap in the tower coverage network such that a single tower leaves only trace areas uncovered in the northwestern area due to terrain interference. The region has a mobile command vehicle capable of acting as a repeater station. Its range and radius of communication is dependent on its location during a response event. Of note is that in the representative region, the entire dispatch function is dependent upon the viability of the commercial telephone switch and the main trunk lines that capture and route all 911 calls. The trunk lines shown east and west of the facility are 100% redundant.

5.7.2 Determine the Asset Impact Profile

The system model generates asset impacts based on reference to the area impact assessment. When an event generates an impact within a grid zone, the next version of RR/SAP will draw on the RAMCAP data for the amount of damage, performance degradation and recovery profiles of

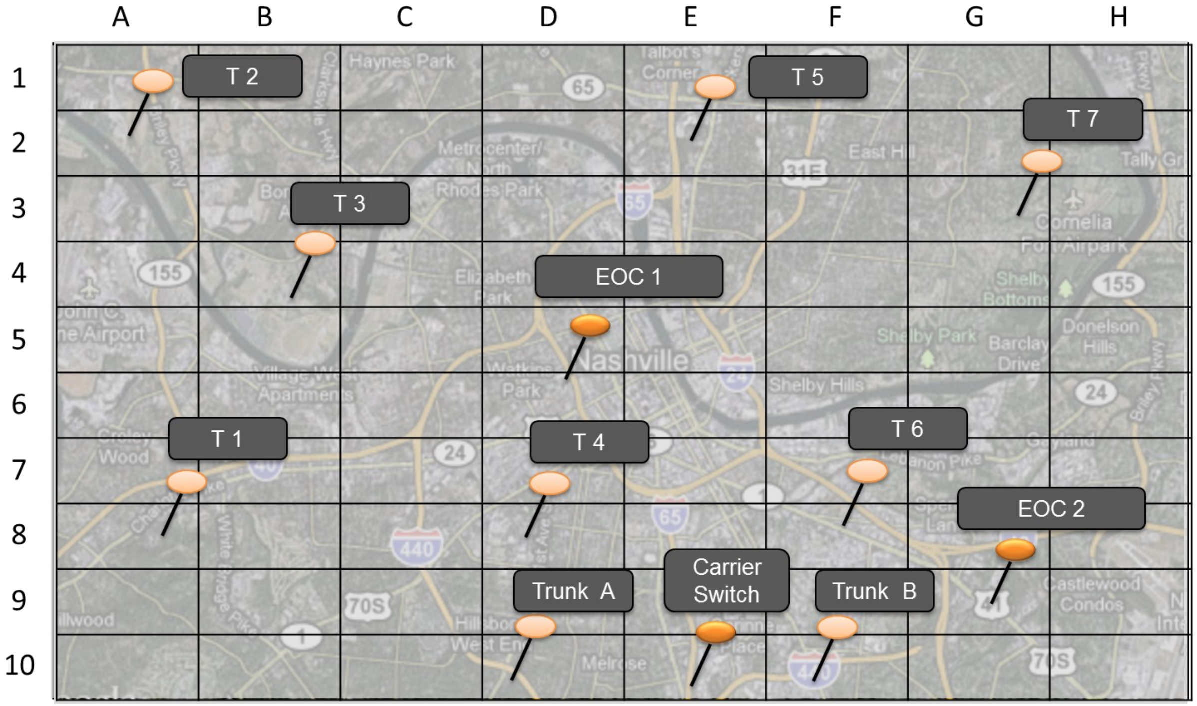


Figure 5.9 **Emergency Communications Asset Inventory and Spatial Distribution (Map Overlay)**

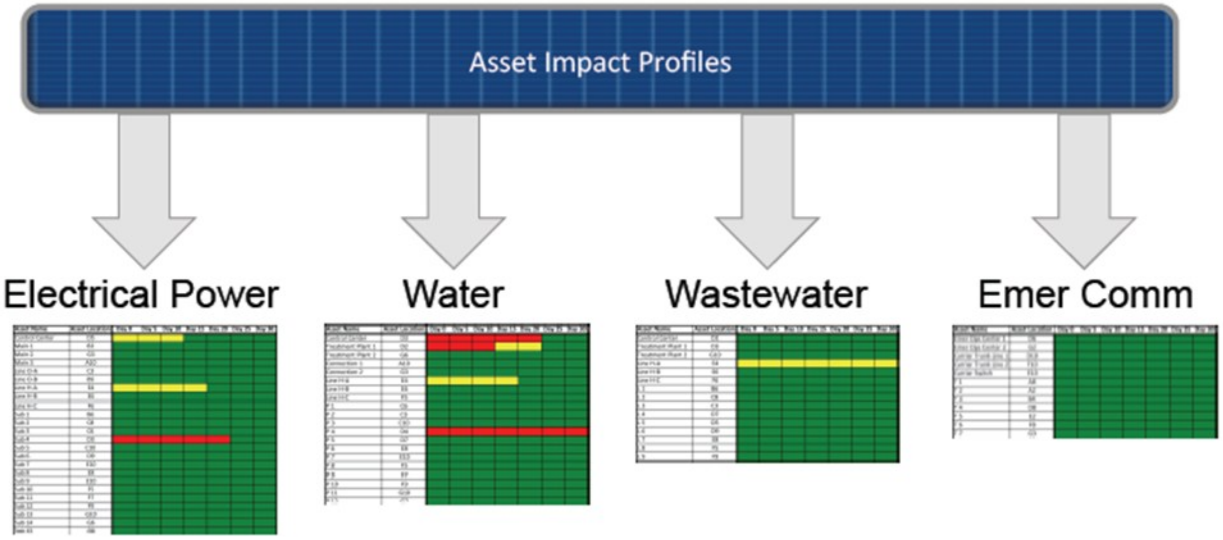


Figure 5.10 **Asset Impact Profiles based on an Event**

infrastructure assets in the zone. In this initial prototype (and the absence of the RAMCAP data), default impact levels are applied to applicable infrastructure assets and default recovery profiles are assigned. The degree of performance degradation is associated with the designation of "no impact," "cordon," or "evacuation". The model assumes a default value of 50% degradation (yellow) in the performance of an asset under cordon conditions and a default value of 100% degradation (red) under evacuation conditions. The recovery profile is related to the degree of degradation and the duration of the cordon or evacuation. The default recovery profile is a linear gradient assuming a 10% restoration factor per day.

The asset impact tool provides an asset impact summary by infrastructure and identifies the recovery timeline in for each asset in Gantt chart form as illustrated in *Figure 5.10.*[14]   The asset-specific bars represent the length of time of the asset is compromised, while the color represents how severely compromised. Analysts are able to select and modify the percent of degradation and the recovery profile based on the information captured in the RR/SAP Phase 2 facility/asset assessment when even partial information is available.

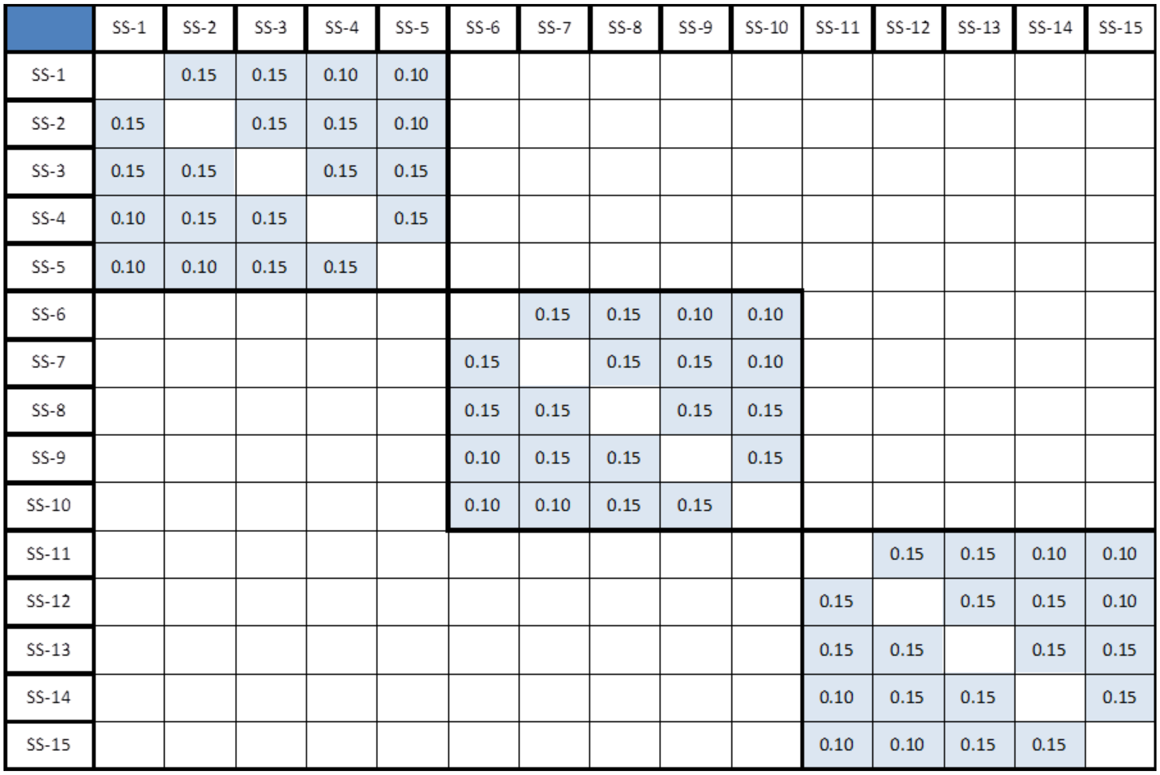
5.7.3 Determine the Impact of Load Management and Alternate Paths

The approach recognizes that damage to or destruction of an infrastructure asset represents an interruption in the operation of the grid. Under these conditions, the method employs an algorithm to emulate control functions that seek to identify load redistribution options and alternate delivery paths that continuously establish a best available distribution pattern. To accomplish this, the model uses a capacity substitution matrix, which is a simplification of the complex process that utility operators engage in when resolving system failures in a real-time process. The actual process uses a SCADA system supported by the highly trained engineering teams that iteratively conduct distribution planning for maintenance and service restoration during post-event and throughout the recovery period. The matrix reflects the ability of one asset to "fill-in" for capacity loss that occurs when another asset is degraded or destroyed, recognizing constraints associated with the real world such as the availability of transferrable capacity, the physical capability to

---

[14] For illustrative purposes only to display the Gantt chart timeline recovery of the assets, not the asset list itself.

Figure 5.11 **The Electrical Power Asset Substitution Matrix**



	SS-1	SS-2	SS-3	SS-4	SS-5	SS-6	SS-7	SS-8	SS-9	SS-10	SS-11	SS-12	SS-13	SS-14	SS-15
SS-1		0.15	0.15	0.10	0.10										
SS-2	0.15		0.15	0.15	0.10										
SS-3	0.15	0.15		0.15	0.15										
SS-4	0.10	0.15	0.15		0.15										
SS-5	0.10	0.10	0.15	0.15											
SS-6							0.15	0.15	0.10	0.10					
SS-7						0.15		0.15	0.15	0.10					
SS-8						0.15	0.15		0.15	0.15					
SS-9						0.10	0.15	0.15		0.15					
SS-10						0.10	0.10	0.15	0.15						
SS-11												0.15	0.15	0.10	0.10
SS-12											0.15		0.15	0.15	0.10
SS-13											0.15	0.15		0.15	0.15
SS-14											0.10	0.15	0.15		0.15
SS-15											0.10	0.10	0.15	0.15	

transfer load, and the compatibility of assets within the system.

The matrix shown in *Figure 5.11* captures each of these constraints in a manner that can be used in generation of a grid-cell-by-grid-cell and time-step-by-time-step electrical power LOS forecast. The value shown in intersection of paired cells identifies the degree to which an asset (row) can "fill-in" for degraded performance by another asset (column).

In the example, three distinct subsystems are revealed based on limits to the transfer of load, such as line capacity or lack of compatibility between subsystems (variation in voltage in the case of power). The fraction indicates the percentage of the destination load that can be assumed. Within the model, a call for load transfer to a damaged or destroyed asset (column) leads to a transfer from the highest potential unassigned contributor (row). In cases where there are equal potential contributors, the closest in physical proximity is selected. Once a contributor is used, it is unavailable to support other requests even if there is capacity to do so. As an example, a value of 0.15 in row SS-3 indicates that the asset can assume 15% of the asset load for substations (SS-1, SS-2, SS-4, or SS-5). Likewise, it indicates that excess capacity in SS-15 (row) cannot be transferred to SS-4 (column).

5.7.4 Determine the Level of Service Profile

The final step in the process is development of a grid-cell-by-grid-cell, time-step-by-time-step LOS distribution map that identifies the effects of

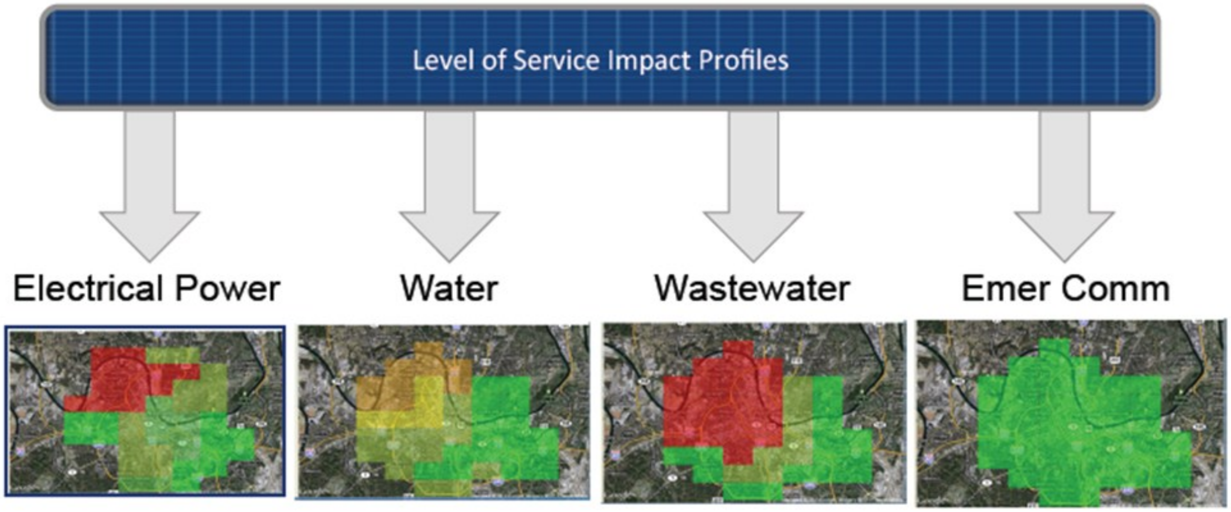


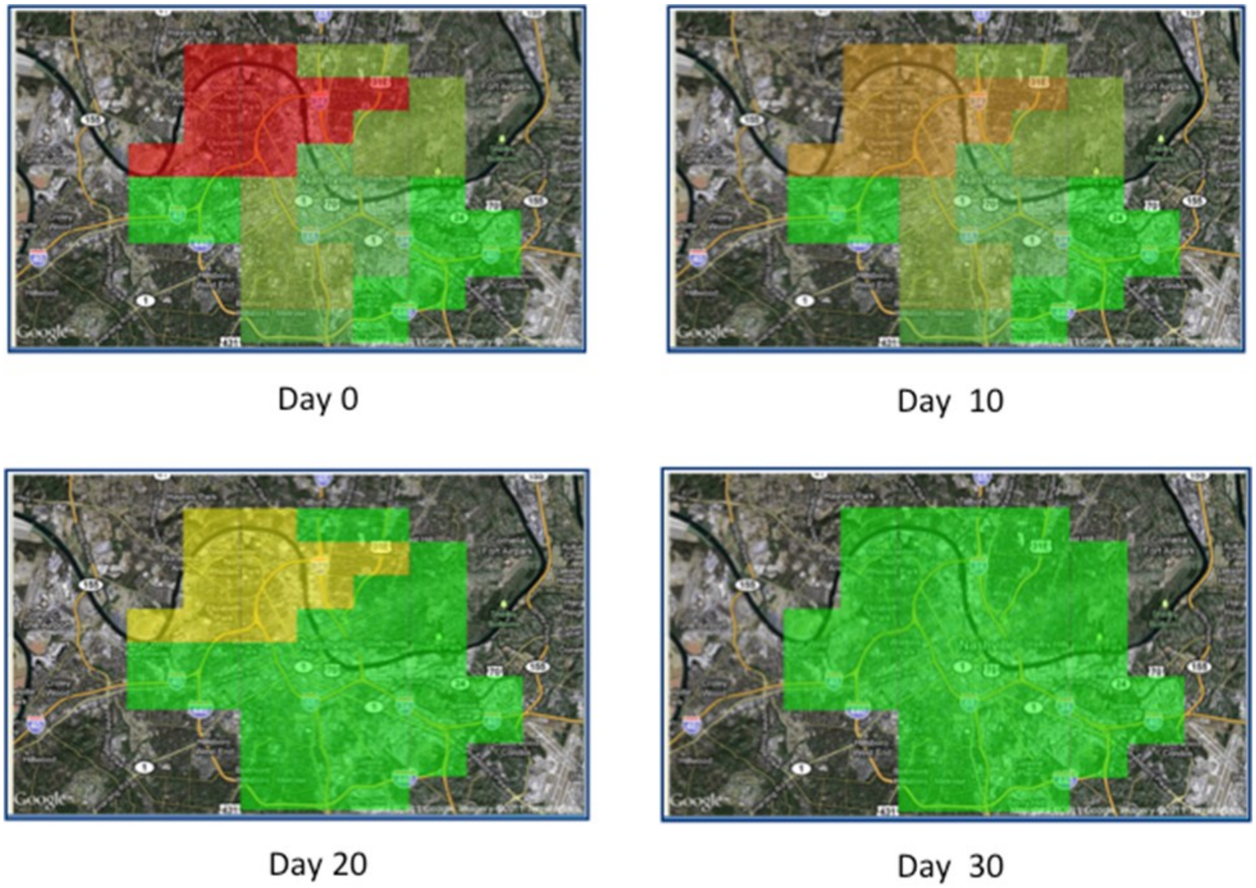
Figure 5.12 **Initial Post-Event LOS Distribution Maps**

asset degradation on service delivery given the application of control measures to achieve a "best available" distribution. The model within SmartMoves considers the many-to-many influence pattern associated with the capacity substitution availability identified in Section 5.3 along with a utility operator-generated prioritization matrix generated by the utility operator that reflects the spatial distribution of critical customers. The model employs an algorithm that adjusts the distribution matrix at each 10-day interval based on the asset recovery profiles identified in Section 5.2.

An example of the post-event LOS distribution maps for each infrastructure is shown in *Figure 5.12*. The maps illustrate the impact of the asset damage associated with the event, the influence of control function load and distribution path balancing given system constraints, and the influence of critical customer locations.

5.7.5 Estimate of the Economic Impact to the Service Provider

The ability to forecast the LOS on a grid-by-grid, time-step-by-time-step basis is a key feature in the assessment of the economic impact of infrastructure breakdown. The LOS distribution map for each of the four infrastructures, generated at time-steps throughout the event and recovery sequence, provide the basis for assessing the economic loss to the operating agency and the economic loss to the customer. The methods in RR/SAP Phase 2 identify the cost of reconstruction of assets and potential gross revenue losses. The service denied and revenue losses are often overstated when looking only at the performance of individual facilities and assets because of the ability to work around damaged system elements as described above. This RR/SAP Phase 3 provides the economic losses associated with the correct lost revenue. This leads to updates to both the owner's risk and


Day 0

Day 10

Day 20

Day 30

Figure 5.13 **Electrical Power LOS Distribution at 10-day Time-steps**

resilience indictors from the previous phase. RR/SAP Phase 4 (Chapter Six) will address the impact of LOS of one infrastructure to impact the ability of other infrastructures to deliver their services. Chapter Eight will relate these infrastructure failures to the public safety services that reduce injuries and fatalities; and Chapter Nine will describe RR/SAP Phase 5, the impact on regional economic activity. The remainder of this chapter will focus on the economic loss to the electrical utility operator based on loss of revenue

Figure 5.13 shows the essential grid-by-grid, time-step-by-time-step LOS progression through various LOS values over the 30-day period following the event. In the example case, the development of alternate power sources and

Figure 5.14 **Computation of Incremental Revenue**[15]

---

[15] For illustrative purposes to demonstrate Realized Revenue is the product of Geographic Revenue Distribution and Power Delivery.

alternate delivery paths is spread out over the entire 30-day period.

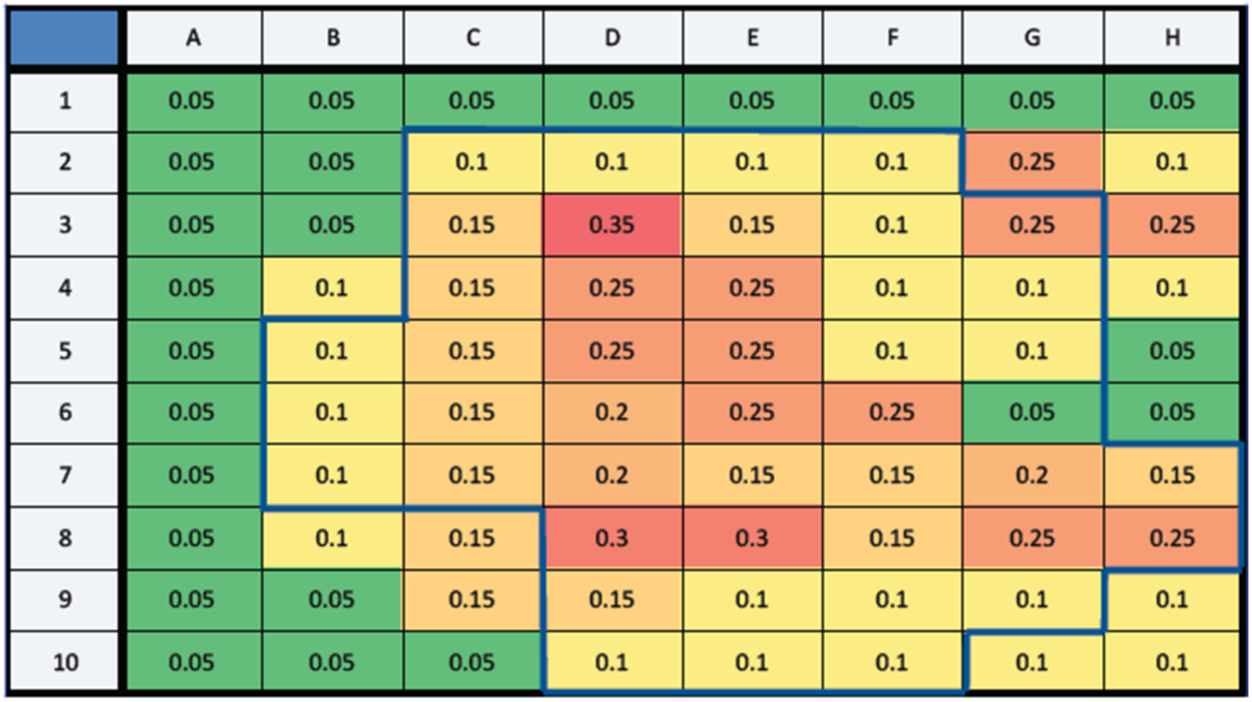
These images are generated by digital estimates of LOS providing the basis for computing an expected loss of revenue profile, which can be seen in *Figure 5.14*. The first task in this computational process is assignment of revenue to grid cells. The electrical utility, in this case, provides a cell-by-cell distribution of average daily revenue that reflects historical billing patterns. The cell-by-cell revenue distribution is multiplied by the time-step-by-time-step LOS distribution matrix to produce a period-specific revenue rate expressed as a percentage of the daily average. (Note that these figures appear at a legible scale elsewhere in this chapter.)

5.8 Case Study – Electrical Power Revenue Loss – Chlorine Spill Scenario

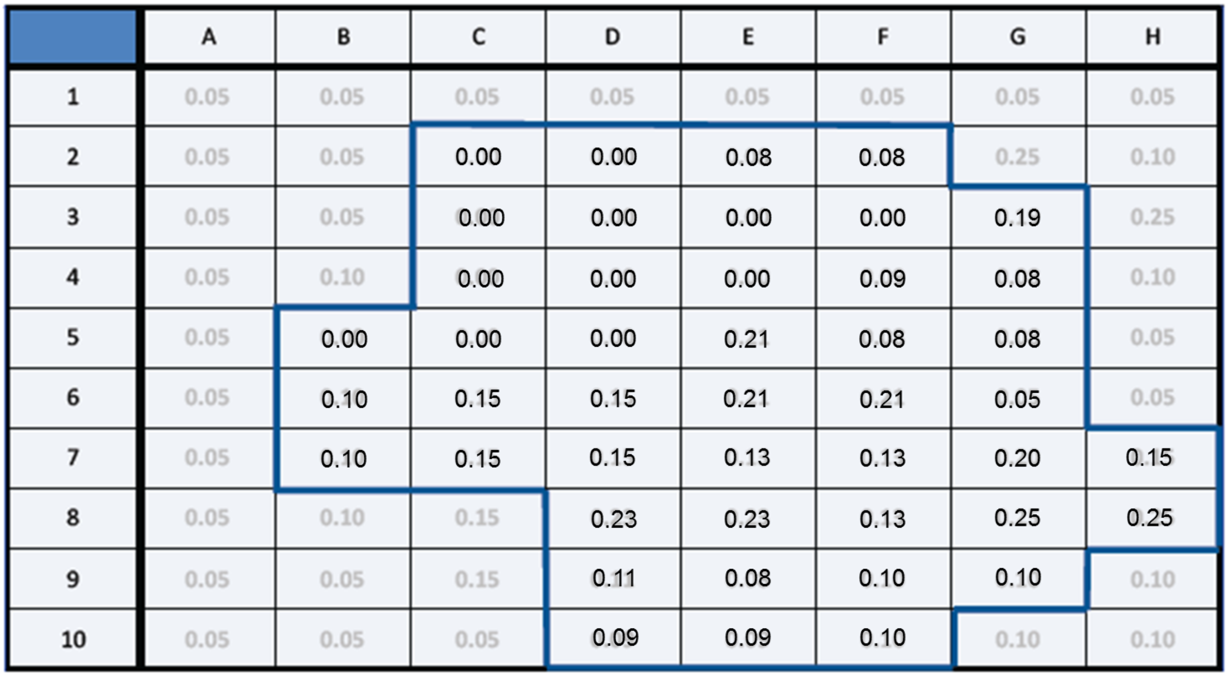
Generate the Revenue Distribution Matrix. The electrical power revenue distribution matrix used in this study is shown in *Figure 5.15*. The total revenue is normalized to a value of 10.0. Cell revenue assignments represent the portion of the average daily revenue that is attributed to the customer base within that cell. The values shown are representative of those that can be generated based on publicly available density and land use data and residential and commercial utility rates. The values are subject to refinement by the service provider as true cell-by-cell values are identified and substituted.

Generate the Time-step-by-Time-step LOS Matrix. The electrical power revenue LOS matrix is generated by the systems model previously presented in this chapter. The cell-by-cell, time-step-by-time-step values are generated in conjunction with the visualization of the recovery profile. The four time-step matrices for electrical power are displayed in *Figures 5.16-5.19* below. Note the interaction between the incremental LOS and the revenue. In the scenario examined, cell D-3 is the highest revenue contributing cell. Through the sequence, its contribution is governed by the rate of recovery profile of the individual assets and the control functions that seek to optimize the LOS-based system incrementally improving capabilities and the need to serve critical customers. Revenue recovery in cell D-3 lags the regional average due to available excess capacity and subsystem compatibility.

Figure 5.15 **The Revenue Distribution Matrix for the Electrical Power Utility**



	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.1	0.1	0.1	0.1	0.25	0.1
3	0.05	0.05	0.15	0.35	0.15	0.1	0.25	0.25
4	0.05	0.1	0.15	0.25	0.25	0.1	0.1	0.1
5	0.05	0.1	0.15	0.25	0.25	0.1	0.1	0.05
6	0.05	0.1	0.15	0.2	0.25	0.25	0.05	0.05
7	0.05	0.1	0.15	0.2	0.15	0.15	0.2	0.15
8	0.05	0.1	0.15	0.3	0.3	0.15	0.25	0.25
9	0.05	0.05	0.15	0.15	0.1	0.1	0.1	0.1
10	0.05	0.05	0.05	0.1	0.1	0.1	0.1	0.1



	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.00	0.00	0.08	0.08	0.25	0.10
3	0.05	0.05	0.00	0.00	0.00	0.00	0.19	0.25
4	0.05	0.10	0.00	0.00	0.00	0.09	0.08	0.10
5	0.05	0.00	0.00	0.00	0.21	0.08	0.08	0.05
6	0.05	0.10	0.15	0.15	0.21	0.21	0.05	0.05
7	0.05	0.10	0.15	0.15	0.13	0.13	0.20	0.15
8	0.05	0.10	0.15	0.23	0.23	0.13	0.25	0.25
9	0.05	0.05	0.15	0.11	0.08	0.10	0.10	0.10
10	0.05	0.05	0.05	0.09	0.09	0.10	0.10	0.10

Figure 5.16 **Day 1-10 LOS Distribution**

	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.04	0.04	0.08	0.08	0.25	0.10
3	0.05	0.05	0.05	0.12	0.05	0.04	0.19	0.25
4	0.05	0.10	0.05	0.09	0.09	0.09	0.08	0.10
5	0.05	0.04	0.05	0.09	0.21	0.08	0.08	0.05
6	0.05	0.10	0.15	0.15	0.21	0.21	0.05	0.05
7	0.05	0.10	0.15	0.15	0.13	0.13	0.20	0.15
8	0.05	0.10	0.15	0.23	0.23	0.13	0.25	0.25
9	0.05	0.05	0.15	0.11	0.08	0.10	0.10	0.10
10	0.05	0.05	0.05	0.09	0.09	0.10	0.10	0.10

Figure 5.17 **Day 11-20 LOS Distribution**

	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.05	0.05	0.10	0.10	0.25	0.10
3	0.05	0.05	0.08	0.18	0.08	0.05	0.25	0.25
4	0.05	0.10	0.08	0.13	0.13	0.10	0.10	0.10
5	0.05	0.05	0.08	0.13	0.25	0.10	0.10	0.05
6	0.05	0.10	0.15	0.20	0.25	0.25	0.05	0.05
7	0.05	0.10	0.15	0.20	0.15	0.15	0.20	0.15
8	0.05	0.10	0.15	0.30	0.30	0.15	0.25	0.25
9	0.05	0.05	0.15	0.15	0.10	0.10	0.10	0.10
10	0.05	0.05	0.05	0.10	0.10	0.10	0.10	0.10

Figure 5.18 **Day 21-30 LOS Distribution**

	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.10	0.10	0.10	0.10	0.25	0.10
3	0.05	0.05	0.15	0.35	0.15	0.10	0.25	0.25
4	0.05	0.10	0.15	0.25	0.25	0.10	0.10	0.10
5	0.05	0.10	0.15	0.25	0.25	0.10	0.10	0.05
6	0.05	0.10	0.15	0.20	0.25	0.25	0.05	0.05
7	0.05	0.10	0.15	0.20	0.15	0.15	0.20	0.15
8	0.05	0.10	0.15	0.30	0.30	0.15	0.25	0.25
9	0.05	0.05	0.15	0.15	0.10	0.10	0.10	0.10
10	0.05	0.05	0.05	0.10	0.10	0.10	0.10	0.10

Figure 5.19 **Day 31+ LOS Distribution – Return to Normal**

Table 5.2 **Computation of Revenue Loss during an Event and Recovery Period**

Revenue Loss Model - 30-Day Assessment		
Average Daily Revenue (System Wide)		$2,070,050
Day 0-10 Daily Revenue Loss		$584,789
Day 11-20 Daily Revenue Loss		$432,640
Day 21-30 Daily Revenue Loss		$217,355
Total Expected Revenue		$62,101,500
Total Realized Revenue		$49,753,652
Total Revenue Loss		**$12,347,848**

Generate the Revenue Profile. The electrical power revenue profile is generated by incrementally computing the realized revenue over the recovery time period. The average daily revenue value used in the assessment is $2,070,050. Total realized revenue is computed by integrating over the 30-day period. Revenue loss is found as the difference between expected revenue and forecast revenue.

The total revenue loss is computed incrementally by time-step period computing and then summing the losses experienced during each time-step. *Table 5.2* identifies the total revenue loss over the entire period as approximately 20% of expected revenue.

Estimate Service Default Penalties. Some customers may have contacts with the infrastructures that penalize non-delivery of service in the form of payments. By knowing the geographic locations, severity and duration of the outages, and the location of such customers, the likely penalty payments can be estimated and included in the owner's losses.

Update Owner's Risk and Resilience Indicators. The total revenue loss (plus any penalty payments or additional damage) calculated here is substituted for the gross revenue loss (static) estimated in RR/SAP Phase 2 for the adjusted owner's revenue loss and the adjusted owner's risk and resilience (dynamic) indicators are updated as appropriate. The geographical areas of service reduction are preserved for use in the next phase of the analysis.

In the RR/SAP assessment cycle, these risk/resilience indicators point to the most pressing challenges to the infrastructure's owners. In the RR/SAP evaluation cycle, they estimate important parts of the benefits to the owner of the respective options.

5.9 Summary and Conclusions

The distributed service systems model is an important component of the overall risk/resiliency assessment process. It provides a structured method to examine the impact of an event on the assets that comprise a specific infrastructure and how they adapt over time to maintain as high as possible a level of service while full system capacity is restored. The methodology and data requirements have been developed in a manner that promotes transferability, focusing on generally available metrics, and acceptance of a wide range of precision. This allows decision-makers to base investment decisions on quantified estimates of the impact of the degradation in individual infrastructure systems. The example provided addresses a single system, electrical power. A complete assessment would address each of the four distributed infrastructure systems – power, water, wastewater, and emergency communications. Assessment of the individual infrastructures is a prerequisite for the system-of-systems model assessment described in Chapter Six.

CHAPTER 6

Analyzing Infrastructure Interdependency: The System-of-Systems Model

6.1 System-of-Systems Analysis for Assessing Infrastructure Interdependencies

Chapter Five presented Phase 3 of the Regional Resilience/Security Analysis Process (RR/SAP) for modeling the individual infrastructure service delivery systems on a regional scale. One conclusion was that, through the operations of modern SCADA systems and conscientious planning and engineering, some utilities experience considerably less service denial and associated revenue loss than might be estimated using only the static, facilities-based analysis in Phase 2. This chapter describes RR/SAP Phase 4 (*Figure 6.1*), the system-of-systems modeling that permits the assessment of the interactions among infrastructures as they depend on one another.

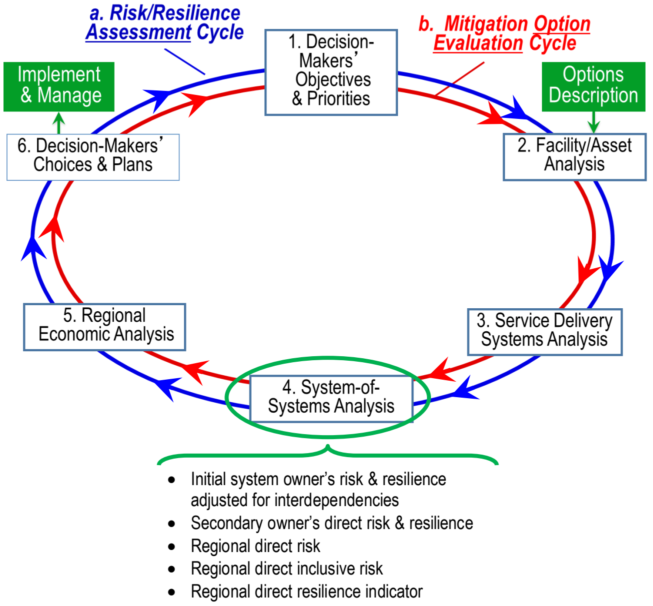


Figure 6.1 **RR/SAP Phase 4: System-of-Systems Analysis**

Where Phase 3 was directed toward identifying the specific impacted areas of the region and correcting the estimated service outages and revenue losses, Phase 4 examines the dependencies of one infrastructure on others. When mutual dependencies are located, the term, interdependencies, is used, although it has become popular to refer to any dependency of one infrastructure on another by this term as well. Because of the unique configurations of infrastructures and their SCADAs, generalizations about such interactions are rarely useful to decision-makers. There is simply no alternative to doing the analysis.

The objectives of Phase 4 analysis are to

1. Map the geographic area(s) impacted by a hazardous event both directly and through interactions with other infrastructures;
2. Estimate the duration and severity of service outages in each area and each infrastructure, making additional adjustments to the initial infrastructure's risk and resilience and estimating the *new* risk and resilience challenges to *other systems and organizations impacted by the location-specific outage*; and
3. Calculate the total direct *regional* risk and resilience and the total direct regional inclusive loss – the interim dollar loss plus the value of statistical lives and injuries.

These direct regional risks and resilience indicator levels are necessarily always incomplete because they can include only the systems that have been explicitly modeled. They will change, usually increasing but not always, with each additional system included in the system-of-systems model. The results of this analysis are the most comprehensive estimate of risk and resilience that can be tied directly back to specific pathways of events and asset or facility failures. It is at this level that the *regional* (as opposed to system-specific) decision-makers can evaluate the acceptability of the security and resilience situation and set priorities for evaluating options. Chapter Nine presents the approach for estimating the total regional loss, both direct and indirect, as well as other key economic metrics.

6.2 Basic Concept

Distributed infrastructure delivery systems are usually dependent upon one another. They are linked together at points of intersection where an asset in one infrastructure is a consumer of the service delivered by another infrastructure. Identifying intersections between consumer infrastructure assets and provider infrastructure services is key to assessing the potential for cascading infrastructure failures that lead to rapid transition from the right hand end of the continuum of regional activity to points on the left hand end of the continuum as illustrated earlier, in *Figure 5.2*.

Prior to the proliferation of SCADA systems and the implementation of grid management concepts, the critical intersections between infrastructure consumer and infrastructure provider were identified via an overlay methodology in which the intersections were identified by laying out the service line locations of the provider infrastructure and overlaying the asset locations of the consumer infrastructure. As an example, a customer infrastructure – say, wastewater service – is dependent on a provider infrastructure – say, electrical power – to support lift station and treatment plant operations. In frame one of *Figure 6.2*, the wastewater system functionality is presented in schematic form. In frame two, the interdependency between the wastewater service system and the electrical power system is illustrated. In frame three, the potential for a single-tier or a multi-tier cascading failure is illustrated by a failure at one or both of the electrical power substations involved in the depicted wastewater service schematic.

The system-of-systems methodology recognizes that the interdependency between infrastructures can generate a set of unforeseen consequences that accelerate breakdown in regional patterns of life and economic activity

A single-tier cascading failure occurs when there is a failure at the substation or in one of the in-line electrical power service delivery assets that serve the lift station. A multi-tier cascading failure occurs when there is a failure at the substation or in one of the in-line electrical power service assets that services the wastewater treatment plant. Failure at the wastewater treatment plant generates a multi-line breakdown in service that may affect a specific area, a sub-region, or the region as a whole, as well as the performance of assets that are parts of infrastructures (frame three), depending on the system design for resiliency and the duration of the electrical power failure.

While the example was shown as a simple intersection of service lines at a common point, the proliferation of SCADA systems and the associated advanced ability to operate infrastructures on a grid basis, as opposed to a line basis, make identification of critical points of intersection a more complex process requiring a methodology and modeling approach that supports assessment of grid-asset interaction.

Within the RR/SAP, the grid-asset interaction assessment is accomplished using a methodology and a tool set developed by Alion Science and Technology. The methodology has been developed over the past five years providing a transferrable method to rapidly outline and model the performance of infrastructure systems on an independent basis, as illustrated in Chapter Five, using the systems modeling methodology and on an interdependent basis as illustrated in this chapter using the system-of-systems methodology. The system-of-systems methodology recognizes that the interdependency between infrastructures can generate a set of unforeseen consequences that accelerate

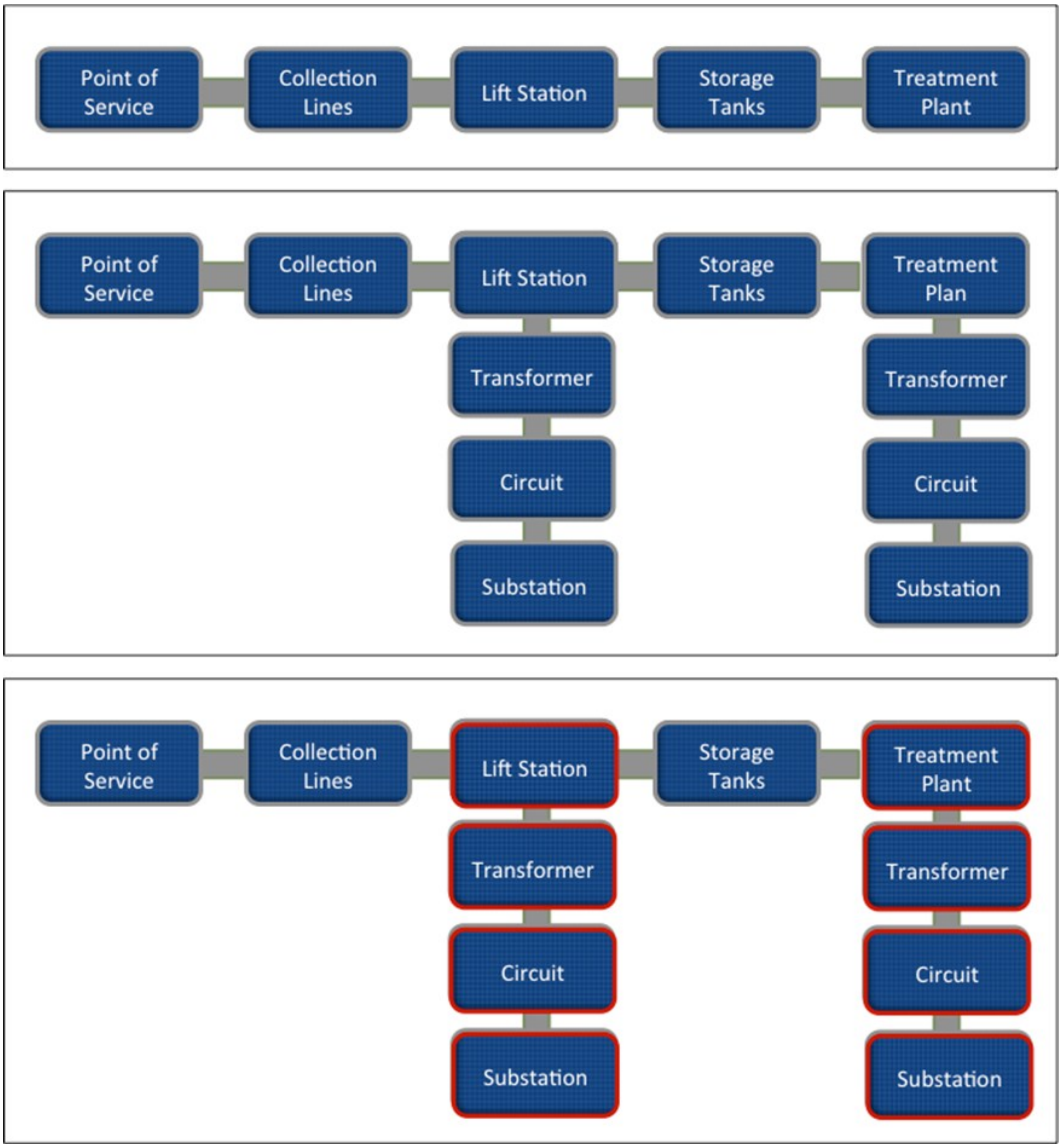


Figure 6.2 **Infrastructure Interdependency and Potential for Cascading Failures**

breakdown in regional patterns of life and economic activity due to stress on infrastructure caused by natural or man-made events.

As identified in Chapter Five, the link between infrastructure performance and regional activity is delivered level of service (LOS) across the foundational infrastructures considered in this study. These infrastructures include electrical power, water, wastewater, emergency communications, and transportation. Each individual system is evaluated in the post-event environment to determine a LOS that indicates, on a scale of 0.0 to 1.0, the ability of the system to independently balance supply and demand given event-related damage or destruction of critical assets. This chapter presents the method used to evaluate the impact of a reduced LOS in one infrastructure (provider infrastructure) on the LOS of another infrastructure (consumer infrastructure). This methodology employs a system-of-systems model capable of mapping and tracking the many-to-many grid-asset intersections that comprise a complex set of infrastructure relationships.

The system-of-systems model generates an LOS for each infrastructure using an iterative solution process that runs multiple, computationally interleaved solution strands. The primary strand is LOS assessment based on event-driven asset degradation and recovery profiles. The systems model generates a time-sequenced assessment of the LOS for each system considering overall system capacity, individual asset contributions to capacity, the post-event recovery profile of individual assets, and the ability of system control functions to overcome asset degradation or destruction via implementation of alternate load distribution plans and delivery paths.

The secondary solution strands are driven by the generation of a secondary asset degradation and recovery profile that reflects the asset performance impact of the failure or degradation of another infrastructure system. The system-of-systems model walks through the time-sequenced LOS estimates updating them as required based on the interdependency influence. The system-of-systems model publishes the revised post-event LOS map for each infrastructure included in the assessment. This model recognizes that LOS distribution will be differentially distributed throughout the region and that the patterns will change over time as assets are brought back into service through asset repair, restoration of services by another infrastructure, and revision to control-function load balance and alternate path selection schemes. The model provides spatial and temporal LOS forecasts for the 30-day period following an event. LOS output values from the system model support economic impact assessment including lost revenue to the service provider and lost productivity to the customer.

The system-of-systems methodology views the interdependency as intersections between the supply of service from one infrastructure (provider) and demands for that service by an asset within another infrastructure (consumer). In effect, the infrastructures are integrated in layers as illustrated in the adaptation of a Venn diagram shown in *Figure 6.3*. Degree of dependency is represented by overlap of one infrastructure with another. In this case, all infrastructures are dependent upon electrical power at various degrees. In the example, there is overlap between electrical power and water, electrical power and wastewater, electrical power and emergency communications, and electrical power and transportation, and, of course water supply with wastewater. There is no overlap between secondary tier infrastructures although; there can be in certain infrastructure configurations. In this case, the relationships with the tier one infrastructure (electrical power) and the tier two infrastructures (water, wastewater, emergency communications, and transportation) are secondary strands. Interactions between second tier infrastructures (water and wastewater) are considered tertiary

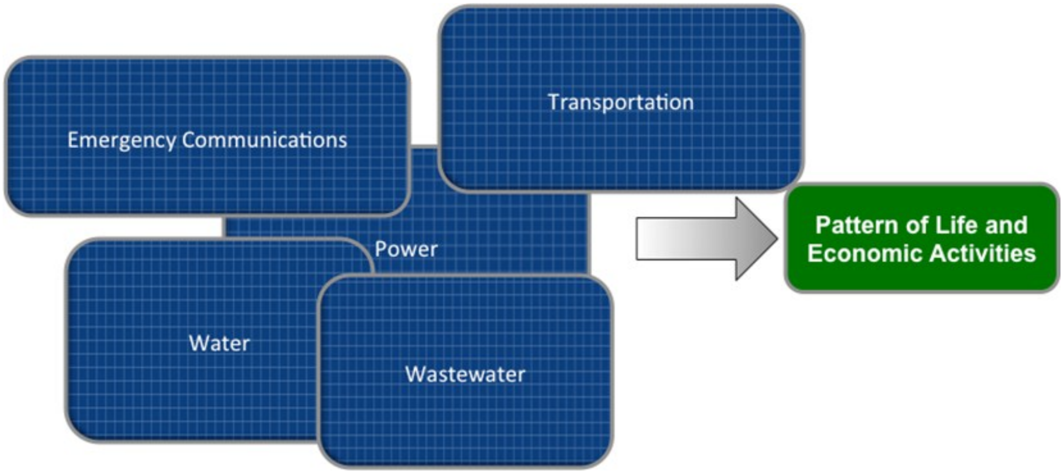


Figure 6.3 **Interaction between Infrastructures - Supports Pattern of Life and Economic Activities**

strands. In cases where there are additional tiers, order of precedence flows from the bottom up.

Every region examined will have a different interdependency intersection diagram that reflects the connections between infrastructures and the relative degree of the dependencies. *Figure 6.3* indicates that the ability for a region to conduct a specific level of activity is dependent upon the performance of the system of infrastructures individually and collectively. The methodology discussed in this chapter pertains to the primary and secondary strands with the exception of transportation. Transportation, because of the unique modeling approach employed, is addressed separately in Chapter Seven.

6.3 Principles of the Methodology

The system-of-systems assessment methodology is a cause-and-effect-based approach in which cause and effect are shared elements in a simultaneous, time-sequenced, multi-strand solution estimation environment. The method is based on the same principles as stated in Chapter Five, with the additions of the following:

- Principle Five — An LOS degradation of one infrastructure in a particular location may invoke a performance degradation and recovery profile on the physical assets or control functions of another infrastructure.
- Principle Six — A provider-consumer relationship can be defined between infrastructures that provide direct service to other, "consumer" infrastructures in enough detail to support assessment of the influence of the provider LOS degradation on the consumer LOS and that this relationship can be quantified over time by incrementally assessing the provider-consumer pair over the entire period of assessment.

6.4 Multi-Strand Cause and Effect Modeling

Modeling the multi-strand cause and effect phenomena associated with infrastructure interdependency requires use of discrete event techniques that are based on a cyclical assessment concept as illustrated in *Figure 6.4*. The technique is based on definition of a distinct time-step that governs the tempo of the model and the granularity of its outputs. Shorter time-steps provide increased granularity but require robust data streams and significant computing power. Longer time-steps may be inadequate because significant but short duration perturbations in performance in one or more interleaved solution strands may go undetected and a significant consequence of interdependency may not be discovered through the course of the assessment. Time-steps can range from hours to days depending on the purpose of the assessment and the granularity of the input data.

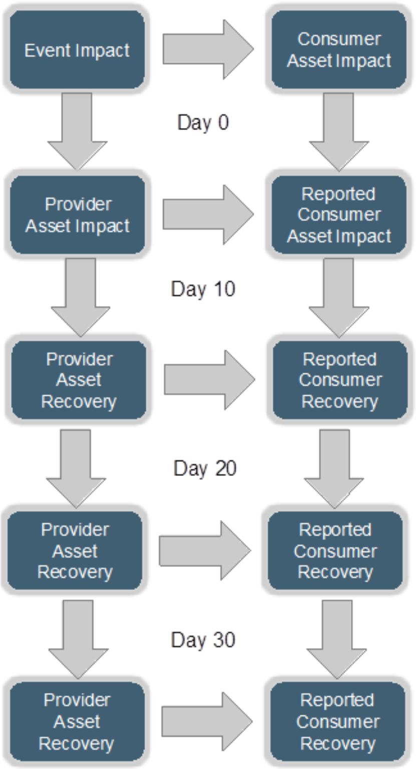
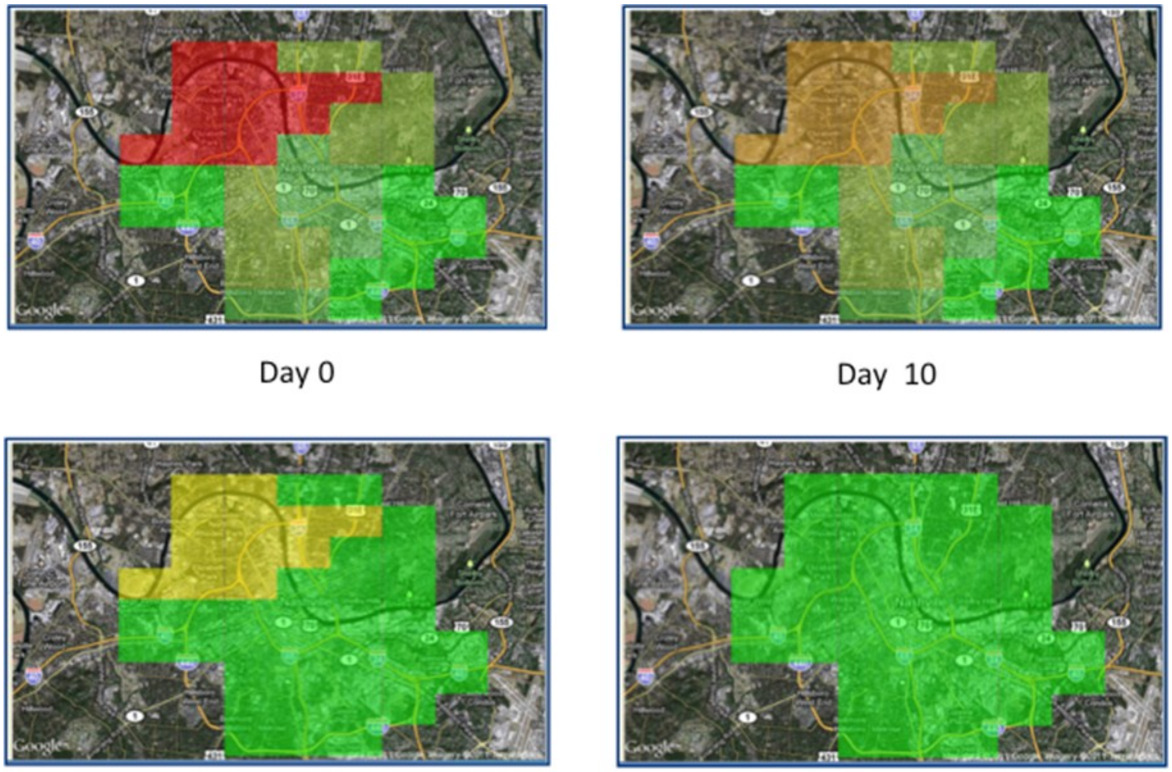


Figure 6.4 **The Multi-strand Solution Schema Showing a 10-day Reporting Interval**



Day 0

Day 10

Day 20

Day 30

Figure 6.5 **Electric Power Performance after the Example Toxic Gas Spill**

As a guide, the minimum practical time-step is controlled by the data associated with the primary strand. Data for secondary strands should be generated at integer value multiples of the governing primary strand time-step. For example a 5-day primary strand time-step can support secondary strand time-step values of 5, 10, or 15 days, etc. For some simulations, a variable time-step may be used with shorter time-steps employed during the most dynamic periods immediately following an event. The time-step used in this study was 5 days for each of the strands assessed. The multi-strand assessment schema used is shown in *Figure 6.4*. The schema indicates a 10-day interval between reports. The 10-day interval was used to simplify the output for presentation.

6.5 Precedence within the Multi-Strand, System-of-Systems Model

As in Chapter Five, the illustrative scenario to support the study is a HAZMAT event that takes place at 9:00 AM on a Wednesday in the spring. The case is a chlorine spill of approximately ten tons in the southeastern corner of Grid C-4. The resulting toxic gas plume is carried by prevailing southwesterly winds generating an area impact pattern as shown in *Figure 6.5*, as impacts on the electric power system over 30 days (repeated from Chapter Five). A total of nine grid zones are impacted encumbering approximately 15 square miles and affecting numerous critical infrastructure assets related to the electrical power system, the water system, and the wastewater system.

Selection of the secondary strand precedence for application of the system-of-systems model follows the order of precedence protocol identified in a Section 6.2. Dependencies with equal tier values, as determined by the technique illustrated in *Figure 6.6*, ordered an assessment based on severity of LOS impact identified in application of the system model.

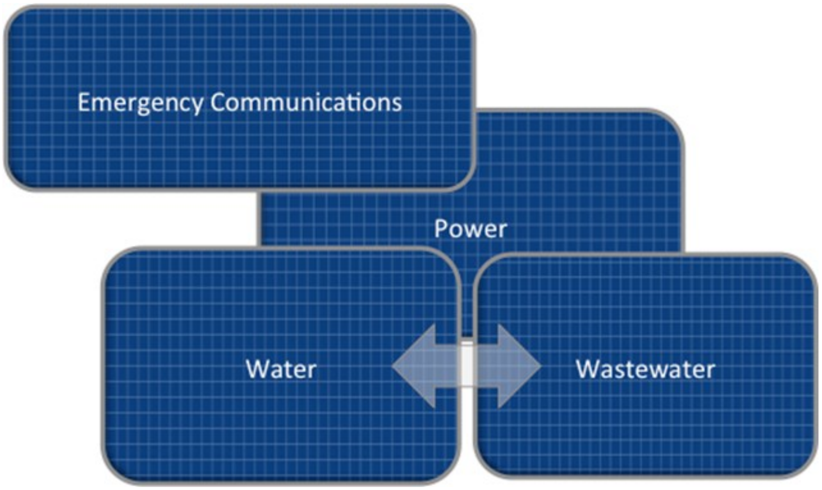


Figure 6.6 **System Dependency Precedence Model**

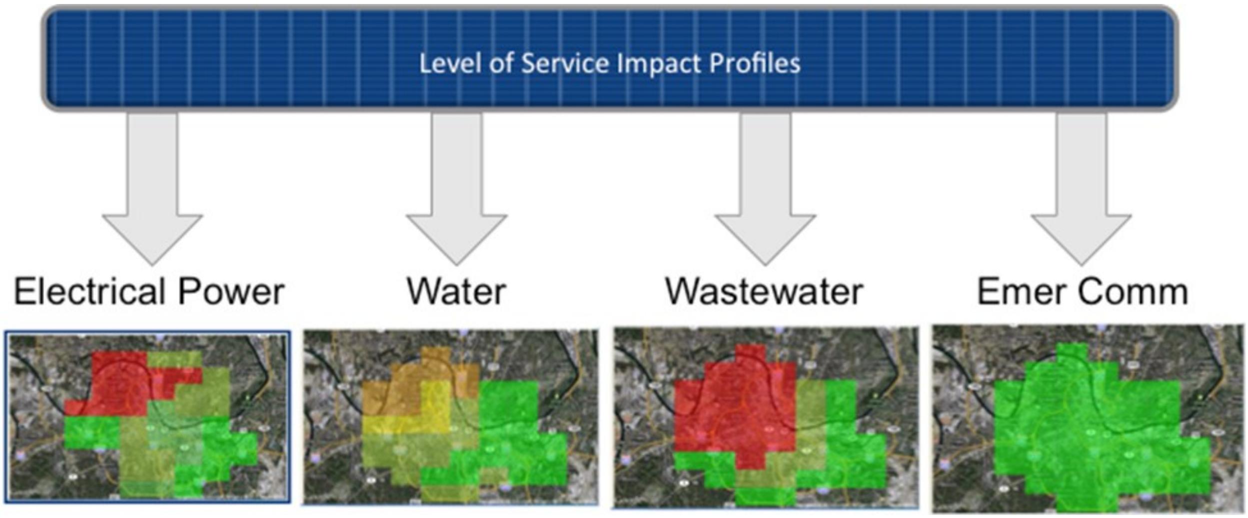


Figure 6.7 **System Model LOS Impact - Independent System Assessment**

The diagram indicates dependencies at the second and third tiers. Water, wastewater, and emergency communications have a second tier LOS dependency on electrical power. Water has a third tier capacity balance dependency with wastewater as indicated by the bi-directional arrow. Precedence within the second tier requires input from the system model assessment of the event impact on water, wastewater, and emergency communications. The assessment indicates order of LOS degradation severity from highest to lowest is wastewater, water, and emergency communications as illustrated in *Figure 6.7*, based on the area of lowest LOS. Based on this assessment, wastewater dependency on electrical power is selected as the first precedence for secondary strand assessment. Water dependency on electrical power is selected as the second precedence for secondary strand assessment. Wastewater dependency on water is selected as the first precedence for tertiary strand assessment.

6.6 Application of the Grid-Asset Intersection Method

Assessing the impact of distributed system LOS degradation requires an approach that accommodates the incredible agility that operators have given the capability of modern SCADA. In effect, modern distributed systems operate as grids such that the failure of one or more assets may be completely masked by the ability to redistribute load to alternate sources and reroute delivery along alternate paths. This situation requires an update to traditional fault tree-based dependency evaluations that rely on identification of points of intersection between provider infrastructure lines and consumer infrastructure assets. The simpler approach is still appropriate for systems that have a more "root-and-branch" architecture, but, in the modern era, the model shifts to one that searches for the intersection of provider-infrastructure grid service zones and points of consumer infrastructure asset demand.

6.6.1 Establishing Grid Performance

Establishing grid performance for the provider infrastructure is accomplished within the system model in the case of a tier one provider infrastructure or the system-of-systems model in the case of a tier two or higher provider infrastructure. The LOS distribution map for each time-step is generated and used as a backdrop for assessing the LOS realized by each consumer infrastructure asset. *Figure 6.8* illustrates this concept as employed within this study in which each consumer infrastructure asset is tested for location on the provider infrastructure grid.

6.6.2 Determining the Impact over Time

Consumer infrastructure assets affected by the degraded provider infrastructure LOS are identified and then tested at each time-step to determine the level of asset degradation. The testing procedure is illustrated conceptually in *Figures 6.9 – 6.12* in the four time-sequenced diagrams that relate electrical power LOS to the degradation of lift stations 3 and 5 (the control center and the treatment plant are sustainable on backup power). The diagrams have been de-cluttered removing the assets not affected or those that suffered event-driven impacts that exceed the dependency degradation in both severity and duration.

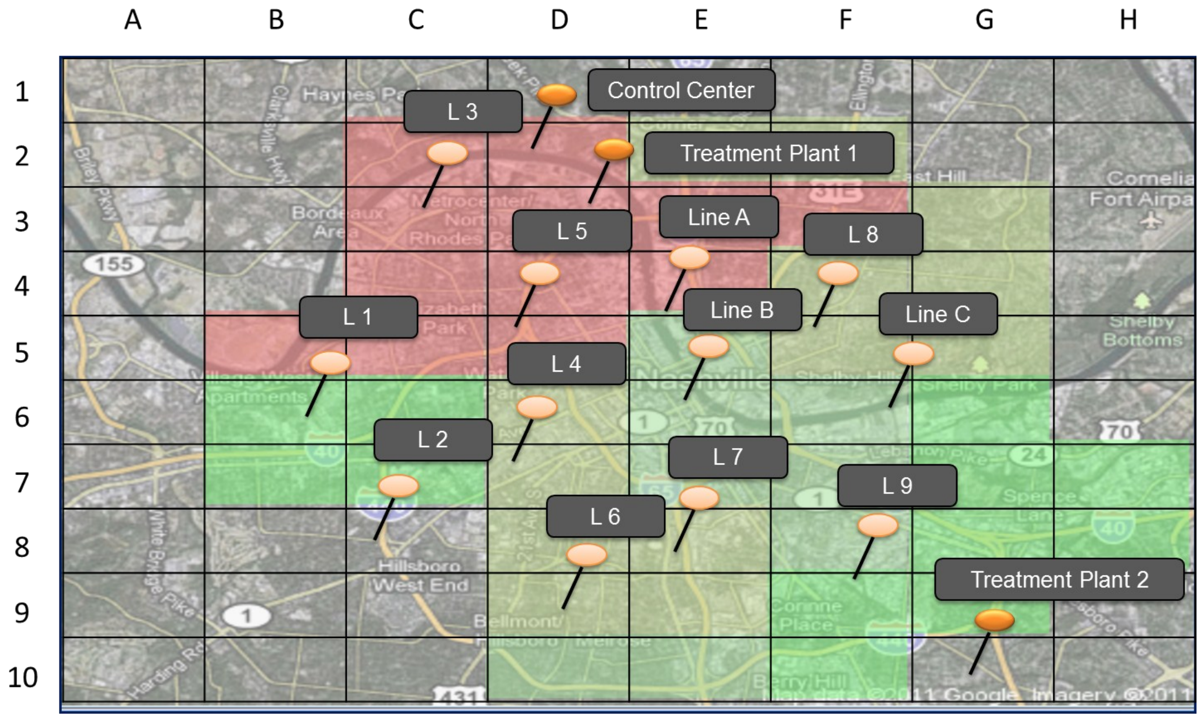
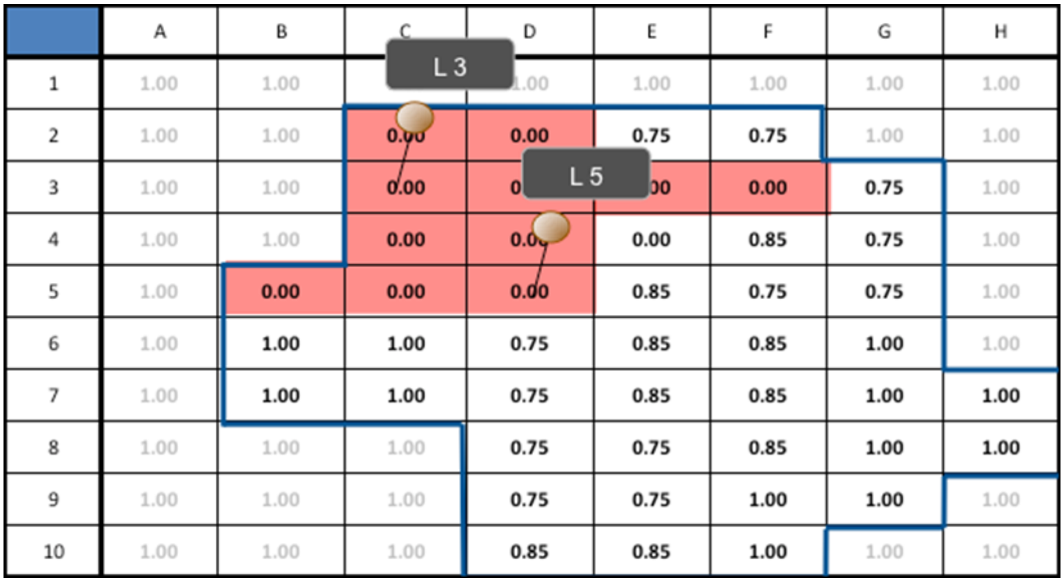
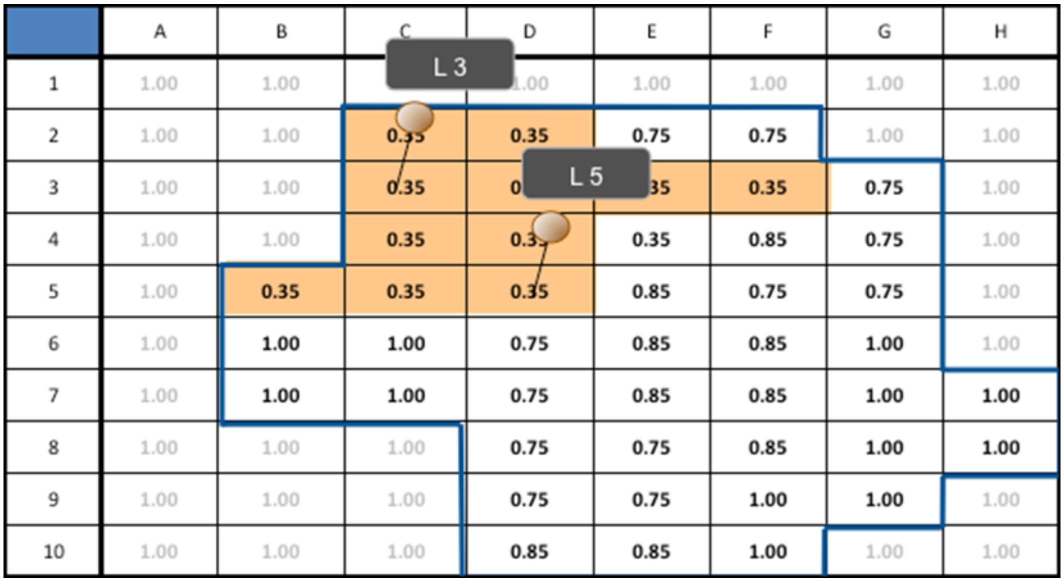


Figure 6.8 **Illustration of the Grid-Asset Intersection Assessment Method**



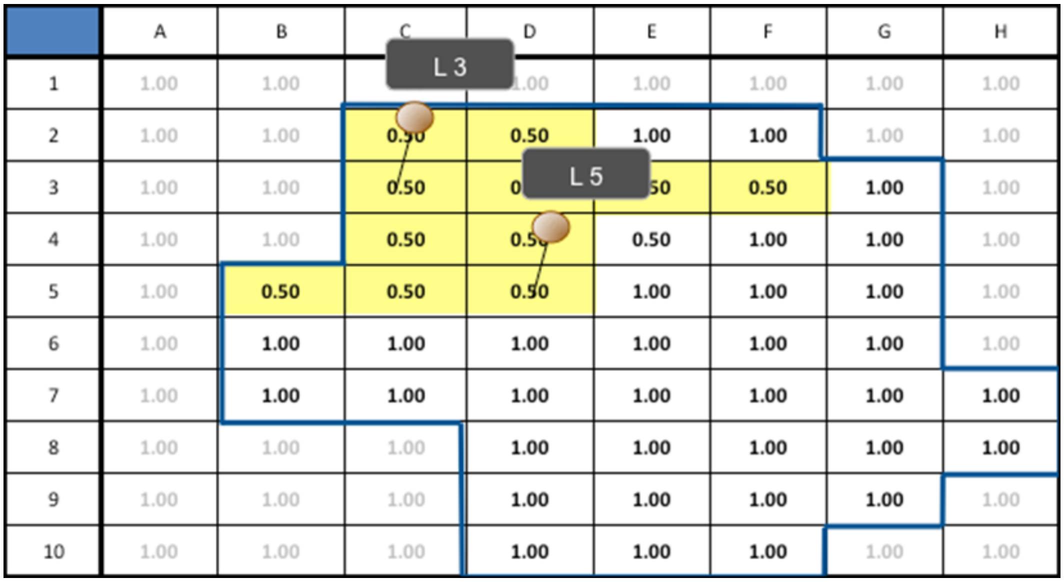
	A	B	C	D	E	F	G	H
1	1.00	1.00		1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	0.00	0.00	0.75	0.75	1.00	1.00
3	1.00	1.00	0.00	0	00	0.00	0.75	1.00
4	1.00	1.00	0.00	0.0	0.00	0.85	0.75	1.00
5	1.00	0.00	0.00	0.00	0.85	0.75	0.75	1.00
6	1.00	1.00	1.00	0.75	0.85	0.85	1.00	1.00
7	1.00	1.00	1.00	0.75	0.85	0.85	1.00	1.00
8	1.00	1.00	1.00	0.75	0.75	0.85	1.00	1.00
9	1.00	1.00	1.00	0.75	0.75	1.00	1.00	1.00
10	1.00	1.00	1.00	0.85	0.85	1.00	1.00	1.00

Figure 6.9 **Day 1-10 Electrical Grid LOS Influence on Wastewater Assets**



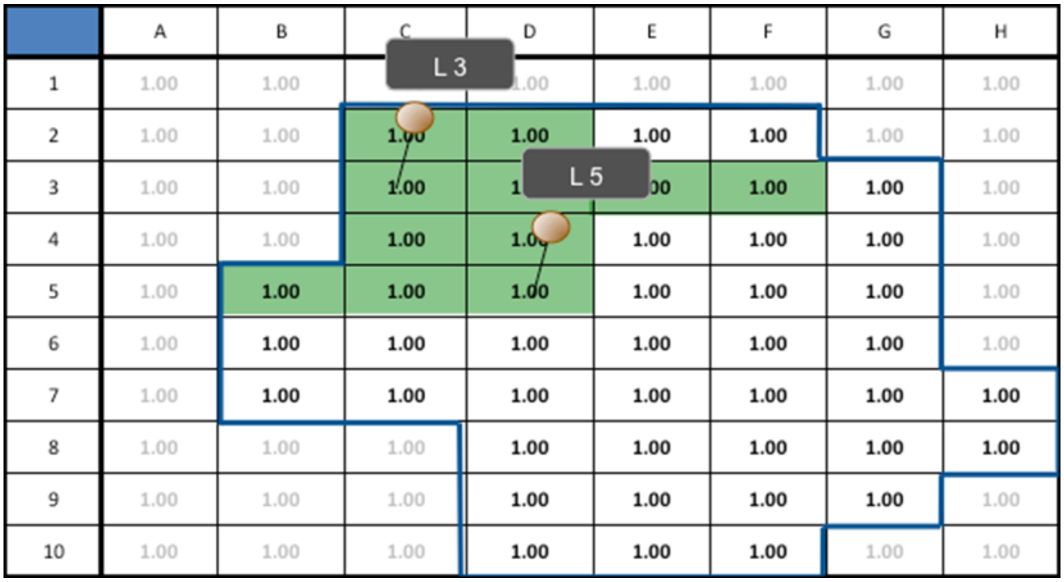
	A	B	C	D	E	F	G	H
1	1.00	1.00		1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	0.35	0.35	0.75	0.75	1.00	1.00
3	1.00	1.00	0.35	0	35	0.35	0.75	1.00
4	1.00	1.00	0.35	0.3	0.35	0.85	0.75	1.00
5	1.00	0.35	0.35	0.35	0.85	0.75	0.75	1.00
6	1.00	1.00	1.00	0.75	0.85	0.85	1.00	1.00
7	1.00	1.00	1.00	0.75	0.85	0.85	1.00	1.00
8	1.00	1.00	1.00	0.75	0.75	0.85	1.00	1.00
9	1.00	1.00	1.00	0.75	0.75	1.00	1.00	1.00
10	1.00	1.00	1.00	0.85	0.85	1.00	1.00	1.00

Figure 6.10 **Day 11-20 Electrical Grid LOS Influence on Wastewater Assets**



	A	B	C	D	E	F	G	H
1	1.00	1.00		1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	0.50	0.50	1.00	1.00	1.00	1.00
3	1.00	1.00	0.50	0	50	0.50	1.00	1.00
4	1.00	1.00	0.50	0.50	0.50	1.00	1.00	1.00
5	1.00	0.50	0.50	0.50	1.00	1.00	1.00	1.00
6	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Figure 6.11 **Day 21-30 Electrical Grid LOS Influence on Wastewater Assets**



	A	B	C	D	E	F	G	H
1	1.00	1.00		1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	1.00	1.00	1.00	1	00	1.00	1.00	1.00
4	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
5	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
6	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Figure 6.12 **Day 31+ Electrical Grid LOS Influence on Wastewater Assets**

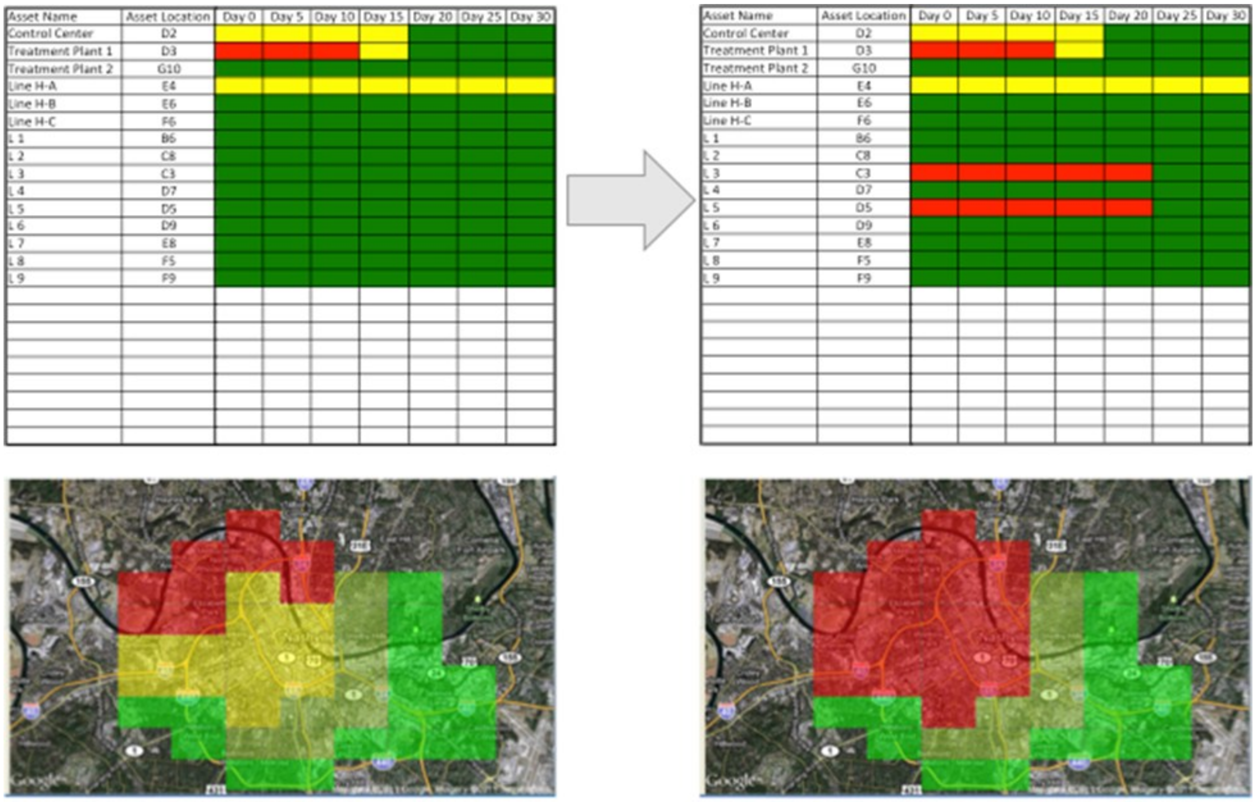
6.6.3 Generating Asset Performance Profiles Based on Dependency

Once the affected assets are identified and the time-step associated degradation levels are determined, the asset degradation profile is updated to serve as the interactive data set for reference during system-of-systems simulations. *Figure 6.13* displays the update to the profile for the wastewater utility assets. On the left is the simulation without the dependencies, with the Gantt chart showing which assets are compromised (yellow) or fully inoperable (red) for the lengths of time and the map showing the geographic areas affected. On the right are the same charts repeated, but for a simulation with the full effects of the dependencies in effect. The impact of including the dependencies is that a significantly larger area suffers total outage as two lift stations are without power to operate. This illustrates the necessity of updating the estimates made in Phase 3 in the system-of-systems model of Phase 4.

6.7 Estimation of the Economic Impact to the Service Provider

Estimating the economic impact on the service provider in the system-of-systems model requires implementation of the discrete event methodology within a modeling framework capable of running the primary and secondary strand simulations as well as being capable of interleaving the results of the simulations such that a time-sequenced interdependency-influenced LOS distribution is generated. As identified in Section 6.4, for the purpose of this example, there are three interdependencies that require examination.

Figure 6.13 **Example of a Revised Asset Performance Profile and the Impact on LOS**[16]



Asset Name	Asset Location	Day 0	Day 5	Day 10	Day 15	Day 20	Day 25	Day 30
Control Center	D2	🟨	🟨	🟨	🟨	🟩	🟩	🟩
Treatment Plant 1	D3	🟥	🟥	🟥	🟨	🟩	🟩	🟩
Treatment Plant 2	G10	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Line H-A	E4	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Line H-B	E6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Line H-C	F6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 1	B6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 2	C8	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 3	C3	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 4	D7	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 5	D5	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 6	D9	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 7	E8	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 8	F5	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 9	F9	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Asset Name	Asset Location	Day 0	Day 5	Day 10	Day 15	Day 20	Day 25	Day 30
Control Center	D2	🟨	🟨	🟨	🟨	🟩	🟩	🟩
Treatment Plant 1	D3	🟥	🟥	🟥	🟨	🟩	🟩	🟩
Treatment Plant 2	G10	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Line H-A	E4	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Line H-B	E6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Line H-C	F6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 1	B6	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 2	C8	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 3	C3	🟥	🟥	🟥	🟥	🟥	🟩	🟩
L 4	D7	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 5	D5	🟥	🟥	🟥	🟥	🟥	🟩	🟩
L 6	D9	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 7	E8	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 8	F5	🟩	🟩	🟩	🟩	🟩	🟩	🟩
L 9	F9	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Day 10

Day 10

---

[16] For illustrative purposes only to display the Gantt chart timeline recovery of the assets, not the asset list itself.

The first is wastewater dependency on electrical power. The second is water dependency on electrical power. The third is wastewater dependency on water. The time horizon for all runs is 30 days, with computations run on a 5-day interval and reports generated on a 10-day interval.

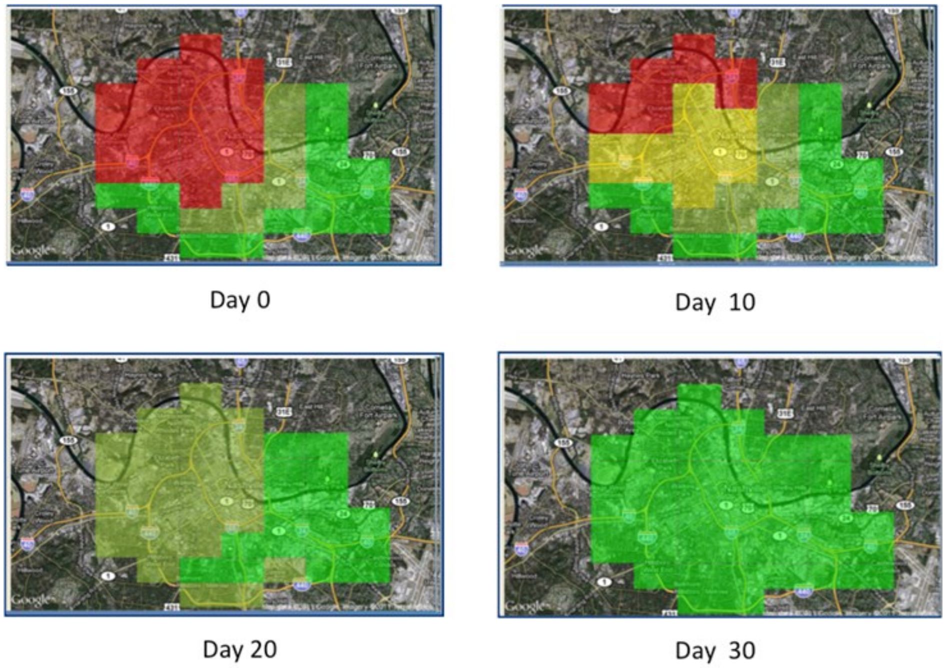
6.7.1 Case 1 – The Wastewater System

The event impact on wastewater LOS distribution was run in the independent and interdependent modes to support the assignment of value to operator revenue losses. The independent mode considers only the event-driven asset damage and destruction for the subject infrastructure. The interdependent mode considers the event-driven damage and the provider infrastructure service delivery degradation that influences asset performance within the consumer infrastructure. *Figures 6.14* and *6.15* show the LOS distribution output from the system over the 30-day period following the event both under independent system evaluation and under interdependent system-of-systems evaluation. The difference in the rate of restoration of service is driven by the outage at electrical power substation 4 which provides primary power to wastewater lift stations 3 and 5. These images are generated by digital estimates of LOS that provide the basis for computing an expected revenue loss by the system operator and the regional economic loss.

Wastewater Operator Revenue Loss – Independent Analysis

Step 1: Generate the Revenue Distribution Matrix – The wastewater system revenue distribution matrix used in this study is shown in *Figure 6.16*. The total revenue is normalized to a value of 10.0, so, for example, Cell A1 contributes 0.5 percent of the total revenue. Cell revenue assignments represent the portion of the average daily revenue that is attributed to the customer base within that cell. The values shown are representative of those that can be generated based on publicly available density and land use data and residential and commercial utility rates. The values are subject to refinement by the service provider as true cell-by-cell values are identified and substituted.

Figure 6.14 **Wastewater LOS Distribution over a 30-Day Period – Independent Assessment**



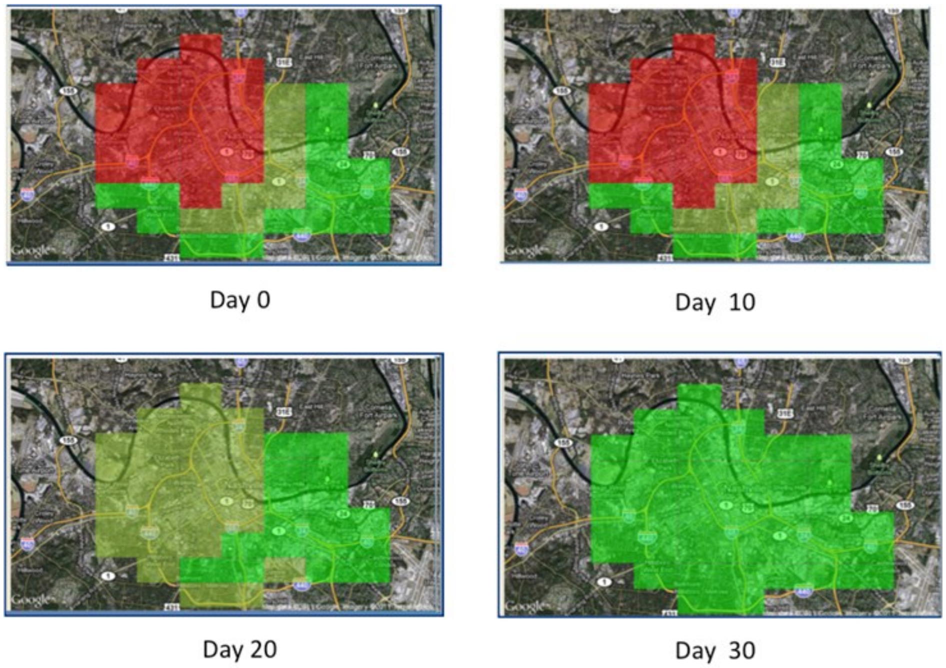
Day 0

Day 10

Day 20

Day 30

Figure 6.15 **Wastewater LOS Distribution over a 30-Day Period – Electrical Power Dependency**

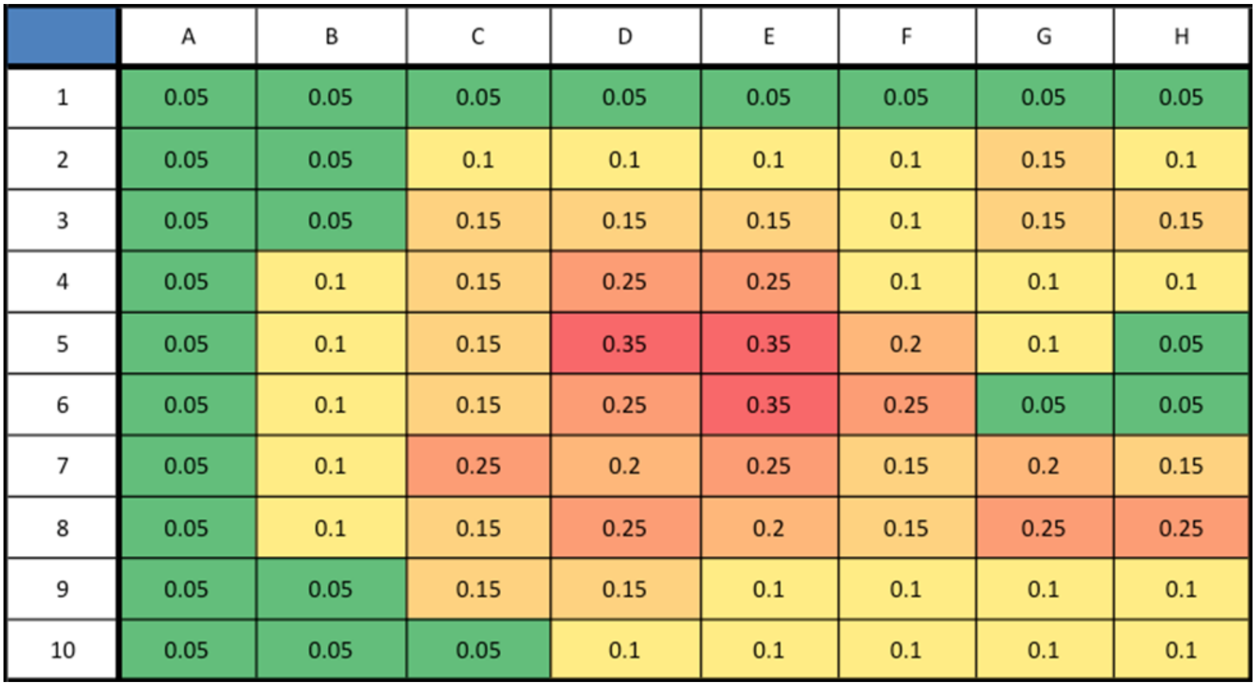


Day 0

Day 10

Day 20

Day 30



	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.1	0.1	0.1	0.1	0.15	0.1
3	0.05	0.05	0.15	0.15	0.15	0.1	0.15	0.15
4	0.05	0.1	0.15	0.25	0.25	0.1	0.1	0.1
5	0.05	0.1	0.15	0.35	0.35	0.2	0.1	0.05
6	0.05	0.1	0.15	0.25	0.35	0.25	0.05	0.05
7	0.05	0.1	0.25	0.2	0.25	0.15	0.2	0.15
8	0.05	0.1	0.15	0.25	0.2	0.15	0.25	0.25
9	0.05	0.05	0.15	0.15	0.1	0.1	0.1	0.1
10	0.05	0.05	0.05	0.1	0.1	0.1	0.1	0.1

Figure 6.16 **The Revenue Distribution Matrix for the Wastewater Utility**

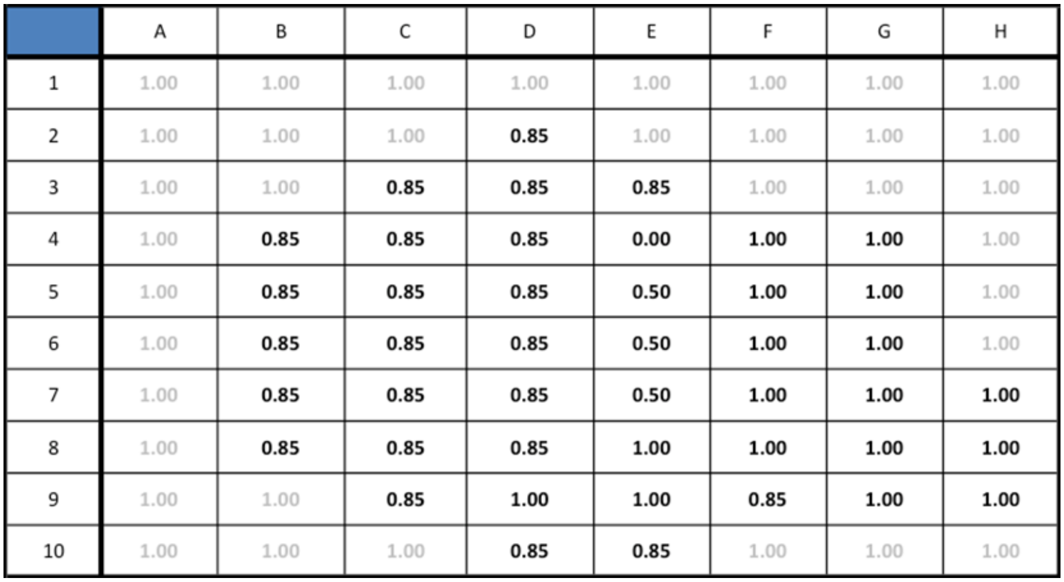
Step 2: Generate the Time-step-by-Time-step LOS Matrix – The wastewater LOS profile generated by the systems model is shown in *Figures 6.17* through *6.20* as matrices that provide the cell-by-cell, time-step-by-time-step LOS values. Values in bold represent the event-responsive area within the region.

	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.00**	**0.00**	**0.00**	1.00	1.00	1.00
4	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
5	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
6	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
7	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00

Figure 6.17 **Day 1-10 LOS Distribution – Wastewater – Independent LOS Distribution Impact**

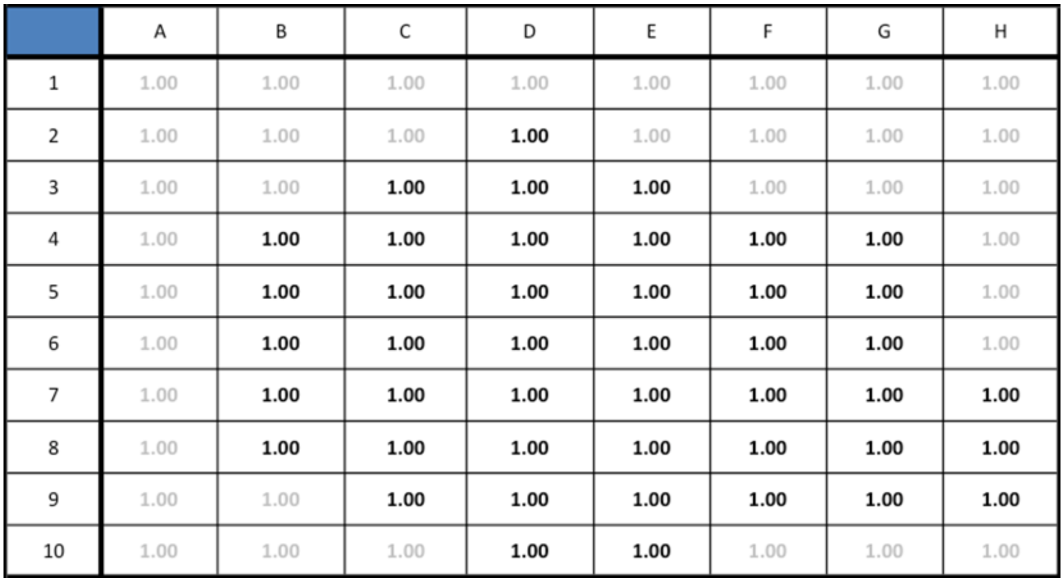
	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.00**	**0.00**	**0.00**	1.00	1.00	1.00
4	1.00	**0.00**	**0.00**	**0.50**	**0.00**	**0.75**	**1.00**	1.00
5	1.00	**0.00**	**0.00**	**0.50**	**0.50**	**0.75**	**1.00**	1.00
6	1.00	**0.50**	**0.50**	**0.50**	**0.50**	**0.75**	**1.00**	1.00
7	1.00	**0.50**	**0.50**	**0.50**	**0.50**	**0.75**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**0.50**	**0.00**	**0.75**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00

Figure 6.18 **Day 11-20 LOS Distribution – Wastewater – Independent LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.85**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.85**	**0.85**	**0.85**	1.00	1.00	1.00
4	1.00	**0.85**	**0.85**	**0.85**	**0.00**	**1.00**	**1.00**	1.00
5	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	1.00
7	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.19 **Day 21-30 LOS Distribution – Wastewater – Independent LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**1.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**1.00**	**1.00**	**1.00**	1.00	1.00	1.00
4	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
5	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
6	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
7	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00

Figure 6.20 **Day 31+ LOS Distribution – Wastewater – Independent LOS Distribution Impact**

Step 3: Generate the Revenue Profile – The wastewater service revenue profile is generated by incrementally computing the realized revenue over the recovery time period. The average daily revenue value used in the assessment is $1,250,985. Total realized revenue is computed by integrating over the 30-day period. Revenue loss is found as the difference between expected revenue and forecast revenue.

The total revenue loss is computed incrementally by time-step period computing and then summing the losses experienced during each time-step. *Table 6.1* identifies the total revenue loss over the entire period as approximately 30% of Expected Revenue.

Wastewater Revenue Loss – Dependency Analysis (Electrical Power)

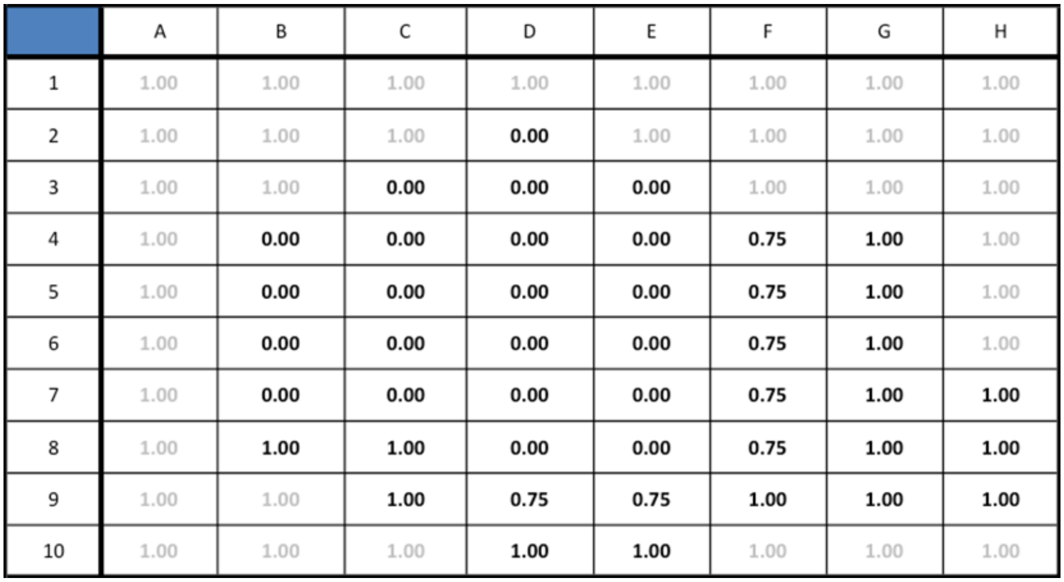
Step 1: Generate the Revenue Distribution Matrix – Same as in *Figure 6.16*.

Step 2: Generate the Time-step-by-Time-step LOS Matrix – The wastewater LOS profile shown in *Figures 6.22* through *6.25* provide the cell-by-cell, time-step-by-time-step LOS values based on dependency on electrical power. As above, values in bold represent the event-responsive area within the region.

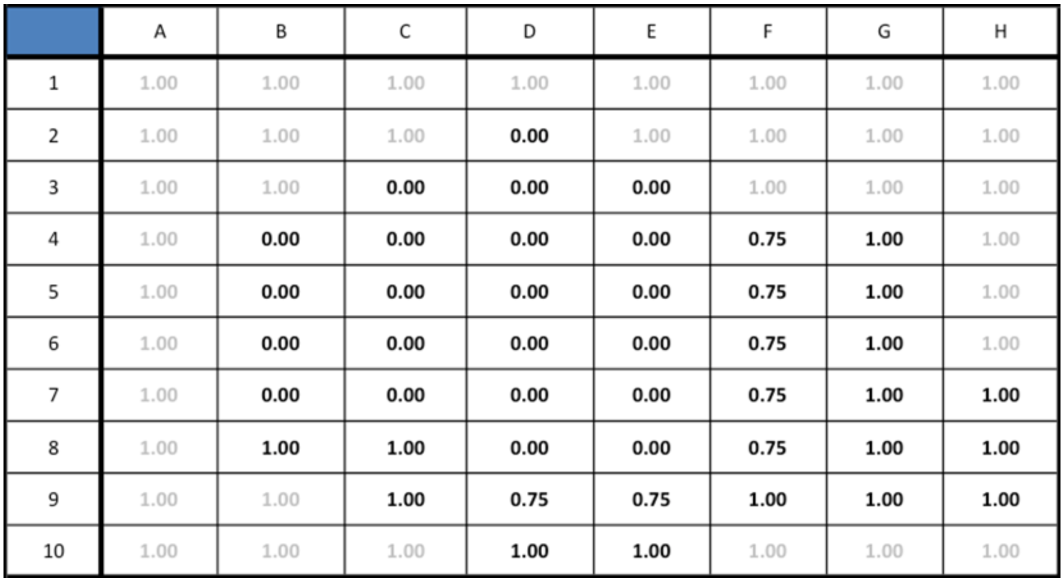
Table 6.1 **Wastewater Revenue Loss under Independent System Evaluation**

Revenue Loss Model - 30-Day Assessment		
Average Daily Revenue (System Wide)		$1,250,985
Day 0-10 Daily Revenue Loss		$578,581
Day 11-20 Daily Revenue Loss		$400,315
Day 21-30 Daily Revenue Loss		$159,188
Total Expected Revenue		$37,529,550
Total Realized Revenue		$26,148,714
Total Revenue Loss		**$11,380,836**

Figure 6.21 **Day 1-10 Wastewater – Interdependent (Electrical Power) LOS Distribution Impact**

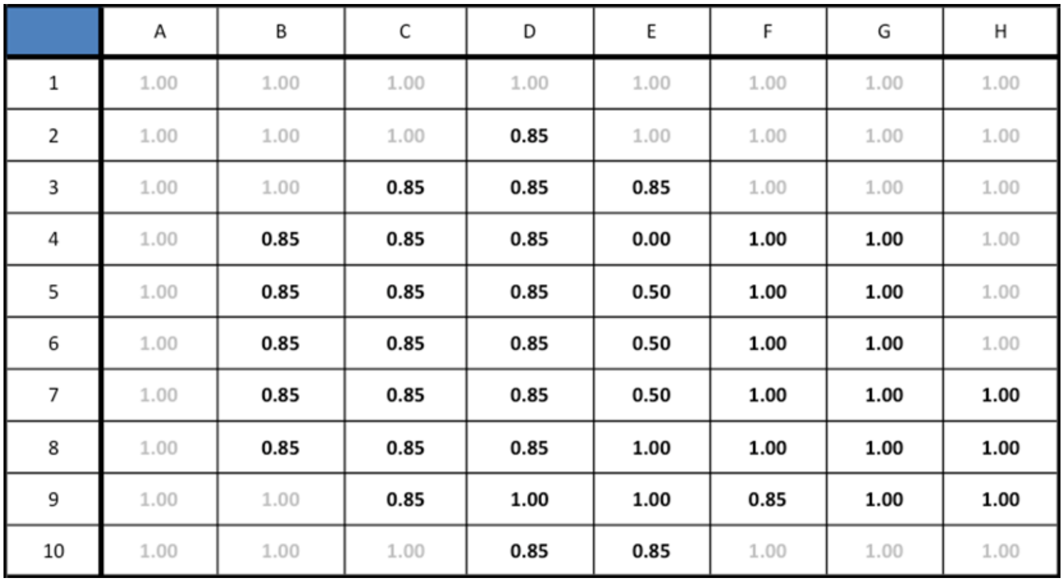


	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.00**	**0.00**	**0.00**	1.00	1.00	1.00
4	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
5	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
6	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
7	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00



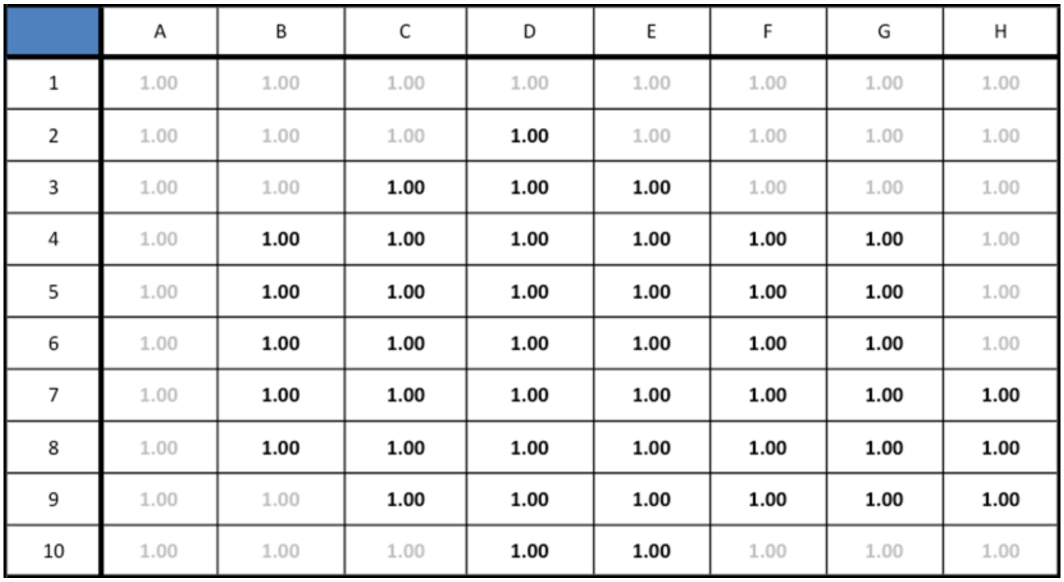
	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.00**	**0.00**	**0.00**	1.00	1.00	1.00
4	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
5	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
6	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	1.00
7	1.00	**0.00**	**0.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**0.00**	**0.00**	**0.75**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00

Figure 6.22 **Day 11-20 Wastewater – Interdependent (Electrical Power) LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.85**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.85**	**0.85**	**0.85**	1.00	1.00	1.00
4	1.00	**0.85**	**0.85**	**0.85**	**0.00**	**1.00**	**1.00**	1.00
5	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	1.00
7	1.00	**0.85**	**0.85**	**0.85**	**0.50**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.23 **Day 21-30 Wastewater – Interdependent (Electrical Power) LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**1.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**1.00**	**1.00**	**1.00**	1.00	1.00	1.00
4	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
5	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
6	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	1.00
7	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
8	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
10	1.00	1.00	1.00	**1.00**	**1.00**	1.00	1.00	1.00

Figure 6.24 **Day 31+ Wastewater – Interdependent (Electrical Power) LOS Distribution Impact**

Step 3: Generate the Revenue Profile – The wastewater service revenue profile is generated by incrementally computing the realized revenue over the recovery time period. The same average daily revenue value used in the assessment is $1,250,985. Total realized revenue is computed by integrating over the 30-day period. Revenue loss is found as the difference between expected revenue and forecast revenue.

The total revenue loss is computed incrementally by time-step period computing and then summing the losses experienced during each time-step. *Table 6.2* identifies the total revenue loss over the entire period as approximately 35% of anticipated revenue.

Table 6.2 **Wastewater Revenue Loss under Dependency Conditions (Electrical Power)**

Revenue Loss Model - 30-Day Assessment		
Average Daily Revenue (System Wide)		$1,250,985
Day 0-10 Daily Revenue Loss		$578,581
Day 11-20 Daily Revenue Loss		$578,581
Day 21-30 Daily Revenue Loss		$159,188
Total Expected Revenue		$37,529,550
Total Realized Revenue		$24,366,060
Total Revenue Loss		**$13,163,490**

6.7.2 Case 2 – The Water System

The event impact on water LOS distribution was run in the independent and interdependent modes to support the assignment of value to operator revenue losses. The independent mode considers only the event-driven asset damage and destruction for the subject infrastructure. The interdependent mode considers the event-driven damage and destruction and the provider infrastructure service delivery degradation that influences asset performance within the consumer infrastructure. *Figures 6.27* and *6.28* show the LOS distribution output from the system over the 30-day period following the event both under independent system evaluation and under interdependent system-of-systems evaluation.

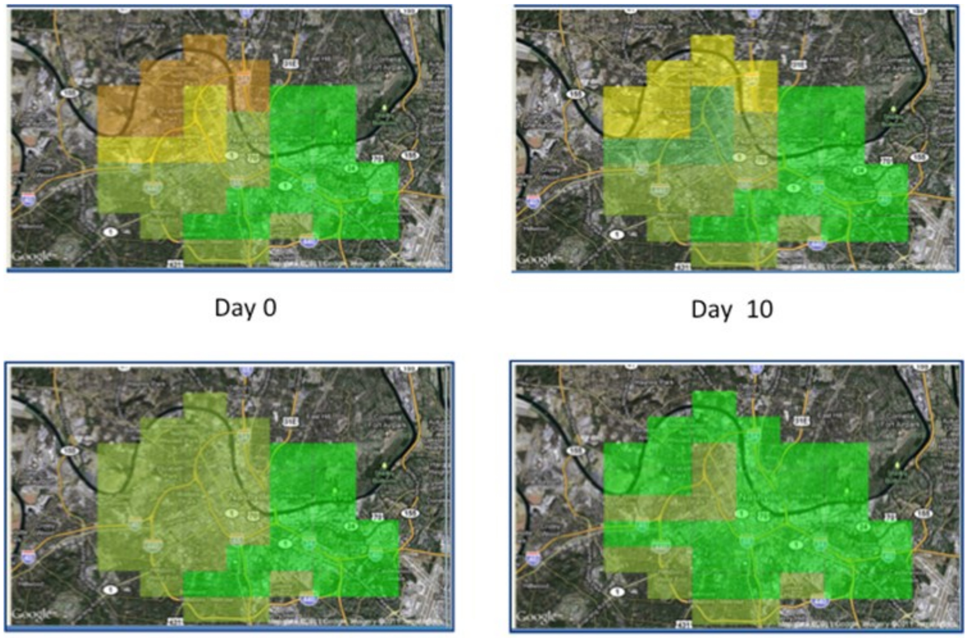
The difference in the rate of restoration of service, most notable in the 10 day figures, is driven by the outage at electrical power substation 4 which provides primary power to pump stations 2 and 4. These images are generated by digital estimates of LOS providing the basis for computing an expected loss of revenue profile.

Wastewater Revenue Loss – Independent Analysis

Step 1: Generate the Revenue Distribution Matrix – The water system revenue distribution matrix used in this study is shown in *Figure 6.29*. As with wastewater, the total revenue is normalized to a value of 10.0. Cell revenue assignments represent the portion of the average daily revenue that is attributed to the customer base within that cell. The values shown are representative of those that can be generated based on publicly-available density and land use data and residential and commercial utility rates. The values are subject to refinement by the service provider as true cell-by-cell values are identified and substituted.

Step 2: Generate the Time-step-by-Time-step LOS Matrix – The water LOS profile generated by the systems model is shown in *Figures 6.30* through *6.33* in matrices that provide the cell-by-cell, time-step-by-time-step LOS values. Values in bold represent the event-responsive area within the region.

Figure 6.25 **Water LOS Distribution over a 30 Day Period – Independent Assessment**



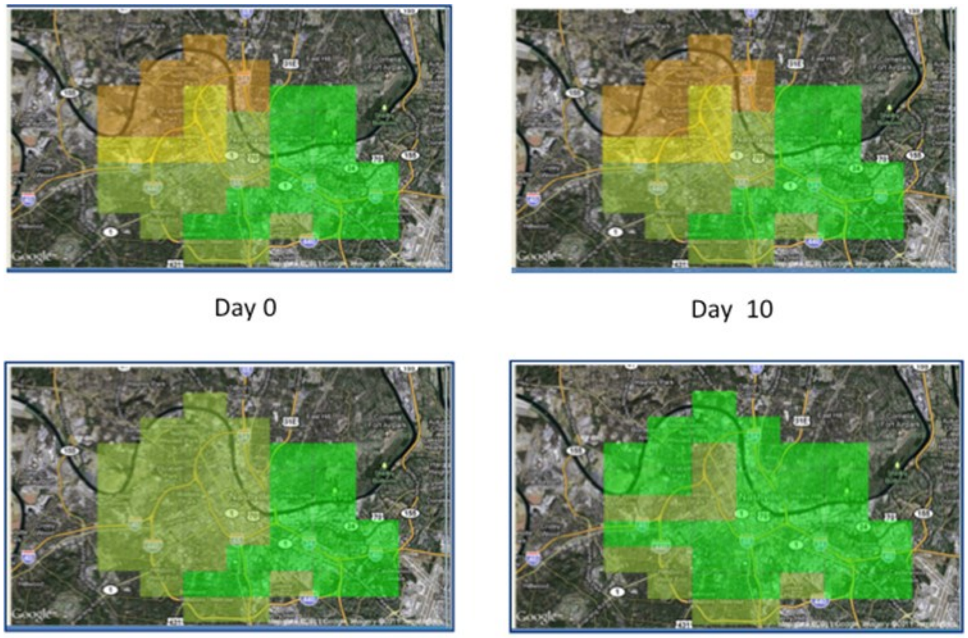
Day 0

Day 10

Day 20

Day 30

Figure 6.26 **Water LOS Distribution over a 30-Day Period – Electrical Power Dependency**

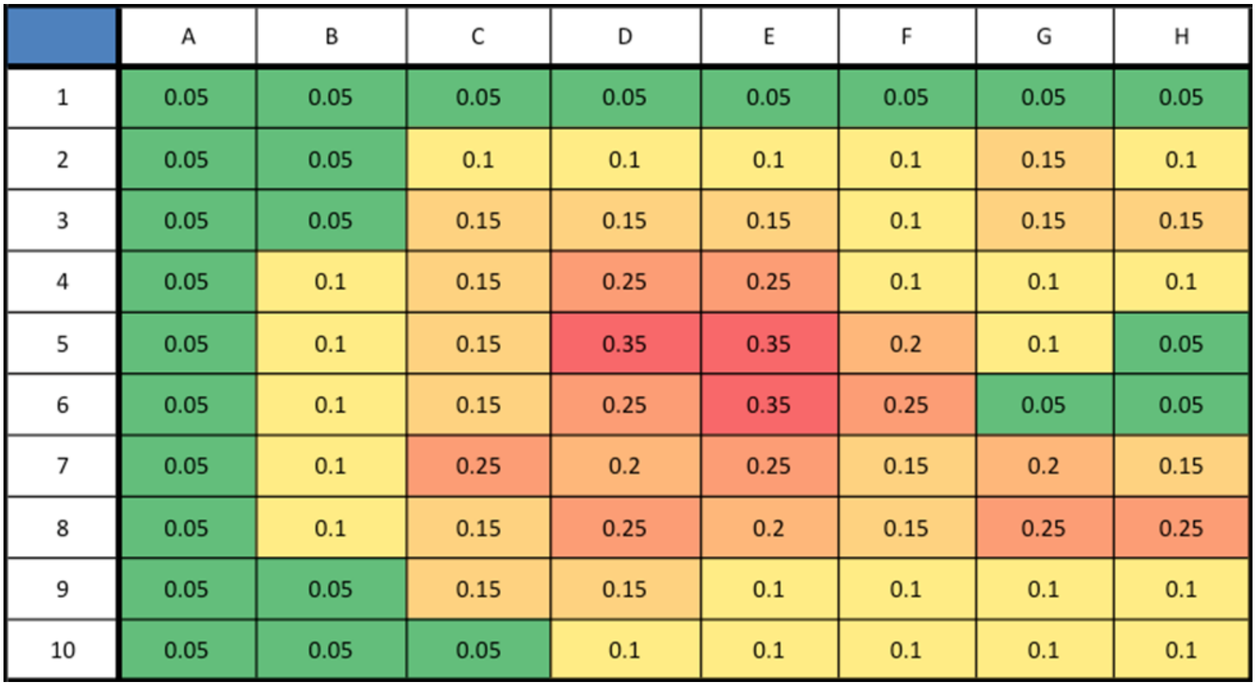


Day 0

Day 10

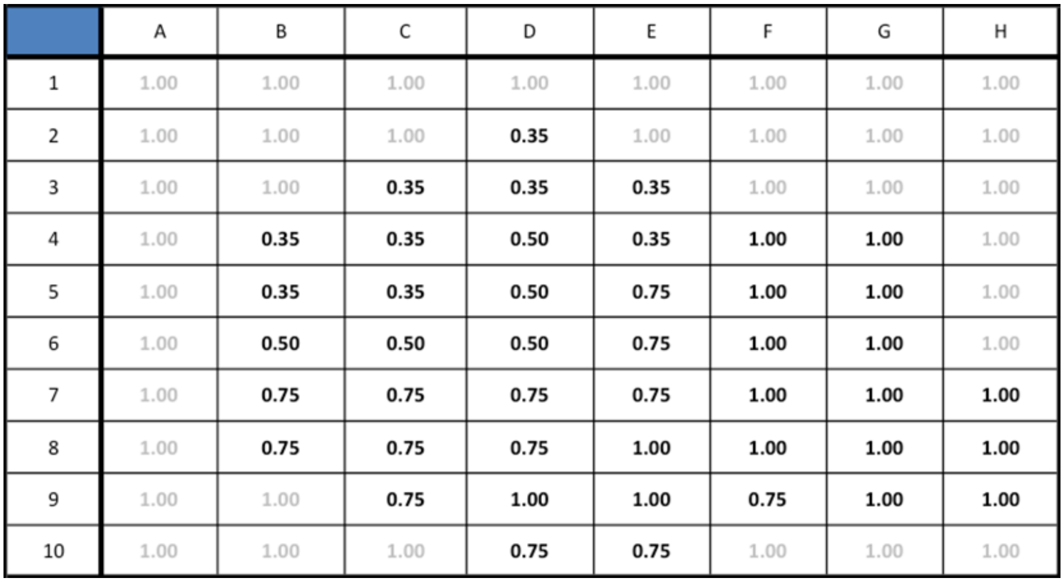
Day 20

Day 30



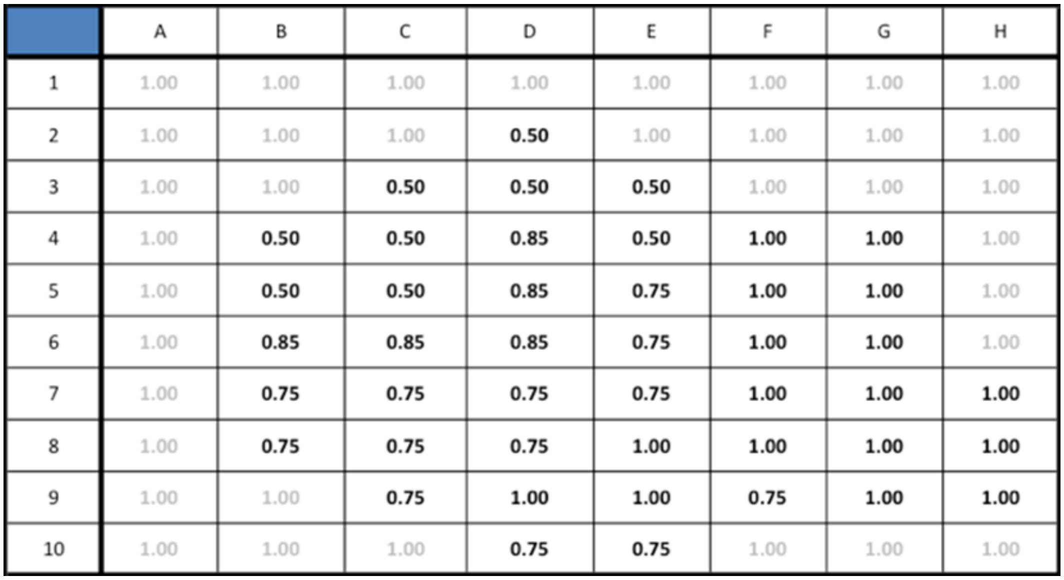
	A	B	C	D	E	F	G	H
1	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05
2	0.05	0.05	0.1	0.1	0.1	0.1	0.15	0.1
3	0.05	0.05	0.15	0.15	0.15	0.1	0.15	0.15
4	0.05	0.1	0.15	0.25	0.25	0.1	0.1	0.1
5	0.05	0.1	0.15	0.35	0.35	0.2	0.1	0.05
6	0.05	0.1	0.15	0.25	0.35	0.25	0.05	0.05
7	0.05	0.1	0.25	0.2	0.25	0.15	0.2	0.15
8	0.05	0.1	0.15	0.25	0.2	0.15	0.25	0.25
9	0.05	0.05	0.15	0.15	0.1	0.1	0.1	0.1
10	0.05	0.05	0.05	0.1	0.1	0.1	0.1	0.1

Figure 6.27 **The Revenue Distribution Matrix for the Water Utility**



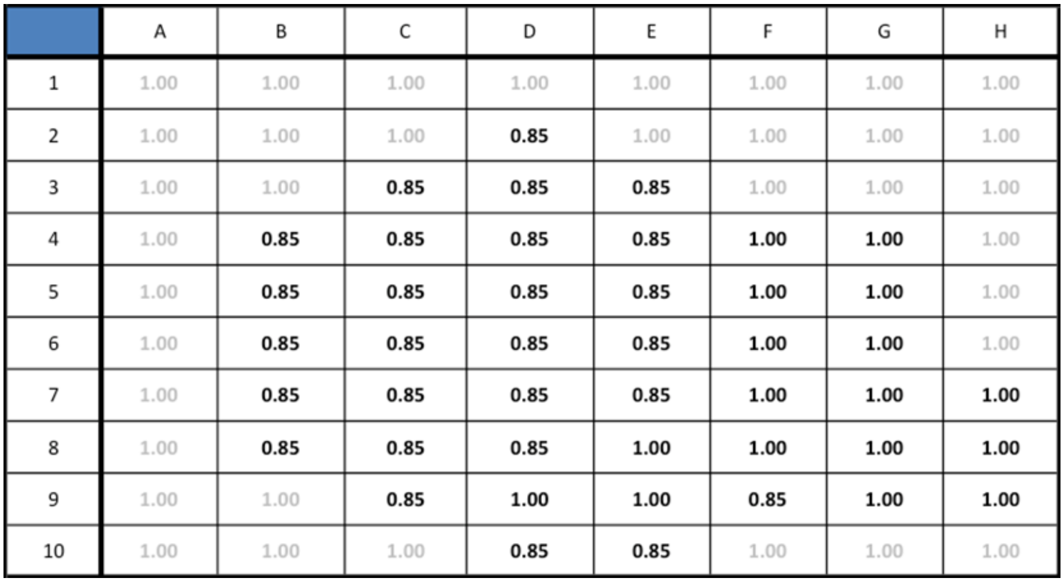
	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.35**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.35**	**0.35**	**0.35**	1.00	1.00	1.00
4	1.00	**0.35**	**0.35**	**0.50**	**0.35**	**1.00**	**1.00**	1.00
5	1.00	**0.35**	**0.35**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
6	1.00	**0.50**	**0.50**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
7	1.00	**0.75**	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
8	1.00	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.75**	**1.00**	**1.00**	**0.75**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.75**	**0.75**	1.00	1.00	1.00

Figure 6.28 **Day 1-10 LOS Distribution – Water – Independent LOS Distribution Impact**



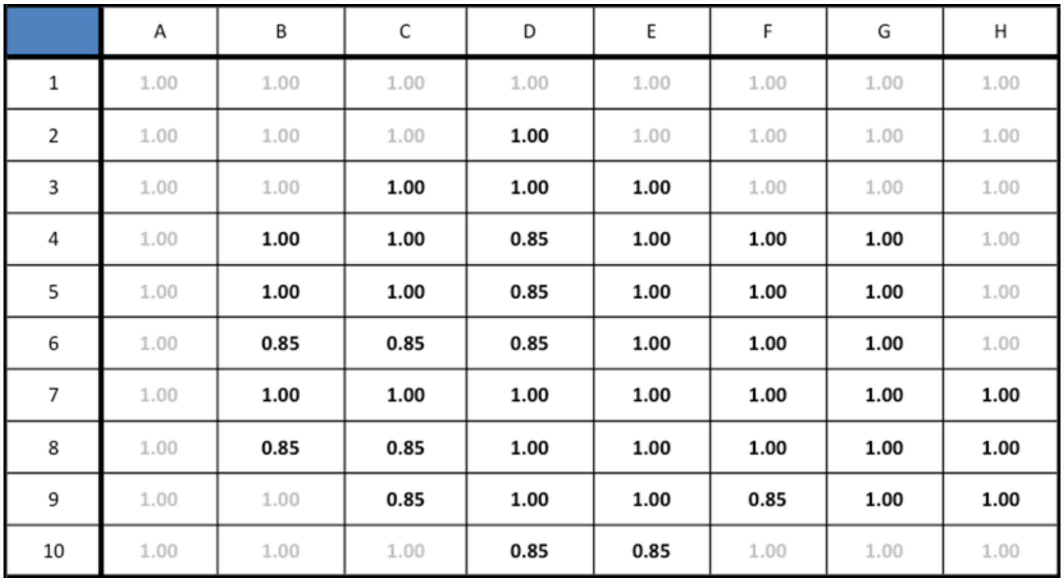
	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.50**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.50**	**0.50**	**0.50**	1.00	1.00	1.00
4	1.00	**0.50**	**0.50**	**0.85**	**0.50**	**1.00**	**1.00**	1.00
5	1.00	**0.50**	**0.50**	**0.85**	**0.75**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**0.75**	**1.00**	**1.00**	1.00
7	1.00	**0.75**	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
8	1.00	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.75**	**1.00**	**1.00**	**0.75**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.75**	**0.75**	1.00	1.00	1.00

Figure 6.29 **Day 11-20 LOS Distribution – Water – Independent LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.85**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.85**	**0.85**	**0.85**	1.00	1.00	1.00
4	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
5	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
7	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.30 **Day 21-30 LOS Distribution – Water – Independent LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**1.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**1.00**	**1.00**	**1.00**	1.00	1.00	1.00
4	1.00	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
5	1.00	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
7	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.31 **Day 31+ LOS Distribution – Water – Independent LOS Distribution Impact**

Step 3: Generate the Revenue Profile – The water service revenue profile is generated by incrementally computing the realized revenue over the recovery time period. The average daily revenue value used in the assessment is $1,723,820. Total realized revenue is computed by integrating over the 30-day period. Revenue loss is found as the difference between anticipated revenue and forecast revenue

The total revenue loss is computed incrementally by time-step period computing and then summing the losses experienced during each time-step. *Table 6.3* identifies the total revenue loss over the entire period as approximately 14% of expected revenue.

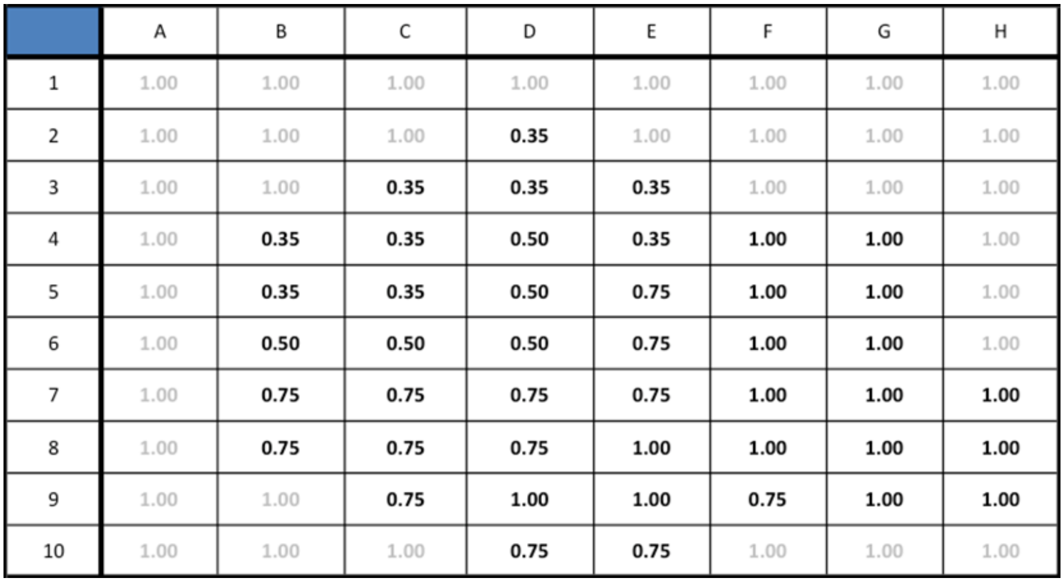
Water Revenue Loss – Dependency Analysis (Electrical Power)

Step 1: Generate the Revenue Distribution Matrix – Same as above.

Step 2: Generate the Time-step-by-Time-step LOS Matrix – The wastewater LOS profile shown in *Figures 6.35* through *6.38* provide the cell-by-cell, time-step-by-time-step LOS values based on dependency on electrical power. Values in bold represent the event-responsive area within the region.

Table 6.3 **Water Revenue Loss under Independent System Evaluation**

Revenue Loss Model - 30-Day Assessment		
Average Daily Revenue (System Wide)		$1,723,820
Day 0-10 Daily Revenue Loss		$346,057
Day 11-20 Daily Revenue Loss		$246,075
Day 21-30 Daily Revenue Loss		$125,408
Total Expected Revenue		$51,714,600
Total Realized Revenue		$44,539,199
Total Revenue Loss		**$7,175,401**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.35**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.35**	**0.35**	**0.35**	1.00	1.00	1.00
4	1.00	**0.35**	**0.35**	**0.50**	**0.35**	**1.00**	**1.00**	1.00
5	1.00	**0.35**	**0.35**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
6	1.00	**0.50**	**0.50**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
7	1.00	**0.75**	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
8	1.00	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.75**	**1.00**	**1.00**	**0.75**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.75**	**0.75**	1.00	1.00	1.00

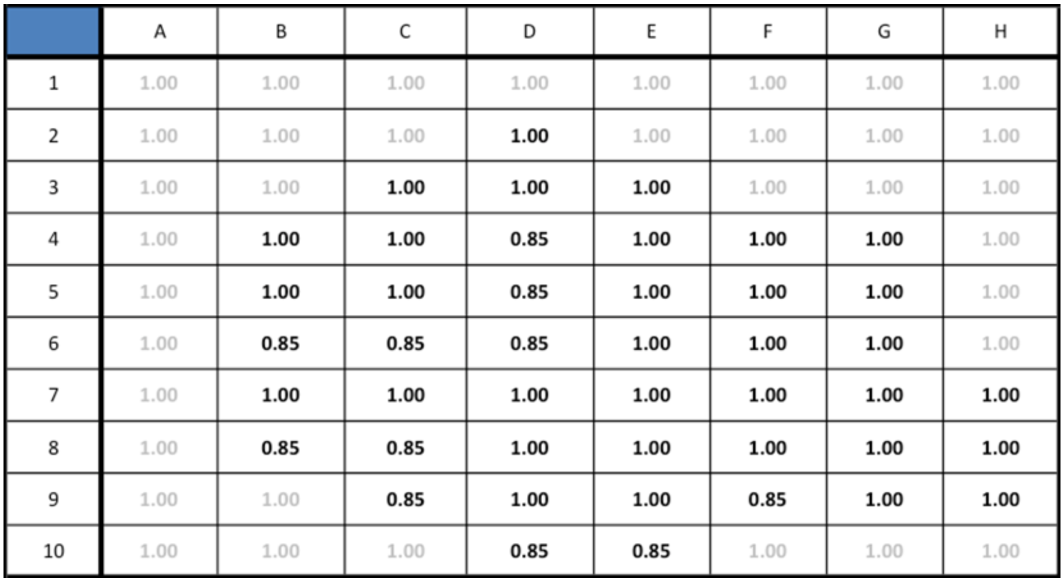
Figure 6.32 **Day 1-10 Water – Interdependent (Electrical Power) LOS Distribution Impact**

	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.35**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.35**	**0.35**	**0.35**	1.00	1.00	1.00
4	1.00	**0.35**	**0.35**	**0.50**	**0.35**	**1.00**	**1.00**	1.00
5	1.00	**0.35**	**0.35**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
6	1.00	**0.50**	**0.50**	**0.50**	**0.75**	**1.00**	**1.00**	1.00
7	1.00	**0.75**	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**
8	1.00	**0.75**	**0.75**	**0.75**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.75**	**1.00**	**1.00**	**0.75**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.75**	**0.75**	1.00	1.00	1.00

Figure 6.33 **Day 11-20 Water – Interdependent (Electrical Power) LOS Distribution Impact**

	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**0.85**	1.00	1.00	1.00	1.00
3	1.00	1.00	**0.85**	**0.85**	**0.85**	1.00	1.00	1.00
4	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
5	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	1.00
7	1.00	**0.85**	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.34 **Day 21-30 Water – Interdependent (Electrical Power) LOS Distribution Impact**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	**1.00**	1.00	1.00	1.00	1.00
3	1.00	1.00	**1.00**	**1.00**	**1.00**	1.00	1.00	1.00
4	1.00	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
5	1.00	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
6	1.00	**0.85**	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	1.00
7	1.00	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
8	1.00	**0.85**	**0.85**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
9	1.00	1.00	**0.85**	**1.00**	**1.00**	**0.85**	**1.00**	**1.00**
10	1.00	1.00	1.00	**0.85**	**0.85**	1.00	1.00	1.00

Figure 6.35 **Day 31+ Water – Interdependent (Electrical Power) LOS Distribution Impact**

Step 3: Generate the Revenue Profile – The wastewater service revenue profile is generated by incrementally computing the realized revenue over the recovery time period. As earlier, the average daily revenue value used in the assessment is $1,723,820. This estimate drives the computations as illustrated in *Figure 6.39*. Total realized revenue is computed by integrating over the 30-day period. Revenue loss is found as the difference between no-disruption revenue and forecast revenue.

The total revenue loss is computed incrementally by time-step period computing and then summing the losses experienced during each time-step. *Table 6.4*, below, identifies the total revenue loss over the entire period as approximately 16% of expected revenue.

Table 6.4 **Water System Revenue Loss under Dependency Conditions (Electrical Power)**

Revenue Loss Model - 30-Day Assessment		
Average Daily Revenue (System Wide)		$1,723,820
Day 0-10 Daily Revenue Loss		$346,057
Day 11-20 Daily Revenue Loss		$346,057
Day 21-30 Daily Revenue Loss		$125,408
Total Expected Revenue		$51,714,600
Total Realized Revenue		$43,539,384
Total Revenue Loss		**$8,175,216**

6.8 Interpretation of Results and Findings

Parallel assessment using the independent and interdependent modes of analysis (see *Table 6.5*) provides results that allow infrastructure operators and municipal and regional officials to objectively assess the impact of cascading failures in terms of operator revenue loss, service delivery loss, and area affected. Clearly, the analysis that accounts for the interaction among the infrastructures provides a more complete estimate of the impacts of disruptive events to owners and the community served. In this example, inclusion of dependencies adjusted the independent assessments by 14-16 per cent in lost revenue and showed significant differences to specific neighborhoods in the region. These results, of course, cannot be generalized because they result from the specific physical configuration of the systems, their flexibility and robustness, and the sophistication of their SCADA systems.

The infrastructure that incurred the initial threat-asset event may have its risk and resilience indicators further adjusted based on these findings to account for interactions with other infrastructures. This analysis also identifies and quantifies risk and resilience challenges to other impacted systems. Risk and resilience indicators for these systems are calculated using the consequences from this phase, mostly revenue losses, with the likelihood and vulnerability from the initial event, estimated in Phase 2. The other systems may address these risks themselves or through collaboration with the initial infrastructure.

This phase is the transition from the focus on the owners' risks and resilience and the regional risk and resilience. To obtain the desired Regional Direct Risk and Regional Direct Resilience indicators, the consequences are summed across all affected systems, both the initial infrastructure and all systems affected by the cascade of events, and weighted by the likelihood and vulnerability of the original initiating threat-asset pair. To obtain the Regional Direct *Inclusive* Risk, add the value of the statistical lives and injuries to the regional direct economic loss.

These results are recognized to be partial because they can only include the systems that are explicitly included in the system-of-systems model. As new systems are added, the total risk may rise. Despite this limitation, these estimates are highly valuable in decision-making because they tie directly back to the specific initiating threat-asset pair, the specific pathways by which the failures were propagated and the specific neighborhoods affected. This specificity permits security and resilience enhancement options to be designed and targeted to specific risks.

Table 6.5 **Infrastructure Impacts as Adjusted Impacts Due to Interdependent Analyses**

	Wastewater			Water			Electricity
	Indep. Anal.	*Interdep. Anal.*	*Adjust. % Diff.*	*Indep. Anal.*	*Interdep. Anal.*	*Adjust. % Diff.*	
Revenue Loss ($K)	11,381	13,163	15.6	7,175	8,175	13.9	12,348
Capacity (Nominal Capacity-Days)	21	19	9.5	26	25	4	
Area (Sq. Miles)							
Days 1-10	35	35	--	14	14	--	
Days 11-20	15	35	233	0	14	N/C	
Days 21-30	0	0	--	0	0	--	

Systems that contribute to the regional economy that have not been explicitly included in the system-of-systems model are accounted for in Phase 5 (Chapter Nine), the regional economic analysis, as are the "ripple effects" on other economic activity.

In the RR/SAP assessment cycle, these results highlight the risk/resilience areas of greatest concern and suggest who might be interested in solutions. In the evaluation phase, these results are the most direct and refined indicators of the benefits of the respective options.

These objective values will support follow-on assessment of the impact on regional life patterns and economic activities and examination of investment options aimed at reducing the effect of natural or man-made events. Even though they are necessarily partial, they are based on individually traceable events, so can be addressed by specific options for improving security and resilience, as described in Chapter Ten.

Assessment of Water to Wastewater Capacity Imbalance: A Special Case
While operator revenue losses and system capacity loss are significant considerations, the more pressing issue in the case of degradation of wastewater systems is public health risk. There is a dangerous mismatch in the level of service in which water service exceeds wastewater service.

The capacity imbalance assessment results shown in *Figure 6.40* represent the case where water and wastewater dependencies on electrical power are not considered. The numbers in the cells represent the ratio by which water capacity exceeds wastewater capacity.

The comparable capacity imbalance assessment results shown in *Figure 6.41* represent the case where water and wastewater dependencies on electrical power are included.

The degree of difference must be addressed to avoid wastewater system storage overload that will result in raw sewage incursion into the river and into the groundwater. This situation could be addressed by powering the lift stations with generators or by public policy action to reduce water usage by voluntary or involuntary means to bring the systems into closer balance. Investment options should consider those that increase resilience of the wastewater system and those that increase the reliability of electrical power at the key power-dependent assets within the wastewater system.

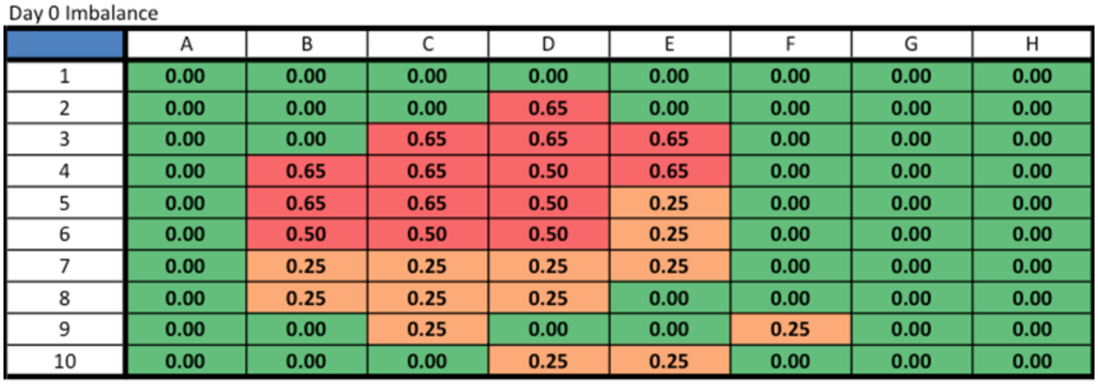
6.9 Summary and Conclusions

The system-of-systems model is an important component of the overall security and resilience assessment process. It provides a structured method to examine the impact of a specific threat -asset event on the performance of assets in the initial system infrastructure and to consider the impact of degradation in other infrastructures and systems. The ability to tie risk and resilience challenges to specific events and propagation pathways uniquely enables the design and evaluation of specific options to enhance security and resilience. The availability of *direct* risk and resilience indictors relevant to *each* system affected by the event and for the region as a whole (even if partial) set the stage for searching for collaborative solutions.

In addition, conducting parallel assessments in the independent and interdependent modes provides a means to examine the compounding affects of single and multi-tier cascading failures generated by interdependency between infrastructures.

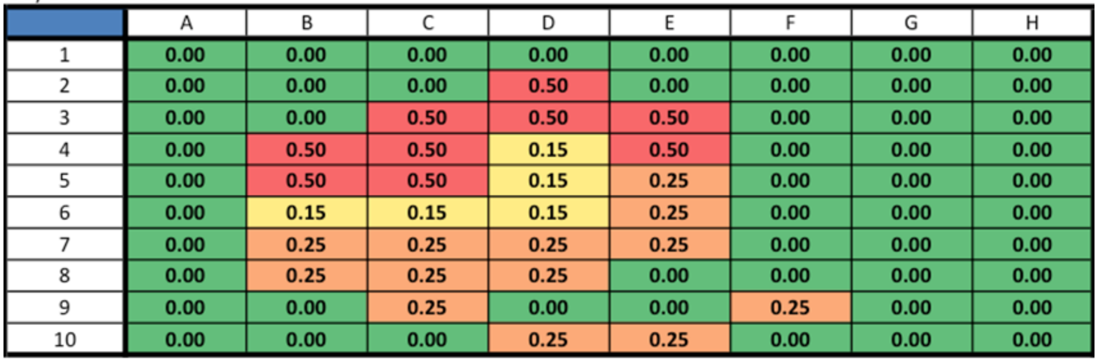
The methodology and data requirements promote transferability, precision, and clear and available metrics. This allows decision makers to have access to quantifiable information that will inform investment decisions based on a quantifiable estimate of the impact of the degradation in individual infrastructure systems and in interdependent system-of-systems. The examples provided address common infrastructure dependencies.

Day 0 Imbalance



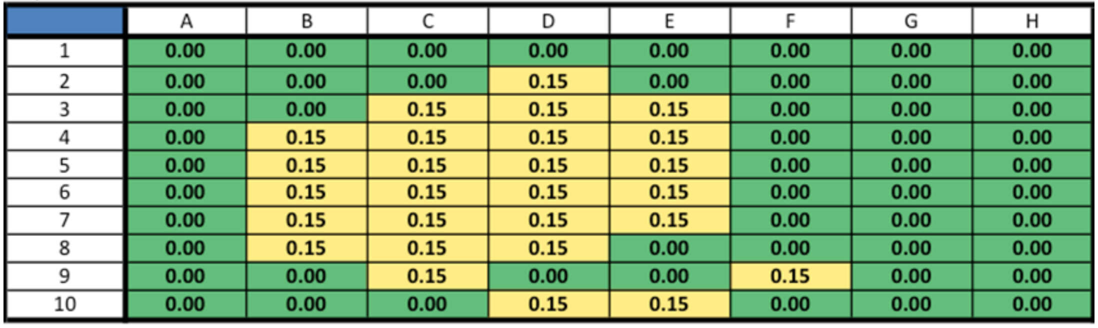
	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.65	0.00	0.00	0.00	0.00
3	0.00	0.00	0.65	0.65	0.65	0.00	0.00	0.00
4	0.00	0.65	0.65	0.50	0.65	0.00	0.00	0.00
5	0.00	0.65	0.65	0.50	0.25	0.00	0.00	0.00
6	0.00	0.50	0.50	0.50	0.25	0.00	0.00	0.00
7	0.00	0.25	0.25	0.25	0.25	0.00	0.00	0.00
8	0.00	0.25	0.25	0.25	0.00	0.00	0.00	0.00
9	0.00	0.00	0.25	0.00	0.00	0.25	0.00	0.00
10	0.00	0.00	0.00	0.25	0.25	0.00	0.00	0.00

Day 10 imbalance



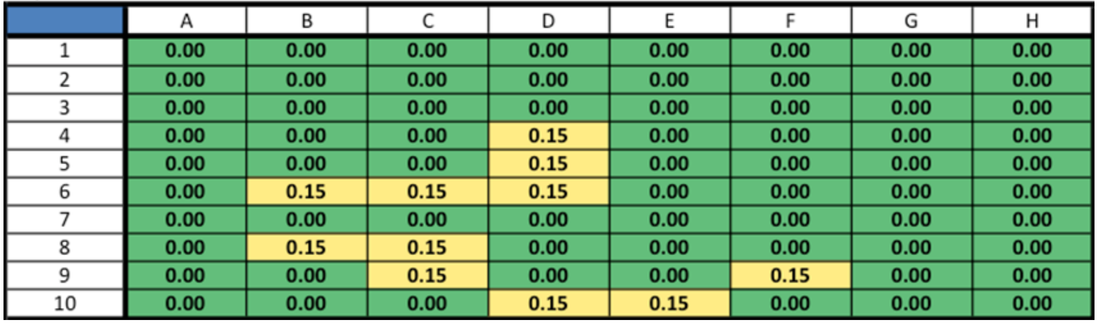
	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.50	0.00	0.00	0.00	0.00
3	0.00	0.00	0.50	0.50	0.50	0.00	0.00	0.00
4	0.00	0.50	0.50	0.15	0.50	0.00	0.00	0.00
5	0.00	0.50	0.50	0.15	0.25	0.00	0.00	0.00
6	0.00	0.15	0.15	0.15	0.25	0.00	0.00	0.00
7	0.00	0.25	0.25	0.25	0.25	0.00	0.00	0.00
8	0.00	0.25	0.25	0.25	0.00	0.00	0.00	0.00
9	0.00	0.00	0.25	0.00	0.00	0.25	0.00	0.00
10	0.00	0.00	0.00	0.25	0.25	0.00	0.00	0.00

Day 20 imbalance



	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
3	0.00	0.00	0.15	0.15	0.15	0.00	0.00	0.00
4	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
5	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
6	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
7	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
8	0.00	0.15	0.15	0.15	0.00	0.00	0.00	0.00
9	0.00	0.00	0.15	0.00	0.00	0.15	0.00	0.00
10	0.00	0.00	0.00	0.15	0.15	0.00	0.00	0.00

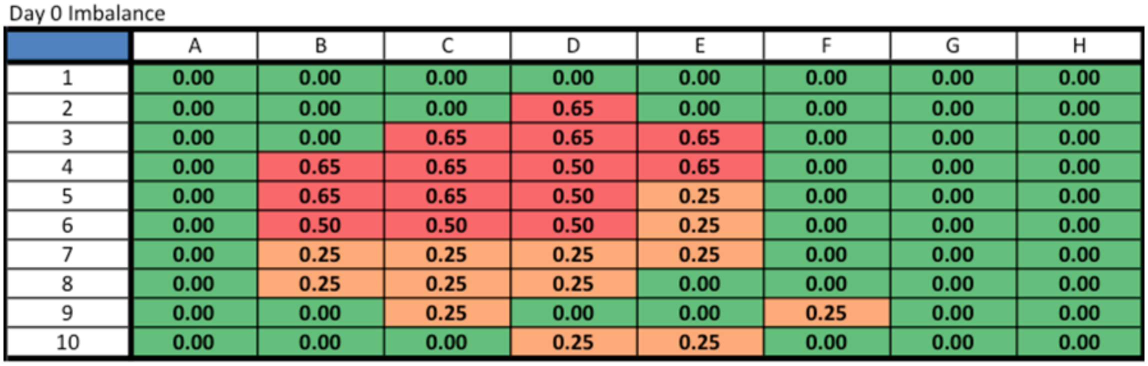
Day 30 imbalance



	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
6	0.00	0.15	0.15	0.15	0.00	0.00	0.00	0.00
7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	0.00	0.15	0.15	0.00	0.00	0.00	0.00	0.00
9	0.00	0.00	0.15	0.00	0.00	0.15	0.00	0.00
10	0.00	0.00	0.00	0.15	0.15	0.00	0.00	0.00

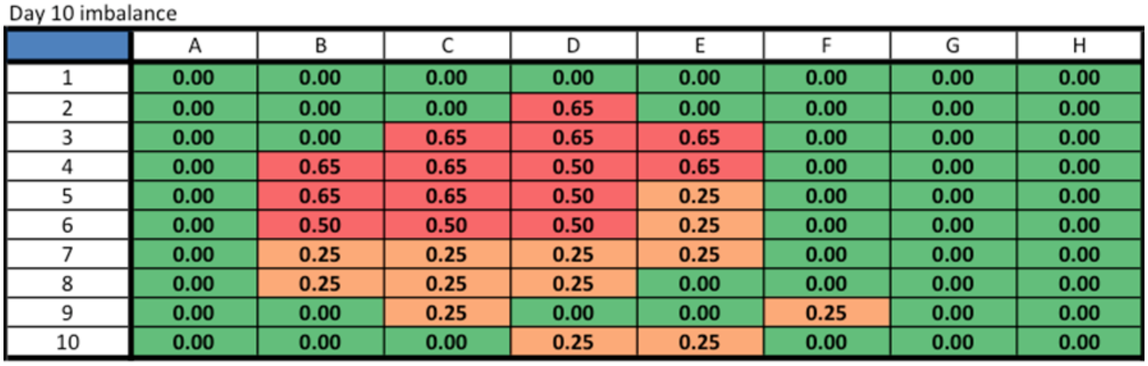
Figure 6.36 **Water-Wastewater Capacity Imbalance - No Electrical Dependency Considered**

Day 0 Imbalance



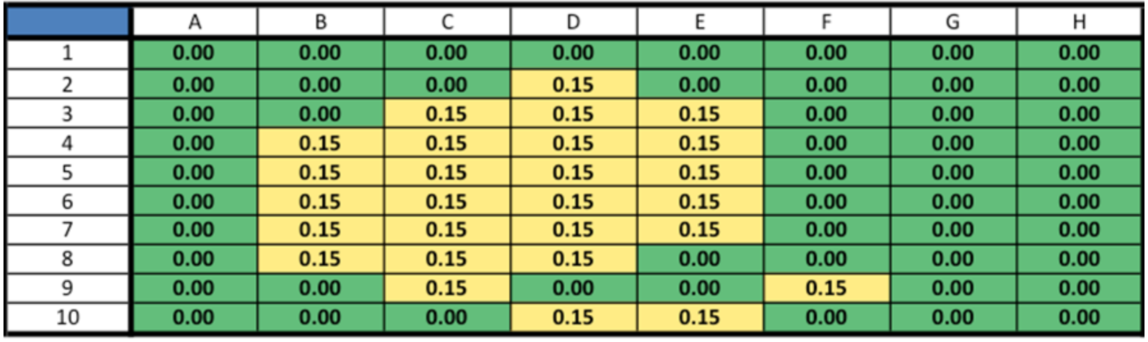
	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.65	0.00	0.00	0.00	0.00
3	0.00	0.00	0.65	0.65	0.65	0.00	0.00	0.00
4	0.00	0.65	0.65	0.50	0.65	0.00	0.00	0.00
5	0.00	0.65	0.65	0.50	0.25	0.00	0.00	0.00
6	0.00	0.50	0.50	0.50	0.25	0.00	0.00	0.00
7	0.00	0.25	0.25	0.25	0.25	0.00	0.00	0.00
8	0.00	0.25	0.25	0.25	0.00	0.00	0.00	0.00
9	0.00	0.00	0.25	0.00	0.00	0.25	0.00	0.00
10	0.00	0.00	0.00	0.25	0.25	0.00	0.00	0.00

Day 10 imbalance



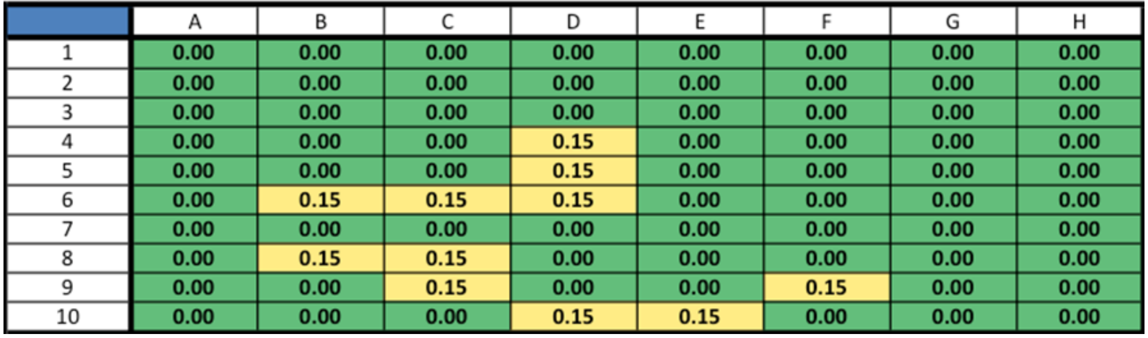
	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.65	0.00	0.00	0.00	0.00
3	0.00	0.00	0.65	0.65	0.65	0.00	0.00	0.00
4	0.00	0.65	0.65	0.50	0.65	0.00	0.00	0.00
5	0.00	0.65	0.65	0.50	0.25	0.00	0.00	0.00
6	0.00	0.50	0.50	0.50	0.25	0.00	0.00	0.00
7	0.00	0.25	0.25	0.25	0.25	0.00	0.00	0.00
8	0.00	0.25	0.25	0.25	0.00	0.00	0.00	0.00
9	0.00	0.00	0.25	0.00	0.00	0.25	0.00	0.00
10	0.00	0.00	0.00	0.25	0.25	0.00	0.00	0.00

Day 20 imbalance



	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
3	0.00	0.00	0.15	0.15	0.15	0.00	0.00	0.00
4	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
5	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
6	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
7	0.00	0.15	0.15	0.15	0.15	0.00	0.00	0.00
8	0.00	0.15	0.15	0.15	0.00	0.00	0.00	0.00
9	0.00	0.00	0.15	0.00	0.00	0.15	0.00	0.00
10	0.00	0.00	0.00	0.15	0.15	0.00	0.00	0.00

Day 30 imbalance



	A	B	C	D	E	F	G	H
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
3	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
5	0.00	0.00	0.00	0.15	0.00	0.00	0.00	0.00
6	0.00	0.15	0.15	0.15	0.00	0.00	0.00	0.00
7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	0.00	0.15	0.15	0.00	0.00	0.00	0.00	0.00
9	0.00	0.00	0.15	0.00	0.00	0.15	0.00	0.00
10	0.00	0.00	0.00	0.15	0.15	0.00	0.00	0.00

Figure 6.37 Water-Wastewater Capacity Imbalance - Electrical Dependency is Considered

CHAPTER 7

Modeling Transportation Systems

7.1 Baseline Concept

The link between infrastructure performance and regional activity is a function of the level of performance of the foundational infrastructures considered in this study, which include: electrical power, water and wastewater, emergency communications, and transportation. The measure of performance used in the assessment of these distributed systems was level of service (LOS), a scale of 0.0 to 1.0 that indicates the ability of the system to balance supply and demand. This was discussed, with its color-based legend shown earlier in *Figure 5.2*.

The measure of performance of the transportation system examined in this chapter, however, is a mobility index. This index is determined for each transportation assessment zone of interest and for the region as a whole. The measure provides an indication of the ability to travel from point-to-point within each individual zone. The mobility index is expressed as a value between 1.0 and 5.0. A value of 1.0 indicates normal travel times. Values above 1.0 are used as multipliers to average non-event-influenced travel times. The maximum value used in the model is 5.0, which essentially indicates that no movement within the zone is possible. This condition can reflect a breakdown in infrastructure or it can reflect event-driven accessibility policies such as evacuations and cordons. The transportation mobility index and the LOS values for the distributed service infrastructures provide the basis for assessing the impact on patterns of life and economic activity.

The transportation system model mobility index estimate is generated on a zone-by-zone basis. The index reflects the balance between the traffic volume (demand) within a zone and the traffic capacity (supply) within each zone. The model recognizes the impact of a disturbance in the balance in terms of traffic pattern shifts. The loss of electrical power to individual traffic signals that may generate a shift in route selection by individual travelers is an example of a capacity-reducing event. This shift will propagate through neighboring zones. The model recognizes the interconnection between the contributors to capacity as it considers zone-specific system lane-mile availability, the role of individual special assets, such as bridges and tunnels in zone-specific capacity, and the functionality of system control and routing features, such as traffic signals and traveler information systems.

The transportation system model recognizes that post-event impact on mobility index values may be evenly or unevenly distributed throughout the region and that the value distribution patterns will change over time as zone-by-zone capacities are restored and zone-by-zone traffic volumes are normalized. The system model accounts for asset restoration profiles and for constraints on alternate path availability. The transportation system model generates spatial and temporal mobility index forecasts for the 30-day period following an event. The transportation system model supports evaluation of traditional transportation economic assessment measures, such as the delay-related user costs as well as the impact on regional patterns of life and economic activity.

The methodology views the transportation system as a network made up of links, nodes, and control functions that are integrated to generate mobility. The physical aspects of the transportation infrastructure system are defined as assets that possess qualities with respect to vulnerability to specific natural or man-made threats. The control aspects of the transportation infrastructure system are defined as the ability to exercise load management and/or path management to accommodate routine asset maintenance, wear-based asset degradation, and event-based asset degradation or destruction. Control functions also possess qualities with respect to vulnerability to specific natural or man-made threats. In all, routes, intersections, bridges and tunnels, with an overarching control center, comprise the elements of the transportation system model.

The methodology assumes that degradation of a physical asset will lead to system performance degradation and that control functions will be used to select alternative load distribution and delivery options to minimize impact and speed recovery.

7.2 Principles of the Methodology

The transportation system model employed in this study is based on the traditional four-step transportation planning model employed by municipal planning organizations throughout the country. The metropolitan area is divided into transportation analysis zones, which are analyzed using the traditional four-step planning model, as employed by the Metropolitan Washington D.C. Council of Governments (MWCOG, 2011), is illustrated in *Figure 7.1*.

The four step process adapted for this study is described below in a step-by-step format.

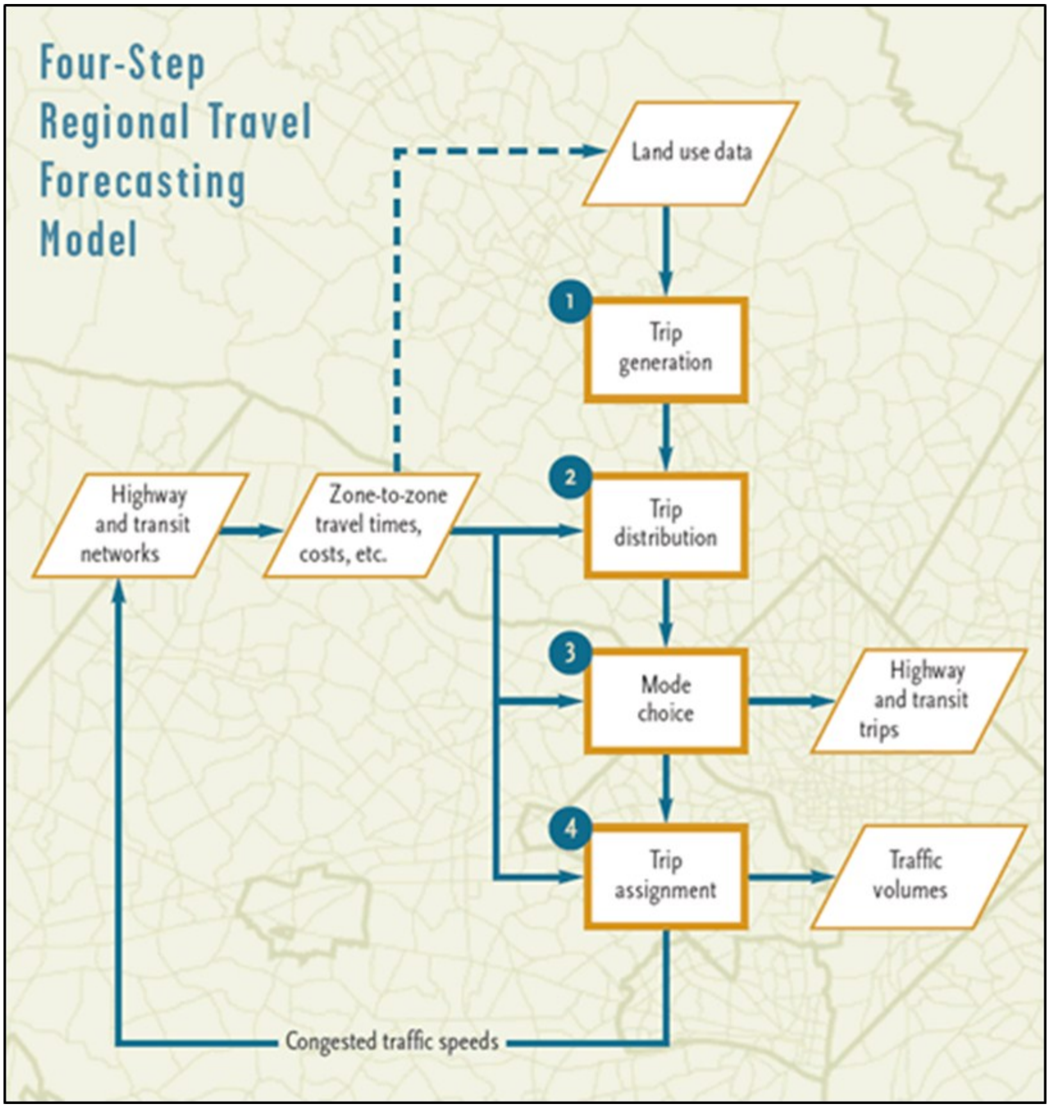


Figure 7.1 **The Traditional Four Step Transportation Planning Model**
(Source: MWCOG, 2011)

Step 1: Trip Generation – How Many Trips – The first step is to estimate the number of trips that occur daily in the region, called trip generation – the number of trips produced from and/or attracted to each transportation analysis zone in the region. The number of trips produced and attracted to each zone (*Table 7.1*) was estimated using assumptions about the number of trips typically made by each type of household and to each type of destination in the region.

Table 7.1 **Trip Generation within Region of Interest**

Population	250,000.00
Persons per Household	2.20
Number of Households	113,636.36
Trip per Household per Day	4.50
Trips per Day	511,363.64

The trip generation procedure estimates the total number of trips produced. These trips are split between different periods of the day. In this study two major periods were defined – peak (includes AM and PM commutes) and off-peak (includes mid-day and night trips). The ratio of peak to off -peak trips used in this study was 80/20. The next step,

Step 2: Trip Distribution – Where Trips Go – The second step, trip distribution, establishes the origins and destinations within the region by identifying the demand for travel through each transportation analysis zone. The trips "produced" and those "attracted" are geographically linked into whole trips. The same process is used to estimate all possible pairs of zones in the region. Time spent traveling is assumed to be experienced negatively by the traveler, with the degree of negatively being proportional to the distance traveled – the greater the distance to the destination, the more undesirable the trip. This results in the majority of trips being as short as possible while accomplishing its purpose. This effect is greatest for non-commuting trips and less for commuting to work because of the large number of long commuter trips that take in regions such as the one examined in this study that include a significant percentage of the population living in suburban areas. This skews the trip distribution as illustrated in *Figure 7.2,* where the height of the bar is the number of trips in each time period and trip-length category.

This procedure yields a set of trips, contained in trip tables, made from and to each zone in the region. Trip tables are produced for each trip type. In the case of this study, three trip tables were generated – peak period trips, off-peak period trips, and commercial trans-regional trips.

Step 3: Mode Choice – Identifying Vehicle Occupancy – In the third step, known as mode choice, travelers choose whether to: (1) drive alone, (2) carpool with others, or (3) take mass transit, based on the availability and desirability of each, considering:

- Automobile ownership rates;
- Relative costs required to use each mode;
- Time required to use each;
- Proximity to carpool lanes; and
- Accessibility of mass transit.

Automobile ownership rates vary substantially across neighborhoods, correlated with land-use patterns and socio-economic status. Costs include mass transit fares, the price of gasoline, parking, and a mileage rate for driving. Time required includes wait time for transit, time transferring between routes, or time spent driving, parking the car and walking to the destination. The mode-choice factors combine to generate a mode-selection pattern establishing an average vehicle occupancy level that establishes the number of vehicle trips by mode that take place during the peak and off-peak periods. For this study, average vehicle occupancy of 1.5 persons per vehicle was used for both peak and off-peak periods.

Step 4: Trip Assignment – Identification of the Route of Each Trip – The last step is to estimate which routes travelers choose to reach their destinations. This step, known as trip assignment or traffic assignment, determines how many

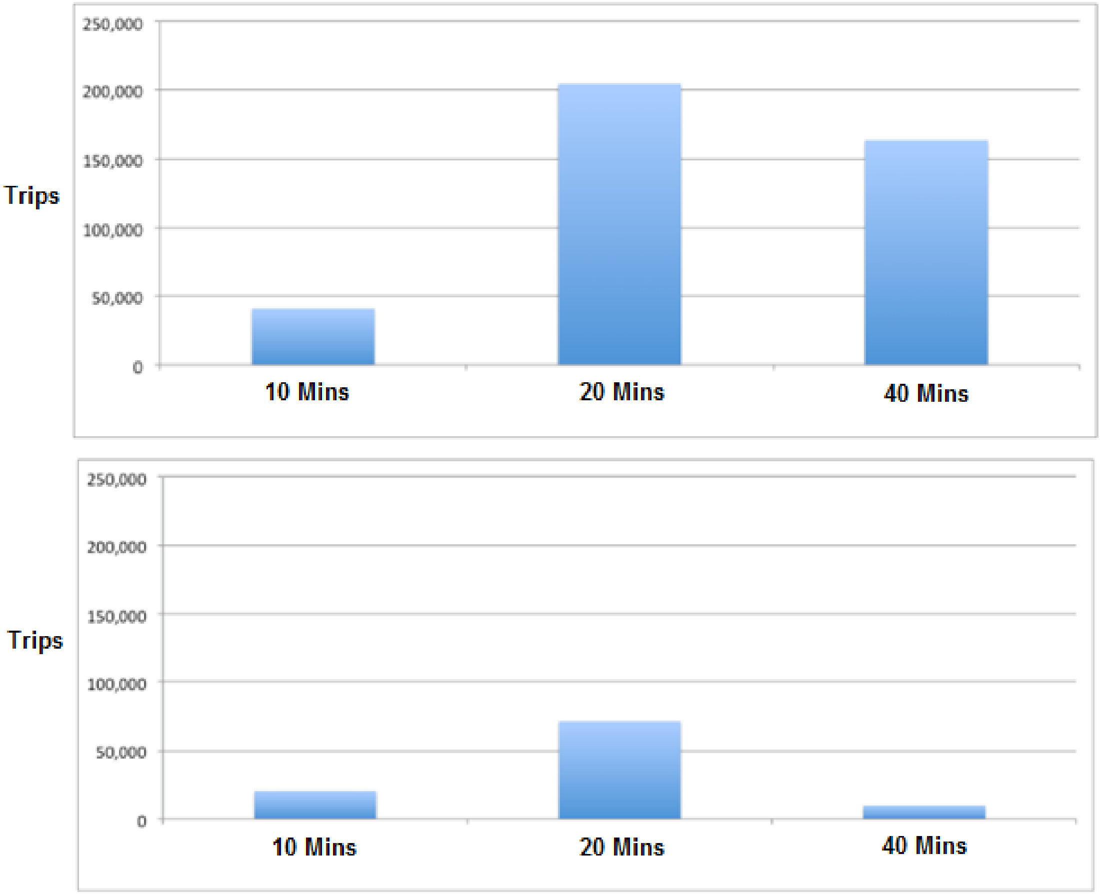


Figure 7.2 **The Peak and Off-Peak Period Trip Distribution by Duration**

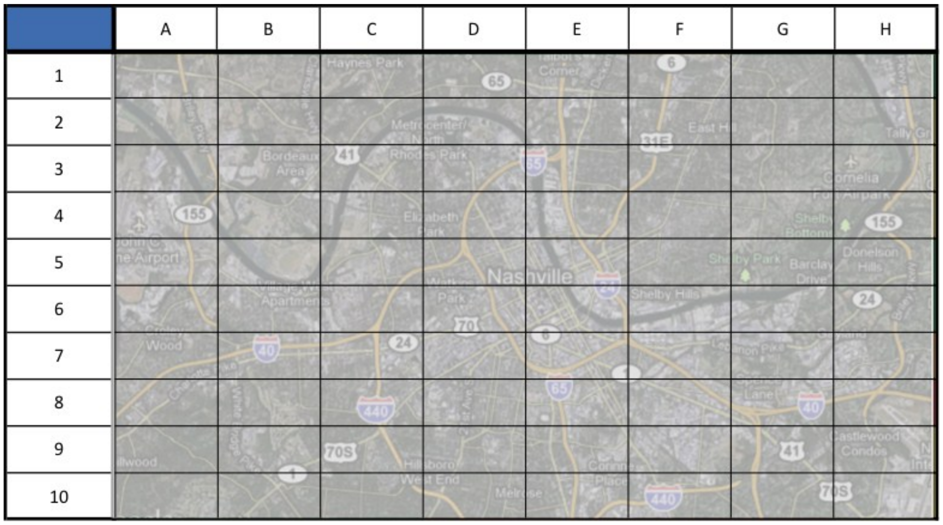
vehicles will travel on each road segment. For the purpose of this study, the normal volumes associated with each transportation link within the analysis zones were determined using average annual daily traffic (AADT) counts. The volume associated with each zone implies a travel time associated with each zone based on link-performance functions under specific roadway element performance levels and load condition.

As roadway element performance is degraded (i.e., loss of lanes due to flooding, power outages at individual signals or at the transportation control center, etc.), or traffic loads are increased due to diversion from neighboring zones, the travel time within a zone will increase. *Figure 7.3* identifies the percent of trips that pass through each transportation analysis zone under normal conditions. *Note again, that the map of Nashville, Tennessee, is used for illustrations but that the data are entirely fictional and for illustration purposes only.*

7.3 Estimation of the Event-Related Transportation Delays

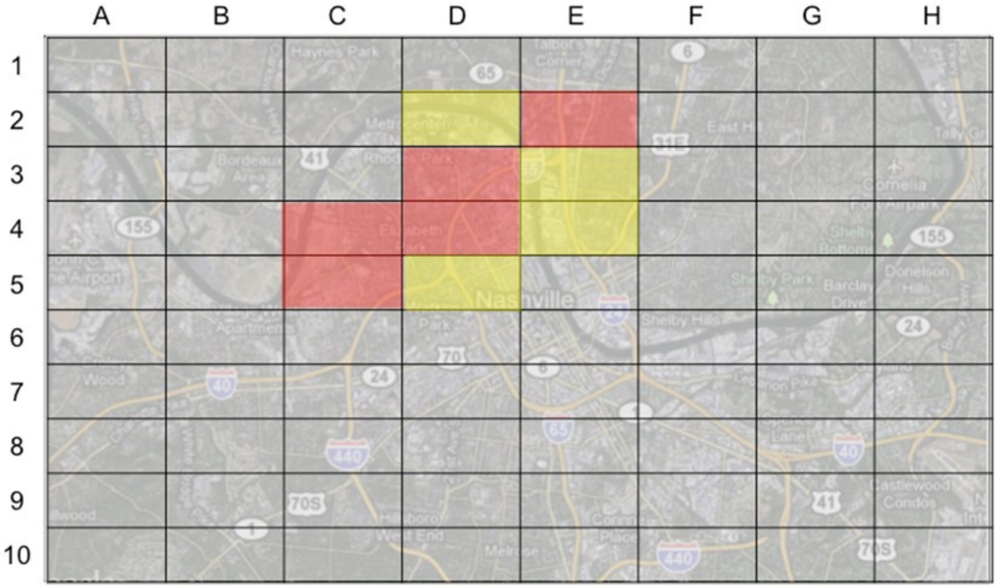
Estimating the event-related transportation delay begins with a review of the event scenario. As in Chapter Five, the illustrative scenario to support the study is a HAZMAT event that takes place at 9:00 AM on a Wednesday in the spring of the year. The case is a chlorine spill of approximately 8500 gallons in the southeastern corner of Grid C-4. The effects of the spill are carried by prevailing southwesterly winds generating an area impact pattern as shown in *Figure 7.4*. A total of nine grid zones are affected encumbering approximately 15 square miles of area.

Figure 7.3 **Normal Travel Pattern (Peak Period) – Percent of Trips that Transit Each Zone**



	A	B	C	D	E	F	G	H
1	1	0.5	0.5	0.5	0.5	1	0.5	0.5
2	1	0.5	1	1	1	1	1.5	1
3	0.5	1	1	1	1	1	1.5	1
4	1	0.5	1	2.5	2.5	1	1.5	1
5	1	0.5	1	2.5	1.5	1.5	1	0.5
6	1	0.5	2	2.5	1.5	2.5	0.5	0.5
7	1	1.5	2	2.5	1.5	1.5	2	1.5
8	0.5	1	2	2.5	2.5	2.5	2.5	2.5
9	0.5	0.5	2	1	1	1	1	1
10	0.5	0.5	0.5	2	2	2	2	1

Figure 7.4 **The Event Impact on Area Accessibility**



The process to determine the event-related delay begins with determination of the mobility index for each affected transportation analysis zone – both primary and secondary. Primary zones are those in which there is a specific damage or degradation of transportation infrastructure performance (red or yellow depending on severity). Secondary zones are those affected by the displacement of travel into neighboring zones (purple or orange depending on severity). To do this, the transportation systems model employs a value computed for each transportation analysis zone.

The day 1-10 assessment is illustrated in *Figure 7.5*. The areas identified as red are completely closed to traffic as directly being affected by the emergency and yellow are only open to residents – not through traffic. Both have mobility indices of 5.0. Those shown in purple indicate the zones impacted by diversion of traffic. The impact on travel time within each zone is indicated digitally in the matrix. In the case of a grid shown in purple, the impact on travel time is a factor of 2.5 (i.e., 2.5 times longer to traverse the zone) due to the increase in travel demand based on diversions and the reduced capacity based on signal outages driven by degradation in electrical power distribution.

The key to support of the full 30-day evaluation period is the grid-by-grid, time-step-by-time-step mobility index forecast shown below in color-coded grid form. *Figure 7.6* shows the progression through various index values over the period following the event.

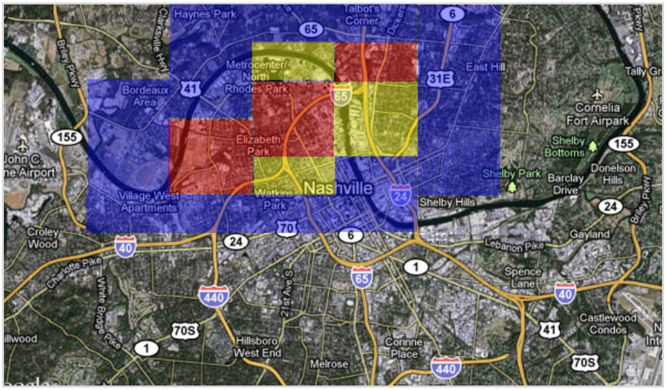
These images are digital representation of the mobility index providing the basis for computing an expected transportation user-cost based on event-induced delay.

Once the mobility index is generated, it is applied to the normal expected travel times within a transportation analysis zone (*Figure 7.7*). The cell-by-cell travel time distribution matrix is multiplied by the time-step-by-time-step mobility index distribution matrix to producing a period-specific event-related delay distribution matrix, as in these figures.

7.4 Estimation of the Economic Impact of Transportation Delays

The economic impact of transportation delay is based on the concept of the value of time. Each metropolitan planning office develops a regional estimate of the value of time that reflects the economic losses on a per person basis of one hour of transportation delay, where delay is defined as the difference between expected travel time and actual travel time. The value of the time estimate is universally applied to all vehicle occupants at the same levy rate for trips of the same purpose taken during the same periods of the day. Because there is no market for buying and selling travel time, indirect methods are used. A variety of transportation agencies have set

Figure 7.5 **Mobility Index Values based on the Chlorine Spill Event - Peak Travel Periods**
(Table on right represents values in Map Overlay)



	A	B	C	D	E	F	G	H
1	1.00	1.00	2.50	2.50	2.50	2.50	1.00	1.00
2	1.00	1.00	2.50	5.00	5.00	2.50	1.00	1.00
3	1.00	2.50	2.50	5.00	5.00	2.50	1.00	1.00
4	1.00	2.50	5.00	5.00	5.00	2.50	1.00	1.00
5	1.00	2.50	5.00	5.00	1.50	2.50	1.00	1.00
6	1.00	2.50	2.50	2.50	2.50	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Figure 7.6 **Mobility Index Distribution (Peak Period) at 10-day Time-steps**

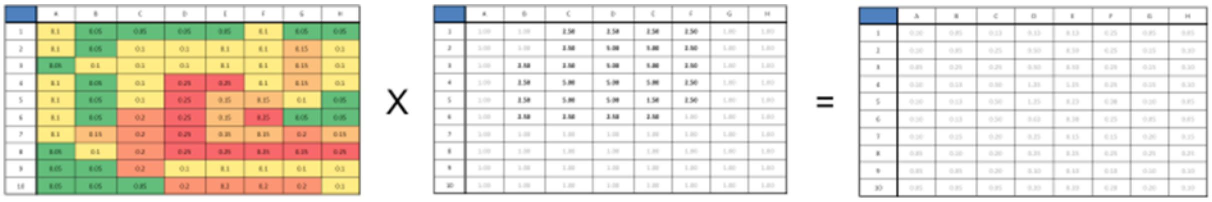
Day 0

Day 10

Day 20

Day 30

Figure 7.7 **Computation of Incremental Revenue** [17]



Travel Time Distribution

Event Mobility Index

Event-Related Delay Distribution

---

[17] For illustrative purposes to demonstrate Event-Related Delay Distribution is the product of Travel Time Distribution and Event Mobility Index.

standards for valuing passenger-time and freight-time costs. Most are based on U.S. Department of Transportation guidance (DOT, 2003) that provides accepted formulas for determining the value of time to be used in transportation planning. These formulas were considered in development of value of time estimates for this study for three user groups of interest:

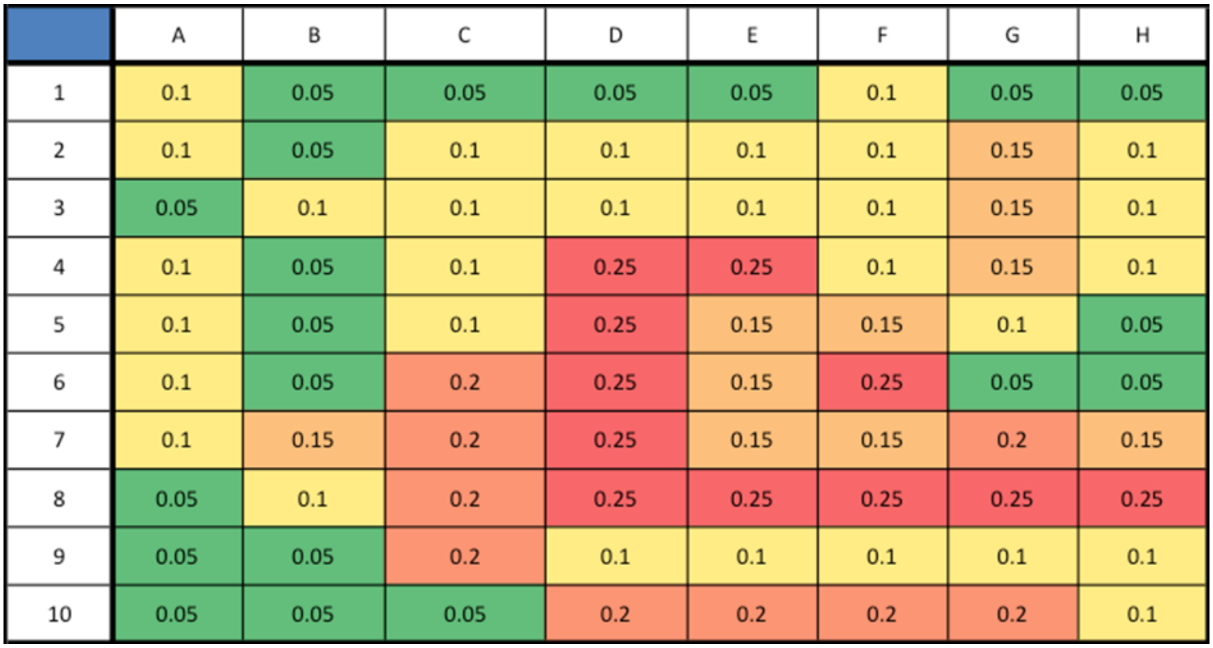
- Person travel peak - $30/hr
- Person travel off-peak - $20/hr
- Freight travel peak and non-peak - $60/hr

These values are used in the three case studies that follow.

Case Study – Transportation User Cost (Peak Period) – Chlorine Spill Scenario

Step 1: Generate the User Cost Distribution Matrix – The transportation user cost distribution matrix used in this study is shown below. The total user cost is normalized to a value of 10.0. Cell cost assignments represent the portion of the average peak period cost that is attributed to the traveler base within that cell. The values shown are representative of those that can be generated based on publicly available AADT data and regional value of time rates. The values are subject to refinement by the municipal planning organization as true cell-by-cell values are identified and substituted. The non-commercial AADT distribution used in this study is shown in *Figure 7.8*. The figure indicates the travel analysis zones where the AADT is concentrated. Note that the concentrations are along the interstate highway corridors at key bridges and interchanges.

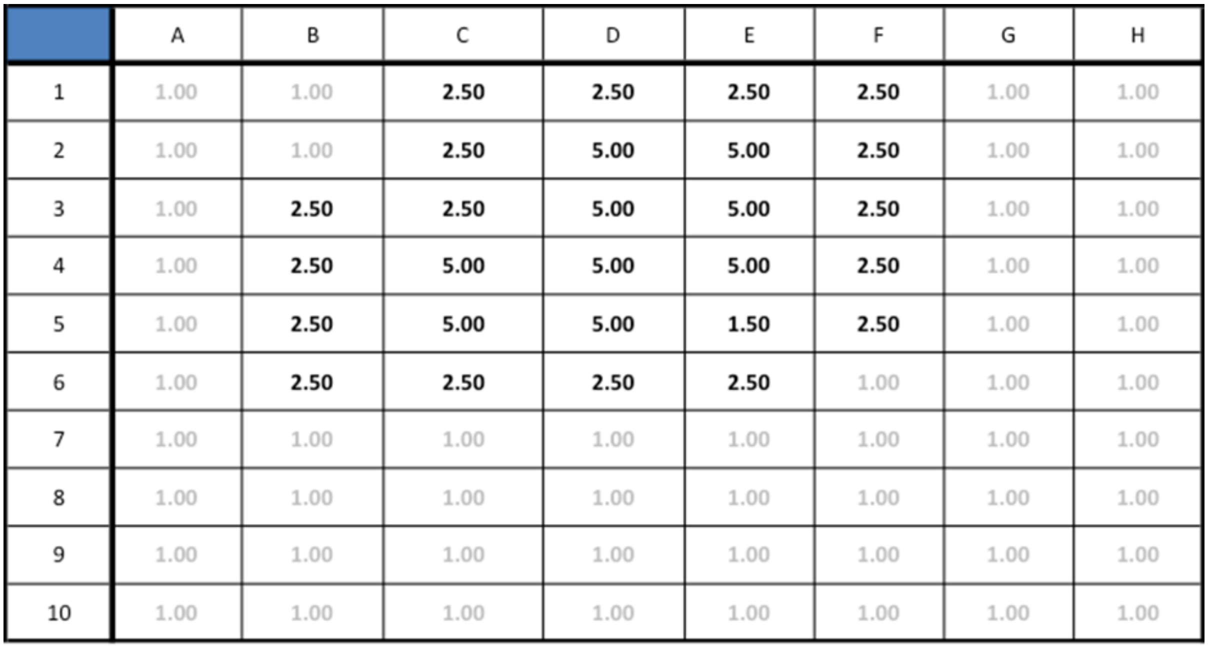
Step 2: Generate the Time-step-by-Time-step Mobility Index Matrix – The mobility index matrix is generated by the transportation systems model previously presented in this chapter. The cell-by-cell, time-step-by-time-step values are generated in conjunction with the visualization of the recovery profile. The four time-step matrices are shown in *Figures 7.9-12*. Note the relationship between the peak transportation analysis zones as compared to the regional average.



	A	B	C	D	E	F	G	H
1	0.1	0.05	0.05	0.05	0.05	0.1	0.05	0.05
2	0.1	0.05	0.1	0.1	0.1	0.1	0.15	0.1
3	0.05	0.1	0.1	0.1	0.1	0.1	0.15	0.1
4	0.1	0.05	0.1	0.25	0.25	0.1	0.15	0.1
5	0.1	0.05	0.1	0.25	0.15	0.15	0.1	0.05
6	0.1	0.05	0.2	0.25	0.15	0.25	0.05	0.05
7	0.1	0.15	0.2	0.25	0.15	0.15	0.2	0.15
8	0.05	0.1	0.2	0.25	0.25	0.25	0.25	0.25
9	0.05	0.05	0.2	0.1	0.1	0.1	0.1	0.1
10	0.05	0.05	0.05	0.2	0.2	0.2	0.2	0.1

Figure 7.8 **The AADT Distribution Matrix for Non-Commercial Travel**

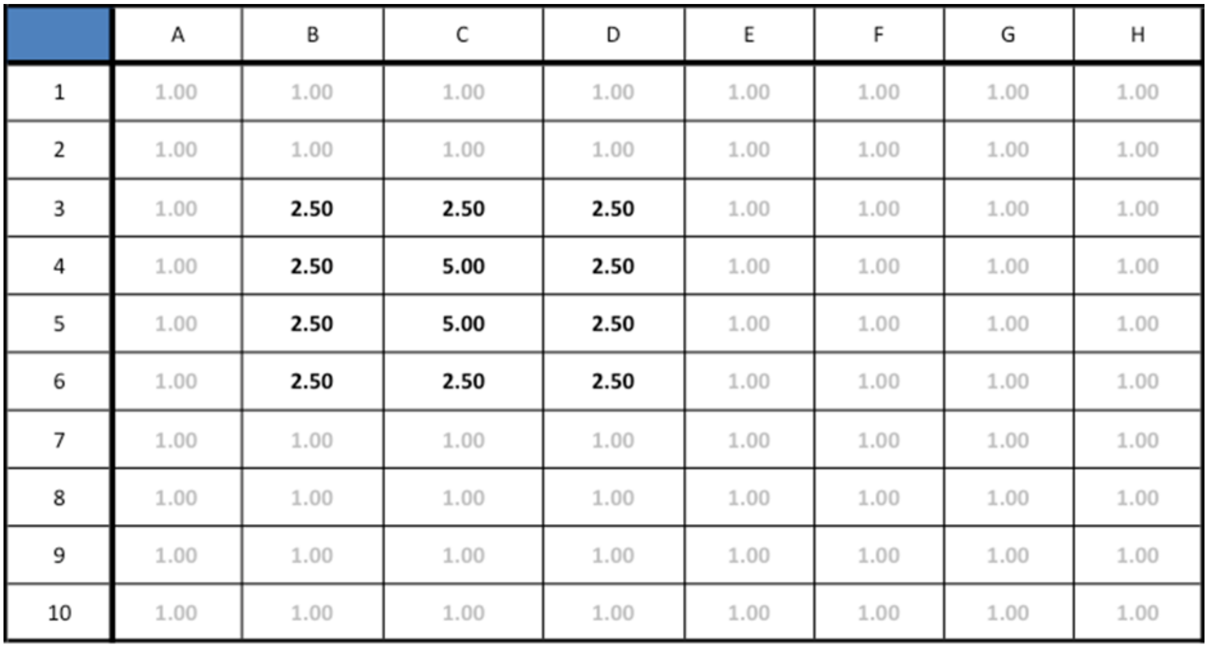
Figure 7.9 **Day 1-10 Delay Distribution**



	A	B	C	D	E	F	G	H
1	1.00	1.00	**2.50**	**2.50**	**2.50**	**2.50**	1.00	1.00
2	1.00	1.00	**2.50**	**5.00**	**5.00**	**2.50**	1.00	1.00
3	1.00	**2.50**	**2.50**	**5.00**	**5.00**	**2.50**	1.00	1.00
4	1.00	**2.50**	**5.00**	**5.00**	**5.00**	**2.50**	1.00	1.00
5	1.00	**2.50**	**5.00**	**5.00**	**1.50**	**2.50**	1.00	1.00
6	1.00	**2.50**	**2.50**	**2.50**	**2.50**	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Day 1-10: Regional Impact on Delay is an 80% Increase

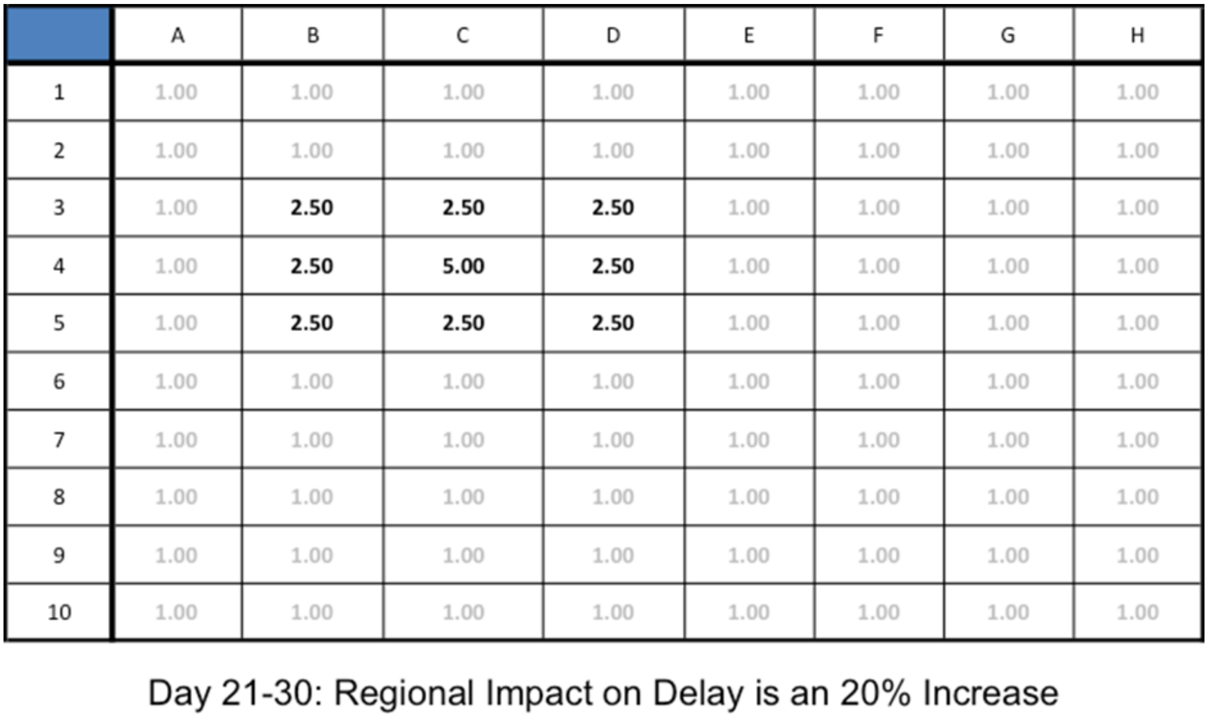
Figure 7.10 **Day 11-20 Delay Distribution**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	1.00	**2.50**	**2.50**	**2.50**	1.00	1.00	1.00	1.00
4	1.00	**2.50**	**5.00**	**2.50**	1.00	1.00	1.00	1.00
5	1.00	**2.50**	**5.00**	**2.50**	1.00	1.00	1.00	1.00
6	1.00	**2.50**	**2.50**	**2.50**	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Day 11-20: Regional Impact on Delay is an 30% Increase

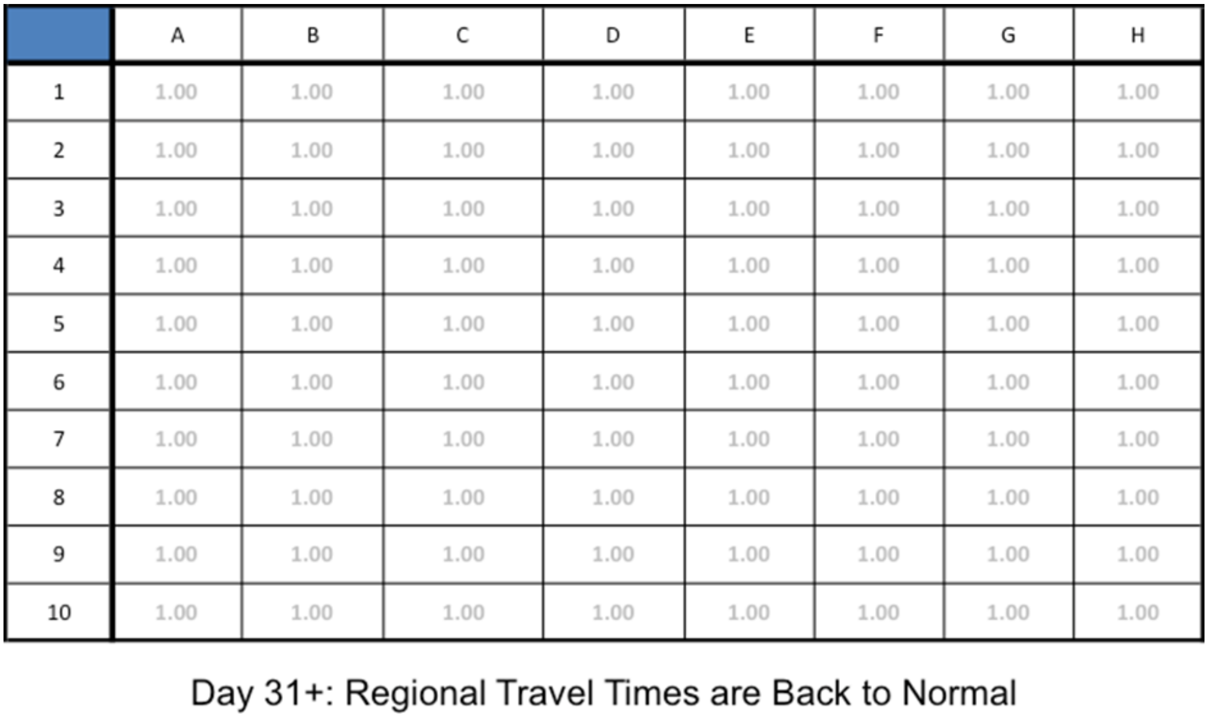
Figure 7.11 **Day 21-30 Delay Distribution**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	1.00	**2.50**	**2.50**	**2.50**	1.00	1.00	1.00	1.00
4	1.00	**2.50**	**5.00**	**2.50**	1.00	1.00	1.00	1.00
5	1.00	**2.50**	**2.50**	**2.50**	1.00	1.00	1.00	1.00
6	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Day 21-30: Regional Impact on Delay is an 20% Increase

Figure 7.12 **Day 31+ Delay Distribution – Return to Normal**



	A	B	C	D	E	F	G	H
1	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
4	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
5	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
6	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
9	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Day 31+: Regional Travel Times are Back to Normal

Step 3: Generate the Non-Commercial Peak Period User Cost Profile – The non-commercial user peak period cost profile is generated by incrementally computing the realized cost over the recovery time period. The average daily cost value used in the assessment is based on generation of approximately 511,000 trips per day with a peak hour factor of 80% (*Table 7.1*).

The peak period trip duration distribution used in the study is *Figure 7.13*.

These assumptions drive the computations to generate non-commercial peak hour user total cost over the 30-day period, as illustrated in the top of *Figure 7.2*.

The total non-commercial user cost during the peak periods is computed incrementally by time-step period computing and then summing the cost experienced during each time-step. *Table 7.2* identifies the total non-commercial user peak period cost over the entire 30-day assessment period.

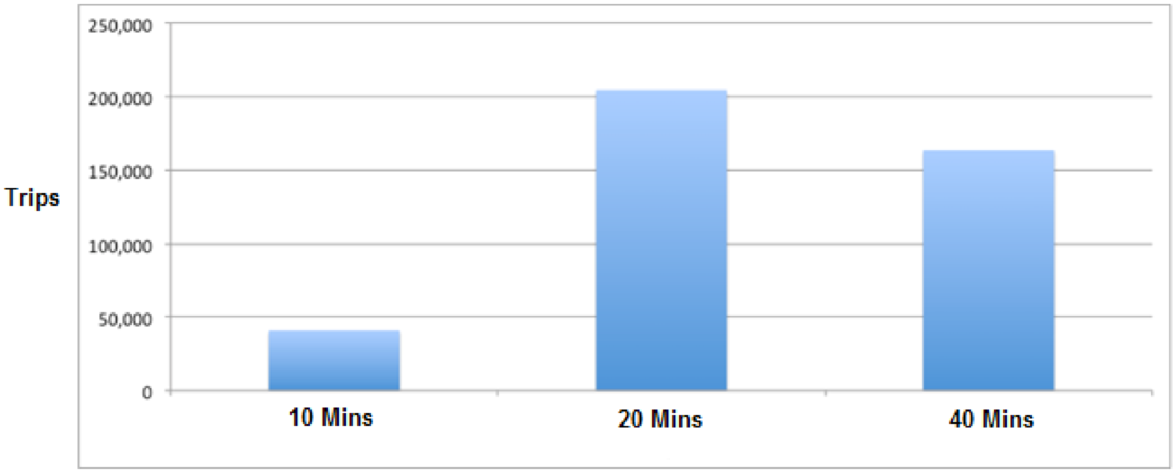


Figure 7.13 **Peak Period Trip Duration Distribution (Normal Case)**

Table 7.2 **Computation of Non-Commercial User Peak Period Cost**

Day 0-10 Daily Event Related Delay Cost		$6,751,534
Day 11-20 Daily Event Related Delay Cost		$2,443,807
Day 21-30 Daily Event Related Delay Cost		$1,615,398
Total Daily Event Related Delay		**$108,107,386.36**

Case Study – Transportation User Cost (Non-Peak Period)

Off-peak user costs recognize the shift in transportation system performance as a result of reduced overall demand. This shift is reflected in the non-peak mobility index values identified in *Figure 7.14*. The orange grid color reflects a mobility index of 1.5 versus the 2.5 factor observed during the peak period.

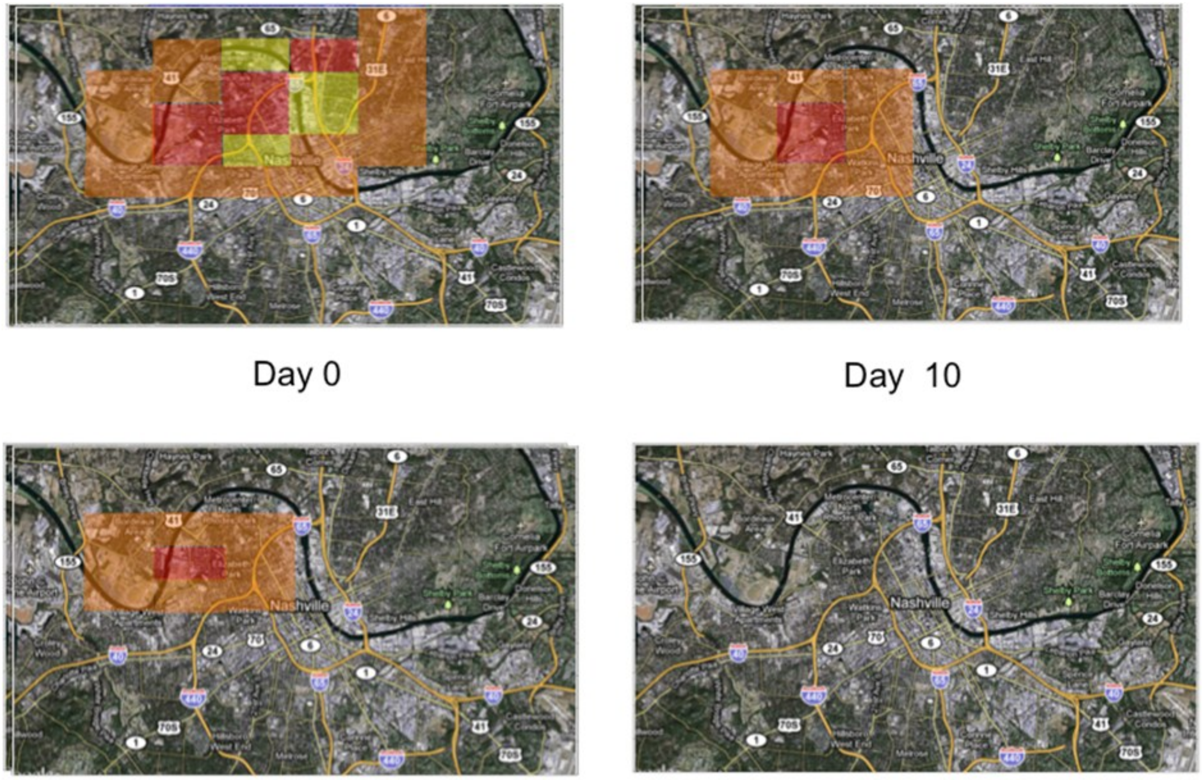
The study assumes 20% of travel is accomplished during the off-peak period and that the concentration of trip duration shifts to favor shorter trips, as shown in *Figure 7.15*.

Table 7.3 identifies the total non-commercial user off-peak period cost over the entire 30-day assessment period.

Case Study – Transportation Freight User Cost

Freight user costs are based on an average daily through freight demand of approximately 51,000 trips per day. *Table 7.4* shows the total commercial period cost over the entire 30-day assessment period.

Figure 7.14 **Mobility Index Distribution During Non-Peak Periods**



Day 0

Day 10

Day 20

Day 30

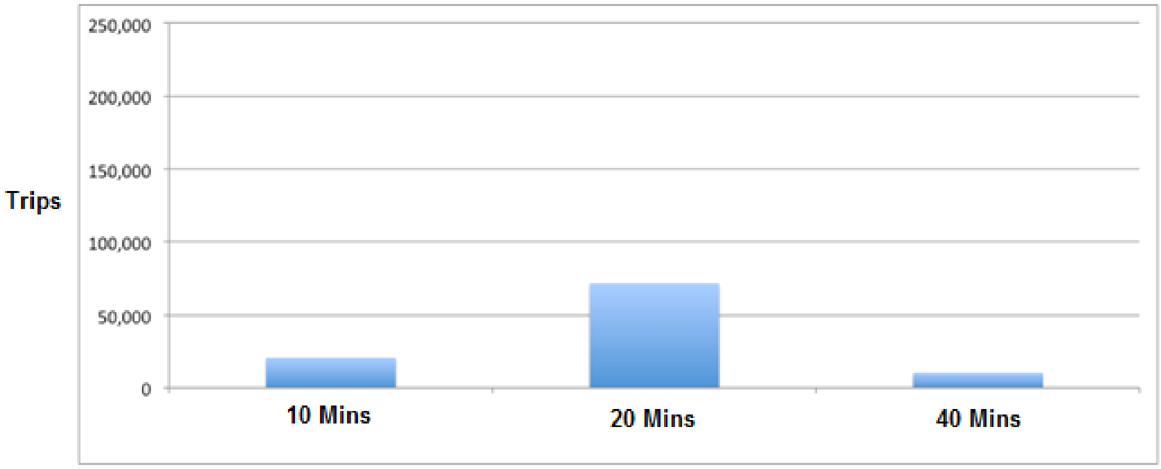


Figure 7.15 **Trip Duration Distribution During Non-Peak Periods**

Table 7.3 **Computation of Non-Commercial User Non-Peak Period Cost**

Day 0-10 Daily Event Related Delay Cost		$756,818
Day 11-20 Daily Event Related Delay Cost		$237,784
Day 21-30 Daily Event Related Delay Cost		$97,159
Total Daily Event Related Delay		**$10,917,613.64**

Table 7.4 **Computation of Freight User Cost**

Value of Time Model - 30-Day Assessment		
Through Frieght Trips per Day		$56,818
Total Freight Travel Time (hrs) per Day		$19,413
Vehicle-Hours per Day		$19,413
Value of Time (Freight)		$60
Day 0-10 Daily Event Related Delay Cost		$8,619,322
Day 11-20 Daily Event Related Delay Cost		$90,270
Day 21-30 Daily Event Related Delay Cost		$110,653
Total Daily Event Related Delay		**$10,628,551**

7.5 Summary and Conclusions

The transportation system model considers the dependence of the transportation system on electrical power and the interdependence that exists between the physical transportation assets and transportation control systems. The model recognizes the impact of traveler route choice in response to an event and the impact that diversion has on transportation system performance. The analysis conducted in this chapter illustrates the level of impact a degraded transportation system has on productivity and on transportation system user cost. Productivity is impacted by transportation delay, which at the beginning of the scenario, was 80% higher than normal on a regional basis. This exceptionally high value was driven by the location of the chlorine spill and the impact the plume had on major transportation assets, including a major river crossing and sections of the major regional route structure, followed by local travelers. The user cost, which is a universal measure of economic impact of transportation delay, is driven by the sheer number of trips affected, the degree of delay experienced, the duration of major disruptive aspects of the event, and the size of the area in which normal traffic flow was impacted.

As with the prior system assessment chapters, the methodology and data requirements have been developed in a manner that promotes utilization of information employed in normal planning processes allowing the regional leadership bodies to leverage information they have with the capability of an infrastructure assessment methodology. The output of the transportation system model is presented in accepted terms increasing the utility of event assessments in the capital budgeting processes that help decision-makers prioritize initiatives that have practical day-to-day and resiliency impacts.

CHAPTER 8

RR/SAP Approach to Analyzing Public Safety Functions

8.1 Principle Issues in Analyzing Public Safety Functions

A significant motivation for developing the Regional Resilience/Security Analysis Process (RR/SAP) is to save lives, avoid serious injuries and minimize losses due to various threats. RR/SAP was initially developed as a process for addressing lifeline infrastructures and, later, industries that are the major "drivers" of the regional economy. In the course of developing these methods, it has become clear that when threats or hazards happen anywhere in the region, infrastructures are critical to the overall regional resilience, but certain public safety functions are the actual means by which fatalities and injuries are avoided or managed – specifically fire suppression (FS), emergency medical services (EMS) and police incident management (PIM). These must be included in an analysis of risk and resilience if the full process of response – and the full accounting for consequences – is to be addressed. These public safety functions, however, are *users* of infrastructures, not infrastructures in their own right, so need to be addressed in a slightly different fashion.

To include these functions in the RR/SAP analytic approach required answers to two specific questions:

1. Could the basic RAMCAP approach of RR/SAP Phase 2, developed for stationary infrastructure facilities, be adapted to the dynamic, personnel-centered response functions by defining and prioritizing threat-asset pairs as the primary unit of analysis to capture the information needed to estimate risk and resilience?
2. Could the transportation and system-of-systems models of Phases 3 and 4 support dynamic analysis of the public safety functions to estimate the consequences, especially financial losses, fatalities and serious injuries *in the community*, i.e., beyond the consequences to the fire and police departments or the infrastructures?

This chapter addresses the first of these questions by applying RAMCAP to a fire department to see what adaptations are needed and whether the approach can capture the needed information. The chapter addresses the second question by sketching simple analysis/planning models of the service-delivery process for FS and EMS and determining if they can function in the region as defined by the system-of-systems and transportation models.

Due to the time truncation of the field portion of the project, neither part is carried out to the point of working demonstration, but both proceeded far enough to support the conclusions that public safety functions can be analyzed in the RR/SAP approach with minimal modification. Moreover, this inclusion allows a more complete and accurate analysis, especially of major incidents where human casualties outside the infrastructures and agencies of government are concerned.

8.2 Applying RR/SAP to Public Safety Functions

Relative to the infrastructures for which RAMCAP was designed, the services of public safety functions are much more labor-intensive and are delivered in dynamic, real-time conditions at uncertain (before the incident) geographic points. In most cases, the effectiveness of public safety functions is dependent on the time to reach the location of an incident and the ability to marshal the resources required in terms of number and types of units.

These characteristics set specifications for the RR/SAP to be applied to these functions in Phases 2 through 4.

8.2.1 RR/SAP Phase 2 (RAMCAP Analysis)

To test whether RAMCAP could be used for a public safety function, the project included an in-depth application to the FS, EMS and emergency communications (also considered a critical infrastructure) of a middle-sized metropolitan area. Fire department personnel and the analysts formed a study team to apply the process, modifying it as needed to complete the assessment phase.

Step 1 defined critical assets as including the dispatch system (also considered part of the emergency communications infrastructure), firehouses, vehicles (pump trucks, ladder trucks, mobile command center, mobile oxygen compressor, fuel truck, fire boat), trained personnel, and specialized equipment, such as the stationary oxygen compressor. In step 2, the team determined that the major threats were natural hazards, industrial accidents (e.g., derailings or highway accidents involving toxic or explosive materials, fires at manufacturing plants) although the team would assess the full set of standard RAMCAP threats. Threat-asset pairs were defined by making rough estimates of consequences; they were prioritized by ranked groupings shown in *Table 4.3*, above. The team then proceeded through steps 3 through 6 as described in Chapter Four without difficulty. RR/SAP Phase 2 can, indeed, be applied to public safety functions.

Two modifications to RAMCAP were noted. First was the identification of skilled, trained personnel as assets in the same way that trucks were defined as assets. RAMCAP had previously concentrated only on “hard” assets of equipment, facilities and systems. It is simply meaningless to analyze public safety functions without personnel. Such individuals *personally deliver* the services of public safety. The team designated certain classes of personnel as assets and went forward with the process without problems.

Second, the team recognized that the casualties and serious injuries of interest were not the employees of the infrastructure organizations, but the direct recipients of the public safety service. These services are delivered across the region at times and places unknown before they occur. The amount of time in responding directly impacts the level of these losses and, in many cases, the financial losses as well. This means that analyzing the risk/resilience of public safety functions requires modeling the uncertain, distributed delivery of these services. Such a model would be considerably more complex than RAMCAP uses for analyzing more certain, stationary systems – and also means that this modeling must be done in the context of the transportation and system-of-systems models.

8.2.2 Phases 3 and 4: Distributed Service Models for Analyzing Effectiveness and Dependencies of Public Service Functions

The uncertain location of incidents requiring response and the pre-positioning of assets that are highly mobile require an analytic approach that models the delivery of the services across the transportation grid as well as an intense interaction with a number of infrastructures. The service-delivery model must “sit on top of” and operate in conjunction with the transportation and system-of-systems regional models. This means that it can only be built beyond the conception level after the completion of the other models.

Further, the incidents that call for public safety services to be delivered include the threats to all the other systems that are explicitly modeled in the analysis, as well as incidents outside those systems. The casualties and losses estimated in the analysis of those systems is in part a function of how fast and how well the public safety functions perform.

In delivering public safety services, the agencies involved are highly flexible in moving assets – personnel and equipment – quickly to where they are needed and "back-filling" for these committed assets by moving other assets into position to respond to the next incident. This means that the "move-up" protocols must be modeled as well as the basic dispatch of the assets assigned to the incident. It also underscores the fact that multiple, *simultaneous* incidents are so common that the departments' routine procedures call for preparing for them. That is, in modeling the operations of public safety functions, the capability must include the whole system and multiple, simultaneous, incidents dispersed in uncertain locations – all built "on top" of the transportation and system-of-systems models.

For these reasons, only conceptual models of the public safety functions are presented here.

8.3 Public Safety Service Delivery Model

The objective of the public safety service delivery planning models is to estimate the consequences – the casualties and dollar losses – of various hazard and threat incidents to which public safety systems respond. The model is to be as evidence-based as possible, but must estimate consequences as a function of the location of the incident, time and nature of public safety response, and other variables that determine the consequences. These performance estimates need to be made under three conditions:

1. A base case, in which no hazard is present, based on current conditions, which will include a "business-as-usual" level of calls for public safety services (ideally calibrated to actual performance data).
2. A series of hazard/threat cases as they affect one or more of (a) the public service delivery system, (b) infrastructures included in the system-of-systems model) and/or (c) random locations in the region. In the second of these, casualties and losses estimated in the analyses leading up to the public safety analysis may need to be modified significantly, as the prior estimates made at least implicit assumptions about the effectiveness of the public safety functions in responding to their incidents.
3. The same series of hazard/threat cases in the presence of a specific mitigation option (s).

Differences in performance are the consequences of interest for the assessment. The differences between case 1 and 2, above, define the risk and resilience consequences of interest and the differences between cases 2 and 3 are the consequences used in estimating the benefits of the option(s).

8.3.1 Fire Suppression Basic Model

It is important to note that FS is only one of the functions of the fire department directed to loss reduction and regional resilience. A substantial contribution to loss reduction is made by the fire marshal's activity in reducing fire hazards through building and fire code enforcement, sprinkler regulations and management of access to fire hydrants. The importance of this non-response activity is reflected in the ratings by ISO (formerly the Insurance Service Organization) that contribute to the establishment of community fire insurance ratings.

Figure 8.1 illustrates the simple model we propose to use in the assessment of the FS function. The sequence of events and the time intervals in the model are:

1. A fire ignites.
2. The fire is detected.
3. A call for help is made to the emergency communications system (9-1-1) and is answered – dependent on private telecommunications and electricity.
4. The call is transferred to dispatch for the fire department – dependent on electricity.
5. Fire department dispatcher orders specific units to respond based on their location relative to the incident – dependent on electricity.

6. The assigned units “turn out” by gathering the needed equipment and mounting the vehicles and departing the station – dependent on oxygen compression equipment and motor fuel.
7. The equipment travels to the incident location – dependent on motor fuel and the transportation system.
8. The incident commander assesses the situation and directs the deployment of fire fighters and equipment to extinguish the fire – usually police are required to control traffic and crowds.
9. The fire-extinguishing agent, usually water except in certain chemical or electrical fires, is placed on the fire from the pump engines – dependent on the water and fuels systems and supplies of non-water extinguishing agents.
10. The fire is fought to the point of suppression or abandonment – access, rescue, start water from engines, pull hoses from water sources (hydrants or other) and continue putting water on the fire, ventilate, etc. – dependent on water pressure to hydrants and sprinklers (requiring electric power to move water to the site), fuel systems, supply of full breathing tanks, EMS and hospitals if there are injuries or burn victims.
11. Fire fighters collect the equipment and supplies.
12. Fire fighters return to station, if not called for additional dispatch – dependent on transportation and fuel systems.
13. Fire fighters return to availability for duty.

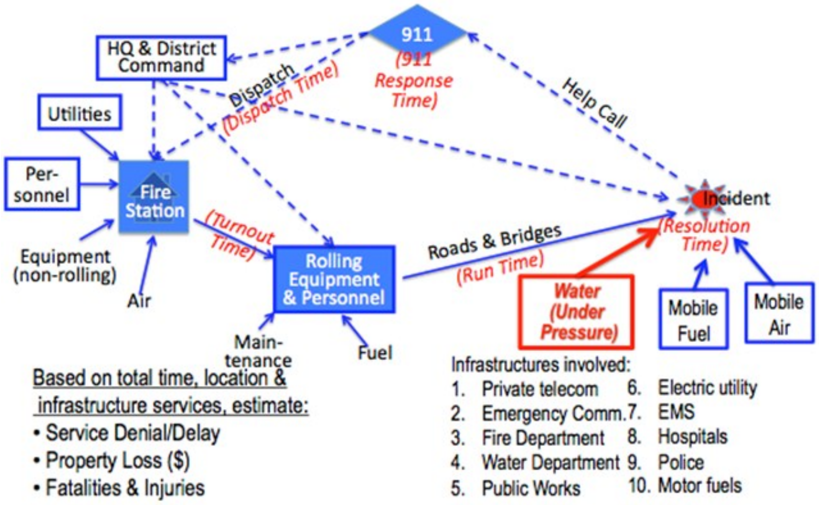
Note that the process requires contributions from at least ten infrastructures, as listed in the figure.

Because of the high redundancy of equipment and the relatively close proximity of the fire stations, we assume all routine fires are treated, but that the time to arrive may vary due to various hazards. Hazards slow the vehicles or necessitate service by vehicles from other stations, farther away (greater travel time). This assumes that the number and magnitude of incidents is manageable within the capacity of the fire department’s resources. Massive or very numerous disruptions or fires could exceed this capacity. The model captures this to the point of overload, then continues to capture consequences of the non-response.

The service area for a specific station is its first-due area and all adjacent areas that are first due for the immediately surrounding stations. The service area’s characteristics determine its types and frequency of fires (see below).

The major impact of the respective hazards and threats is to lengthen one or more of the time elements in the model. For example, a major

Figure 8.1 **Concept for Fire Suppression Planning Model**



tornado would cause trees to be down across streets, extending the run time, as engineers must seek ways around the impediments. Another example would be an attack on a station that could make response impossible, so the dispatch would be relayed to another station farther away, so dispatch time, turnout time and run time would be lengthened.

The general belief in the literature, our interviews and common sense support the general assumption that the longer the time to begin treating the fire, the more it grows, until it reaches the flashover point, after which there is total loss of life and all property in the room of ignition. The fire breaks out into other rooms, causing casualties and losses to grow at an exponential rate until the fire is suppressed or allowed to burn out. The key issue is just how much time is added by various events. The literature consulted to date agrees with the premise, but lacks clear quantitative relationships. Among the reasons for this are the near complete absence of ignition time in the data – reporting starts with the receipt of the call at 9-1-1, not with ignition – and the confounding effects of various neighborhood and operating characteristics in natural fire situations. Combining a statistically useful number of incidents without controlling for these variables clouds the main causal effects of time to losses.

Analytic Construct. The base case is the level of the performance when no hazard impedes the performance of the FS asset being assessed – a specific station or company (equipment and operators). This performance depends on a number of characteristics of the area it serves (which determine the types and frequency of fires experienced) and is grounded in urban, suburban and rural geography, locations, state of development and recent performance history. That is:

$$\textbf{\textit{Performance}}_{\textbf{\textit{base}}} = \textbf{\textit{f(service area conditions, geography, travel time}}_{\textbf{\textit{base}}}\textbf{\textit{, etc.)}} \qquad \textit{Eq. 8.1}$$

And

$$\textbf{\textit{Performance}}_{\textbf{\textit{hazard}}} = \textbf{\textit{f(service area conditions, geography, travel time}}_{\textbf{\textit{hazard}}}\textbf{\textit{, etc.)}} \qquad \textit{Eq. 8.2}$$

Performance is the losses and civilian casualties, so is actually measured as dollar losses, fatalities and serious injuries.

Base performance is the level of losses under historic "business-as-usual." The hazard/threat scenario performance either has little or no effect or has its expected performance degraded – total time is increased – resulting in higher consequences – greater losses. The differences between the performances with the hazard and without it are the consequences of the hazard on the asset, or:

$$\textbf{\textit{Consequences}}_{\textbf{\textit{hazard}}} = \textbf{\textit{Perfomance}}_{\textbf{\textit{hazard}}} - \textbf{\textit{Perfomance}}_{\textbf{\textit{base}}} \qquad \textit{Eq. 8.3}$$

This is the value multiplied by threat likelihood and vulnerability in the risk calculation.

Similarly, the performance with the mitigation option in place is estimated, primarily captured in reduced time to respond and reduced consequences, producing the benefit of the option:

$$\textbf{\textit{Consequences}}_{\textbf{\textit{option}}} = \textbf{\textit{Perfomance}}_{\textbf{\textit{option}}} - \textbf{\textit{Perfomance}}_{\textbf{\textit{hazard}}} \qquad \textit{Eq. 8.4}$$

$$\textbf{\textit{Benetfit}}_{\textbf{\textit{option}}} = (\textbf{\textit{Consequnces}}_{\textbf{\textit{hazard}}} \times \textbf{\textit{V}}_{\textbf{\textit{hazard}}} \times \textbf{\textit{T}}_{\textbf{\textit{hazard}}}) - (\textbf{\textit{Consequnces}}_{\textbf{\textit{option}}} \times \textbf{\textit{V}}_{\textbf{\textit{option}}} \times \textbf{\textit{T}}_{\textbf{\textit{option}}}) \qquad \textit{Eq. 8.5}$$

Graphically, this concept is illustrated in *Figure 8.2*. A unique curve is defined for a manageable number of land-use/building types (e.g., urban-suburban, age and types of construction, etc.). These are weighted by their proportions in each station's primary service area, or "first-due zone". For example, one type curve could be for wood frame residential buildings more than 50 years old. Experts would be asked to advise on

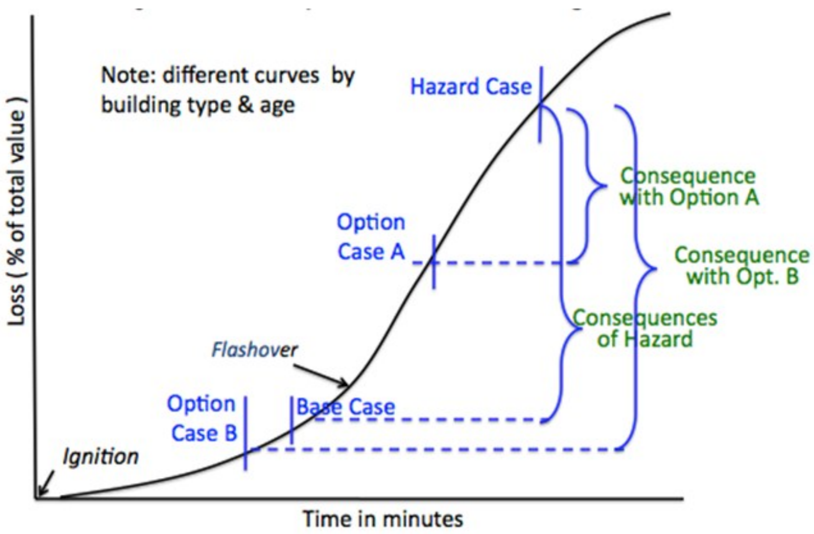


Figure 8.2 **Conceptual Model of Fire Progression**

the parameters of the curve. For each type, the y-axis represents the amount of loss up to 100% of its value (based on replacement cost or market) and its flashover inflection point in time from ignition.

The potential for conflagration would be assessed by the density of such structures. If conflagration occurs, new fire curves are added to the curve for the initial structure. The zonal "fire load" is the weighted aggregation of the proportions of each type. This, of course, requires a typology of structures relevant to fire frequency, acceleration, inflection point, etc., which is constructed from the literature and expert opinion and calibrated to actual first-due areas.

Total response times include dispatch, turnout, travel time, set-up and extinguishing agent application, which are followed by combat time and extinction, which are not included in total response time. Travel time is the key variable in the delay due to hazards. It is estimated by a binary determination (this vehicle/other) based on the amount of damage and the travel time estimated by the transportation model. Successful suppression of the fire also depends on the availability of the needed infrastructures at the incident cite, which is captured in the system-of-systems model.

8.3.2 Emergency Medical Services and other Public Safety Functions

EMS would be modeled in a fashion somewhat similar to the FS model. The incident and dispatch models differ in that the EMS service is not tied to the fire hall and is largely dependent on the continued access to hospital-based emergency rooms. Factors effecting access and function of medical service centers are critical to the function of the EMS system. The EMS vehicles and personnel arrive, assess the situation, perform triage if necessary, stabilize the victim(s) and transport those needing hospital care to the nearest emergency room equipped to handle the victim's particular complaint. For cardiac, major trauma, burns and certain other cases, rapid stabilization and delivery to the emergency room is the essential to a positive outcome. For other cases, time is less important to survival, but is still very important in terms of the way the public regards the agency and government providing the service.

As in modeling FS, modeling EMS would be primarily based on the delays in providing service – caused by the incident being analyzed – both arrival at the incident site and the transportation of victims to emergency rooms. As with EMS, a baseline level of performance is established as the basis for estimating incremental casualties due to specific incidents. These delays could be caused by incidents that happen to the EMS itself (captured in the EMS risk/resilience analysis), incidents that happen to an infrastructure system (adjusting the prior estimates of fatalities and serious injuries), or incidents above the baseline happening at random throughout the region.

Police departments provide public safety functions of a variety of types, including maintenance of order during crises, traffic and crowd control around major incident sites, control of looting, vandalism and other crime to property during major events, and directly addressing certain hazards, such as bomb threats, hazardous materials releases, etc. Some of these are amenable to modeling in ways similar to FS and EMS, but others will require very different approaches. The common thread is that they all must capture fatalities, serious injuries and property losses due to the incidents as they affect their own organizations and as they impact other systems that are part of the regional risk/ resilience analysis.

A series of planning models is needed to include all the public service functions in the RR/SAP analysis. At first, reasonable, assumption-based models would suffice, but over time, more science-based models should replace them. Part of the challenge will be to keep such models small enough and simple enough in their operations and data requirements that they can be integrated with the RR/SAP.

8.4 Public Safety Analysis based on System Dependency and Transportation Modeling

As part of this study, the team examined the impact of infrastructure performance on public safety services and established a framework for evaluation that draws upon the methodologies employed in Chapters Five, Six and Seven. As a first step in the development of the framework, the team examined dependencies for each of the public safety services – police, emergency medical services, and fire suppression. Police and EMS are dependent upon emergency communications and transportation. Fire suppression is dependent on emergency communication, transportation, water, and by extension (due to water and transportation dependency on electrical power in the study region) on electrical power.

Given its high degree of dependency, fire suppression was examined as the prototype public safety discipline for design and future development of the public safety model. The team examined the potential to use the system-of-systems model to determine the impact of an event on fire suppression and found it to be suitable for use based on its ability to run a strand -by-strand dependency analysis on a time step-by time step basis. Like the system-of systems model, the public safety model examines the interactions between the systems of interest using a tier-by-tier assessment methodology working from the bottom up as indicated in *Figure 8.3*.

The first tier examines the interaction between electrical power and water, transportation, and emergency communications. The second tier examines the interaction between fire suppression as a service and water, emergency communications, and transportation. Within the evaluation framework, the level of service (LOS) for each of the distributed service infrastructures and the mobility index for transportation is computed at each time step using the respective models – the system model for power as examined in Chapter Five, the system-of-systems model for water and emergency communication as examined in Chapter Six, and the transportation model as examined in Chapter Seven. These values are stored in a database that supports analysis of fire suppression capability on a zone-by-zone basis as illustrated in the conceptual information exchange environment shown in *Figure 8.4*.

The envisioned framework for modeling public safety operates on a requisite satisfaction basis. It solves the problem based on order of

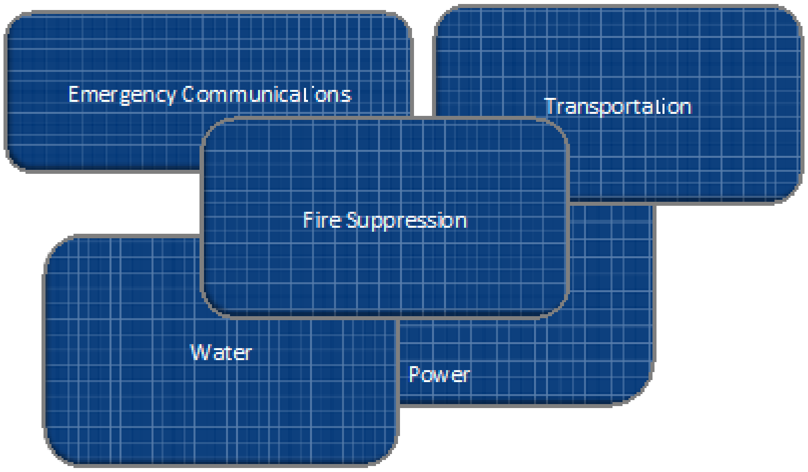
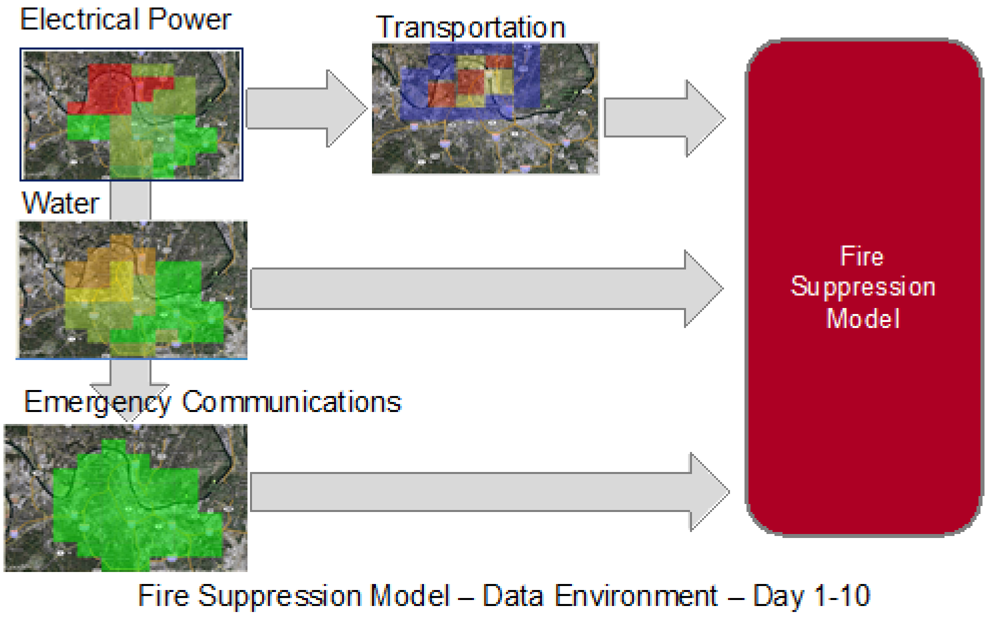


Figure 8.3 **System Dependency Model Establishing Computational Precedence**

operational precedence, which is identified by examining the lifecycle of the public safety response and evaluating each constraint.

In the case of fire suppression the operational order of precedence is – notification and dispatch, distributed water supply viability, and the ability to respond. In this example scenario, during the Day 1 to Day 10 period, emergency communication systems are operating normally and distributed water supply viability is adequate for fire suppression response across the entire region. Limitations in water supply viability in the central, northwest area are the result of pumping station outages due to electrical power failure. These limitations can be overcome in a fire response by a dedicated water management crew that dispatches to major fire events to set flow control valves to ensure a constant volume and pressure at the point of fire suppression. The major limiting factor is the ability to respond in the northwest, central area of the region as indicated by the mobility index value. During the Day 1 to Day 10 period, travel times for first responders will be significantly impacted over a 30+ square mile area. The transportation delay

Figure 8.4 **Conceptual Information Exchange Environment – Fire Suppression Model**



factor in the encumbered zones (purple) is estimated to be 2.5 times normal. Travel within the restricted access zones – those that were evacuated or cordoned off (red and yellow) – is relatively unaffected due to public access restrictions that generate levels of congestion near zero.

8.5 Framework for a Fire Loss Model

Translating the impact of the delayed response into a loss consequence requires a unique model that accounts for the impact of time on fire loss as illustrated in *Figure 8.5*. The elements in the left hand frame, and the center frame are accomplished within a specialized version of the transportation model that considers zone specific mobility index values as well as dispatch protocol within and across first-due boundaries.

For the study region, the normal response time (delay factor/mobility index = 1.0) within the unit's primary response zone is 6 minutes and in the unit's secondary response zone under "move-up" conditions, it is 9 minutes. The event-related response times are increased based on the delay factor/mobility index such that a primary response that travels wholly within the encumbered area will take approximately 15 minutes of travel time and secondary response that travels wholly within the encumbered area will take approximately 23 minutes.

Given that event-related delays increase response times, the key questions are – what is the impact on property losses, the impact on fire-related injuries (non-firefighter), and the impact on fire-related fatalities (non-firefighter)? To answer these questions, the team investigated the fire loss phenomena forming a preliminary model concept that relates key fire loss factors. The preliminary model concept for property loss was illustrated in *Figure 8.2* above.

The concept is based on generation of a chart that relates response time to loss in dollars. Response time is generated as described in the prior sub-section of this chapter. It is to be entered in minutes along the x-axis. The y-axis reflects the maximum loss in dollars for each assessment zone. This value is determined by summing the value of all structures within the zone of interest. The curve relating response time to loss is based on the combustion characteristics associated with the structures within the zone. The concept recognizes that a zone may have several structure classes that require different characteristic curves.

The shape of the characteristic curve is a function of several key factors that were identified through interviews with the fire marshals and fire department officials. The key factors include:

- Material composition of the structures within a class i.e. frame, brick veneer, masonry, etc.;
- Age of the structures reflecting the building codes that were in place at the time of construction;
- Average height of the structures considered;
- Density of structures within the land area as reflected in zoning designations; and
- Average income in the zone reflecting the condition of the structures.

Figure 8.5 **The Multi-Module Fire Loss Modeling Approach**

Through the course of the study, the team collected and analyzed data on fire losses nationwide and examined the potential for generating regional factors that would support an adaptive model as a means to determine property loss potential as a function of response time. Initial results of the data review indicate promise but additional research is required to refine the definition of key variables and to identify national-level trends and regional factors required to adjust to localized conditions. Future research will provide the basis for developing and testing the property loss component of the model and will support extension of the methodology to apply to fire-related (non-firefighter) injuries and fire-related (non-firefighter) fatalities.

CHAPTER 9

Process for Estimating Aggregate Economic Impacts and Benefits

9.1 Overview

Natural or man-made disasters bring damage to properties and critical infrastructure systems, disrupt economic productivity, and cause mortalities in extreme situations. In addition to the disruptions to infrastructure systems, these disasters can trigger a variety of economic effects including the inability of many employees to commute to work, as well as the disruptions to shipments of commodities. Destruction of critical infrastructure assets, such as electric power substations, can create cascading adverse effects across interdependent economic systems. Workforce absence translates to production losses. Delayed commodity shipments also adversely impacts production because local businesses are unable to operate at full capacity without the necessary resources.

The Regional Resilience/Security Analysis Process (RR/SAP) Phases 2 through 4 guide the estimation of owners' risk and resilience at the levels of assets, facilities, and service delivery systems and the region's direct risk and resilience based on the interacting system-of-systems. In estimating the total regional risk and resilience, they always understate the full impact because they cannot model all economic activity in the direct simulations used. This chapter describes how RR/SAP Phase 5 (*Figure 9.1*) uses regional input-output modeling to estimate the total economic risk and resilience – including all direct losses and "ripple effects." Adding the value of statistical life to the previously estimated human casualties is the total regional risk/resilience. By extension of the economic analysis, the expected losses to jobs, wages and sales taxes are also calculated.

The model is an extension of classical input-output modeling that explicitly identifies regional perturbations pursuant to disaster scenarios. Historical data pertaining to the impacts of disasters on various economic sectors are utilized as input scenarios to a dynamic input-output model, with an example based specifically on Tennessee's Nashville metropolitan area. The result is a spreadsheet-based computer tool capable of estimating the distribution of losses across the economic sectors in the region and provides a visualization capability to identify the economic sectors most heavily impacted.

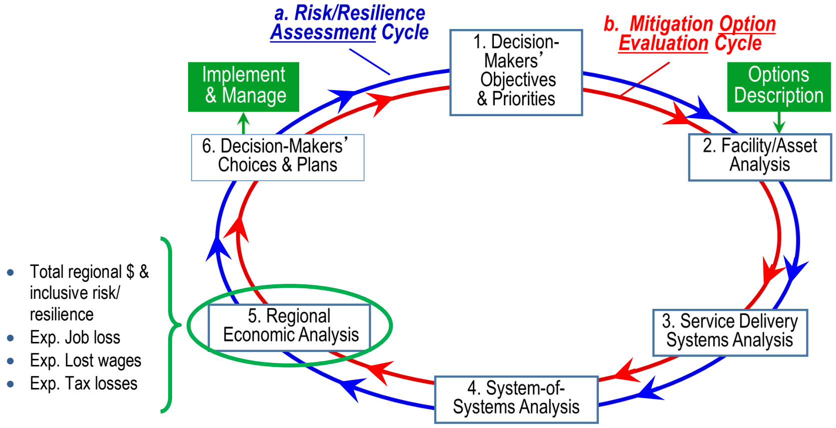


Figure 9.1 **RR/SAP Phase 5: Regional Economic Analysis**

9.2 Inoperability Input-Output Model (IIM)

9.2.1 Background and Previous Uses

At the core of the disaster risk model developed in this chapter is the concept of input-output (I-O) modeling. The I-O model views the economy as a set of interconnected sectors, which both produce and consume goods during the process of production. When the intermediate consumption is combined with the final consumer demand for products, the result is a model useful for understanding the interdependent nature of an economy (Leontief, 1936). Leontief's model has been extended and applied to myriad problems, including the effect of new technologies or taxes on the energy industry and pollution creation and elimination (Miller and Blair, 2009). Understanding the interdependencies and resulting cascading impacts from an emergency event is essential in developing an effective security plan (TISP, 2006). The I-O model is a method for modeling interdependencies across multiple sectors of a given regional economy (Leontief, 1951a, 1951b; Isard, 1960; Miller and Blair, 2009) . The National Cooperative Highway Research Program (2001) recognizes the I-O method in its guidebook for assessing the social and economic factors in infrastructure management domain. Extensions and current frontiers on I-O analysis can be found in Dietzenbacher and Lahr (2004).

The I-O model views the economy as a set of interconnected sectors, which both produce and consume goods during the process of production.

Geographic modeling and decomposition enable a more focused, and hence, a more accurate analysis of regional characteristics, as well as the associated regional interactions. Interdependencies across regions are becoming more and more prevalent due to the increasing trend in interregional transportation and trading activities. Significant segments of the working population commute across regions, as evidenced from the Journey to Work and Place of Work data (US Census Bureau, 2007). The increasing number of commodity shipments across regions bolsters the activities of the freight and trade sectors based on the Commodity Flow Survey (Bureau of Transportation Statistics, 2008). Several Lowry/Echenique I-O model derivatives are available for analysis of disruptions and their adverse effects on workforce and supply chains (e.g., Ruiz-Juri and Kockelman, 2006). The benefits of input-output-based models are many, especially with respect to modeling the effect of disruptive events on interdependent regional sectors. There exists a wealth of data that describe the relationships among the many different sectors of the economy, namely provided by the Bureau of Economic Analysis (BEA) and the U.S. Census. Furthermore, I-O data are essential components within the larger social accounting matrices used in computable general equilibrium modeling (see Minnesota IMPLAN Group 2008).

The Leontief I-O model is formulated as follows:

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c}$$

Eq. 9.1

Where:

- **x** is the production output vector (i.e., the element, x_i, denotes the output of sector *i*).
- **A** is the Leontief technical coefficient matrix (i.e., the element a_{ij} denotes the input requirement of sector *j* from sector *i*, with respect to the total input requirements of sector *j*).
- **c** is the final demand vector (i.e., the element, c_i, denotes the final demand for sector *i*).

One of the strengths of the Leontief model is that it is supported by detailed data collected and compiled by national census and statistical agencies. In the United States, for example, extensive I-O data are published by the BEA to generate the technical coefficient matrix (Miller and Blair, 2009). This methodology is coupled with the BEA's Regional Input-Output Multiplier System (RIMS II) to provide a useful framework for evaluating economic interdependencies (U.S. Department of Commerce, 1997). These data are available from BEA for the nation as a whole, each state, metropolitan regions (using the U.S. Census definitions), and counties. The availability of high-resolution economic data and social accounting matrices enables the application of I-O model and its hybrids for analysis of relatively small regions (e.g., analysis of infrastructure disruptions in Portland (Rose and Liao, 2005)). Other I-O based models can be found in U.S. Department of Transportation (DOT) (2009) and Zhao and Kockelman (2004).

Haimes and Jiang (2001) revisited the Leontief model and expanded it to account for *inoperability*, or the inability for sectors to meet demand for their output. This model, the Inoperability Input-Output Model (IIM), has been featured in several applications. Examples include modeling of infrastructure interdependencies and risks of terrorism (Santos, 2006 and 2008), multi-state regional electric power blackouts (Anderson et al., 2007), inventory management (Barker and Santos, 2010), and hurricane scenarios (Haggerty et al., 2008, Crowther et al., 2007). The IIM was also applied to problems with sequential decisions and multiple objectives, such as the biofuel subsidy analysis explored by Santos et al. (2008). Santos et al. (2007) have also formulated a conceptual framework for bridging I-O analysis with agent-based simulation for interdependent infrastructure systems.

9.2.2 Model parameters

The IIM is structurally similar to the Leontief I-O model in *Eq. 9.1*. The mathematical formulation is as follows:

$$\boldsymbol{q} = \boldsymbol{A}^{*}\boldsymbol{q} + \boldsymbol{c}^{*}$$

Eq. 9.2

Where:

- **q** is the inoperability vector (i.e., the element, q_i, denotes the inoperability of sector *i*).
- $\mathbf{A}^*$ is the interdependency matrix (i.e., the element a^*_{ij} denotes the input requirement of sector *j* that comes sector *i*, normalized with respect to the total input requirements of sector *j*).
- $\mathbf{c}^*$ is the demand perturbation vector (i.e., the element, c^*_i, denotes the demand perturbation to sector *i*).

The parameters descriptions of the IIM, as well as additional discussions on the dynamic model extensions are found below. Details of model derivation and an extensive discussion of model components are found in Santos and Haimes (2004) and also in Santos et al. (2008).

Sector Inoperability

Inoperability is conceptually related to the term unreliability, which expresses the ratio with which a sector's production is degraded relative to some ideal or "as-planned" production level. Sector inoperability (**q**) is an array comprised of 65 interdependent economic sectors. *Annex 9* (at the end of this chapter) lists the sector classifications used in the regional model and examples. The inoperability of each sector represents the ratio of unrealized production (i.e., ideal production minus degraded production) relative to the ideal production level of the industry sectors. To understand the concept of inoperability, suppose that a given sector's ideal production output is worth $100. Suppose also that a natural disaster causes this sector's output to reduce to $90. The production loss is $10, which is 10% of the ideal production output. Hence, the inoperability of the sector is 0.10. Since a region is comprised of interacting sectors, the value of inoperability will further increase due to the subsequent ripple effects caused by sector interdependencies.

Interdependency Matrix

The interdependency matrix ($\mathbf{A}^*$) is a transformation of the Leontief technical coefficient matrix (**A**), which is published by the BEA and is publicly available. It is a square matrix with 65 rows and 65 columns. The elements in a particular row of the interdependency matrix can tell how much additional inoperability is contributed by a column industry sector to the row industry sector.

When the interdependency matrix ($\mathbf{A}^*$) is multiplied with the sector inoperability ($\mathbf{q}$), this will generate the intermediate inoperability due to endogenous sector transactions. Endogenous transactions in the context of this report pertain to the flow of intermediate commodities and services within the 65 sectors. These endogenous commodities and services are further processed by the intermediate sectors (i.e., commodities and services that are not further transformed or those used immediately for final consumption are excluded from endogenous transactions). BEA's detailed I-O matrices can be customized for desired geographic resolutions using regional multipliers, or location quotients based on sector-specific economic data. This process of regionalization is performed to generate region-specific interdependency matrices like the ones used in the case studies for the Nashville metropolitan statistical area.

Demand Perturbation

The demand perturbation ($\mathbf{c}^*$) is a vector comprising of final demand disruptions to each sector in the region. The demand perturbation, just like the inoperability variable in the basic IIM shown in *Eq. 9.2*, is normalized between 0 and 1. In this basic IIM formulation, supply disruptions are modeled as "forced" demand reductions. Consider a hypothetical disruption where the supply for a commodity or service decreases but demand remains virtually unaffected. In this case, the consumers will have to temporarily sacrifice their need for that commodity or service until it bounces back to its as planned supply level. The limitation of the basic model in *Eq. 9.2* is that it uses "forced" demand reduction as a surrogate to supply reduction. To address this shortcoming, the dynamic extension to the IIM was developed to enable a more explicit definition of perturbation parameters, in addition to the formulation of a sector-specific economic resilience matrix.

Economic Resilience

A key motivation that led to the development of the dynamic IIM is the need for linking the concept of economic resilience with time-varying sector inoperability for a given recovery horizon. In general, resilience is defined as the ability or capability of a sector to absorb or cushion against damage or loss (Holling, 1973, and Perrings, 2001). Rose and Liao (2005) suggest that resilience can be enhanced through:

1. Expedited restoration of the damaged capability;
2. Using an existing back-up capability;
3. Conservation of inputs to compensate for supply shortfalls;
4. Substitution of inputs; or
5. Shifting of production locations, among others.

Rose (2009) provides comprehensive definitions and categories of economic resilience including static, dynamic, inherent, and adaptive.

The dynamic formulation of the IIM takes into account the economic resilience of each sector, which influences the pace of recovery of the interdependent sectors in the aftermath of a disaster. The formulation is as follows:

$$\boldsymbol{q}(t+1) = \boldsymbol{q}(t) + \boldsymbol{K}(\boldsymbol{A}^*\boldsymbol{q}(t) + \boldsymbol{c}^*(t) - \boldsymbol{q}(t)) \qquad \textit{Eq. 9.3}$$

The term, $\mathbf{K}$, is a sector resilience coefficient matrix that represents the rates at which sectors recover to their nominal levels of production following a disruption (Lian and Haimes 2006). The model dictates that the inoperability level at the following time step, $\mathbf{q}(t+1)$, is equal to the inoperability at the previous stage, $\mathbf{q}(t)$, plus the effects of the resilience of the sector. The values of $\mathbf{K}$ tend to be negative or zero, thereby detracting from the overall level of inoperability. As seen in *Eq. 9.3*, $\mathbf{K}$ is multiplied with the indirect inoperability resulting from other sectors, $\mathbf{A}^*\mathbf{q}(t)$, plus the degraded final demand, $\mathbf{c}^*(t)$, minus the current level of inoperability, $\mathbf{q}(t)$. The resilience coefficient, $\mathbf{K}$, is assumed to be an inherent characteristic of a particular sector, but multiplying it with the inoperability product term, $\mathbf{A}^*\mathbf{q}(t)$, will result in coupled resilience across directly related sectors. This is particularly relevant when analyzing a sector that heavily depends on another sector for achieving its as-planned productivity levels. Regardless of how inherently resilient a sector is, its productivity will be significantly compromised when another sector it heavily depends on becomes largely inoperable in the aftermath of a disaster.

The dynamic extension (*Eq. 9.3*) answers one of the fundamental limitations of the basic IIM (*Eq. 9.2*), which is the ability to capture time-varying recovery that adapts to some *a priori* and current levels of inoperability within the perturbation and recovery period. For the dynamic extension to the IIM, Lian and Haimes (2006) provide the formulation to estimate the sector resilience coefficient of each sector. This resilience coefficient is a function of:

1. Sector inoperability;
2. Sector interdependencies;
3. Recovery period; and
4. the desired level of inoperability reduction for the target recovery period.

In this economic resilience formulation, economic resilience is inversely proportional to the recovery period. This is because resilience is a desired attribute of any system and, hence, a higher level of resilience is preferred. On the other hand, recovery period (i.e., the time it takes to reach full recovery) is desired to be at minimum to the extent possible. The higher the value of the sector resilience metric, the better equipped it is to protect and recover itself from external perturbations. Hence, increasing the economic resilience metric of a sector reduces its recovery period as well as the associated economic losses.

The dynamic version of the IIM is capable of analyzing the extent to which sector resilience can decrease the magnitude of sector inoperabilities and economic losses, as well as shorten the recovery period. This formulation would create a time-dependent value to better account for the impact of different intensities and durations of a disaster, as longer ones would tend to further stress the sectors impacting their ability to recover. Lian et al. (2007), Santos (2006), Lian and Haimes (2006), and Haimes et al. (2005) applied the model to various regional disaster scenarios to analyze the recovery behaviors of critical economic sectors and infrastructure systems.

Economic Loss

Similar to sector inoperability, economic loss is comprised of 65 interdependent economic sectors. Each element in this array indicates the magnitude of economic loss of each sector, in monetary units (or particularly in US dollars for the scenarios explored in the case studies). The economic loss of each sector is simply the product of the sector inoperability and the ideal production output. For example, an inoperability of 0.1 for a sector whose production output is \$100 will result in an economic (or production) loss of \$10. Economic loss is treated as a separate disaster metric since it complements and supplements the inoperability metric. Both the inoperability and economic loss metrics are desired to be kept at minimum. It is also worth noting that when the 65 sectors are ranked according to the magnitude of their inoperability and economic loss metrics, two distinct rankings will be generated. Suppose that a second sector has an inoperability of 0.2 and a production output of \$40. The resulting economic loss will be 0.2´\$40 = \$8. Although the inoperability of the second sector (0.2) has a higher rank compared to the first sector (0.1), the direction of priority will reverse when economic loss is considered as the sole basis for ranking. To wit, the second sector has an economic loss of \$8, which has a lower rank in contrast to the first sector's \$10 economic loss.

9.2.3 Databases for the Example Metropolitan Region

Disasters can cause severe damage to existing infrastructure – consequently affecting economic productivity. Temporary closure of factories and stores, loss of mobility due to flooding and debris cleanup, repair of damaged infrastructure systems (among others) can drastically affect workforce and commodity flows for prolonged periods of time. Reduction in worker flow decreases productivity, reduction in commodity flow results in cascading demand and supply impacts, and social flows will impact business accessibility. Using detailed journey-to-work data, commodity flow surveys, and social accounting matrices permits the modeling of disruptions to regional productivity. Modeling efforts include the potential for cascading failure, accounting for spatial dependencies and various economic and social travel patterns.

A region expects substantial disruptions to infrastructure capacity, as well as workforce availability and mobility in the aftermath of a disaster. These disruptions in turn can trigger sector productivity degradations. In order to quantify the impact of reduced sector productivity levels on the economy of Nashville, economic data (e.g., input requirements, commodity outputs, and income statistics, among others) for each sector of the region are collected and assembled from different sources.

Sector Classifications

This report configures the data collection methodology using the North American Industry Classification System (NAICS). RIMS II adopts an aggregated version of the detailed sector classification – comprising of 65 sectors (see *Table 9.1*) (U.S. Department of Commerce, 1997).

Input-Output Matrices

In a simplified I-O model formulation, each industry is assumed to produce a distinct commodity. The term “commodity” in this report refers to the output of an industry, which can take the form of goods or services. Realistically however, it is possible that a given industry produces more than one commodity. In addition, a given commodity may not be a unique output of an industry. The BEA makes distinctions between an industry and a commodity in its published I-O data via the “industry-by-commodity” and “commodity-by-industry” matrices. *Figure 9.2*, adapted from Miller and Blair (2009), shows a summary of the types of national I-O accounts maintained by the BEA.

The *make* matrix, denoted by **V**, would show the monetary values of the different column commodities *produced* by the different row industries. The *use* matrix on the other hand,

	Commodity	*Industry*		
Commodity		Use Matrix (**U**)	Exogenous Demand (**e**)	Total Commodity Output (**y**)
Industry	Make Matrix (**V**)			Total Industry Output (**x**)
		Value Added ($\mathbf{z}^T$)		
	Total Commodity Input ($\mathbf{y}^T$)	Total Industry Input ($\mathbf{x}^T$)		

Figure 9.2 **Summary of economic I-O accounts**

denoted by **U**, would show the monetary values of the different row commodities *consumed* by the different column industries. These matrices are typically associated with the following vectors: (1) **e** refers to the commodity-based exogenous (or final) demand; (2) **y** refers to the commodity-based output; (3) **x** refers to the industry-based output; and (4) **z** refers to the value added. Note that *Figure 9.1* does not directly specify the I-O matrix representing an industry-by-industry matrix. Hence, the make and use matrices are normalized first with respect to their column totals, and are then multiplied with each other. The resulting product matrix is typically known as the industry-by-industry technical coefficient matrix in I-O parlance. A column of this matrix shows the input contribution of the row industries to the column sector, expressed as a proportion of the total input requirements of that column sector. The technical coefficient matrix is used for computing the elements of the interdependency matrix of the IIM (i.e., the notation $\mathbf{A}^*$ in *Eq. 9.1*).

Gross Domestic Product

Gross Domestic Product (GDP) consists of final consumption – other than those used as intermediate production inputs to the 65 endogenous sectors. As such, GDP is also interpreted as the value of final uses (or consumptions), which includes personal consumption expenditure, gross private domestic investment, government purchases, and net foreign exports (i.e., difference in exports and imports) (Miller and Blair, 2009). Since the value of GDP is theoretically equal to the gross domestic income, it is also defined by BEA as "the market value of goods and services produced by labor and property in the United States, regardless of nationality; GDP replaced gross national product (GNP) as the primary measure of U.S. production in 1991" (BEA, 2011). GDP data is also available for all states and metropolitan areas within the United States.

Local Area Personal Income

Local Area Personal Income (LAPI) refers primarily to the wages paid to the workers in a given region. Other components of LAPI include "supplements to wages and salaries, proprietors' income with inventory valuation adjustment (IVA) and capital consumption adjustment (CCAdj), rental income of persons with CCAdj, personal dividend income, personal interest income, and personal current transfer receipts, less contributions for government social insurance." (BEA 2011) LAPI data are available for each of the 65 sectors. To convert the output of disaster impact into a measure of workforce sector inoperability, there needs to be a way to translate a percentage decrease in workforce availability into a measure of sector inoperability. Arnold et al. (2006) accomplished this through estimates of worker productivity. To generate worker impact for the RIMS II sectors, the ratio of LAPI to industry output is computed (BEA 2008). The LAPI provides the value of workforce to the industry (the market value of the laborers' work) and dividing this by the industry output gives the proportion of output that is dependent on the workforce. This calculation of inoperability for a given sector is shown in *Eq. 9.4*.

Sector Inoperability =
(Unavailable Workforce / Size of Workforce) ×
(LAPI / Sector Output)

Eq.9.4

The impact on workers is then multiplied with the number of workers in that sector that are unavailable divided by the number of workers in that sector (giving percentage of workers missing) to determine overall sector inoperability. A case in point, Burrus et al. (2002) developed a comprehensive survey describing the impact of various disaster intensities on workforce availability. The sectors included in their survey are similar to the RIMS II classification employed in the study. Such historical workforce recovery data can be used to formulate the time-varying recovery functions.

Employment Numbers by Industry

Employment data are available for different states and metropolitan areas. For example, BEA publishes annual estimates of the total full-time and part-time employment by NAICS industry.

These employment numbers are available only for a subset of the 65 sectors in the IIM. Hence, the regional *per capita income* can serve as a basis for estimating the number of workers in sectors with missing data. These sector-specific employment numbers are used in determining the equivalent number of jobs lost within the disaster horizon.

9.3 Description of Tool

The decision support tool utilized in this Phase of the RR/SAP comprises a front-end graphical user interface (GUI) developed in Microsoft Excel. The spreadsheet tool comprises of five modules:

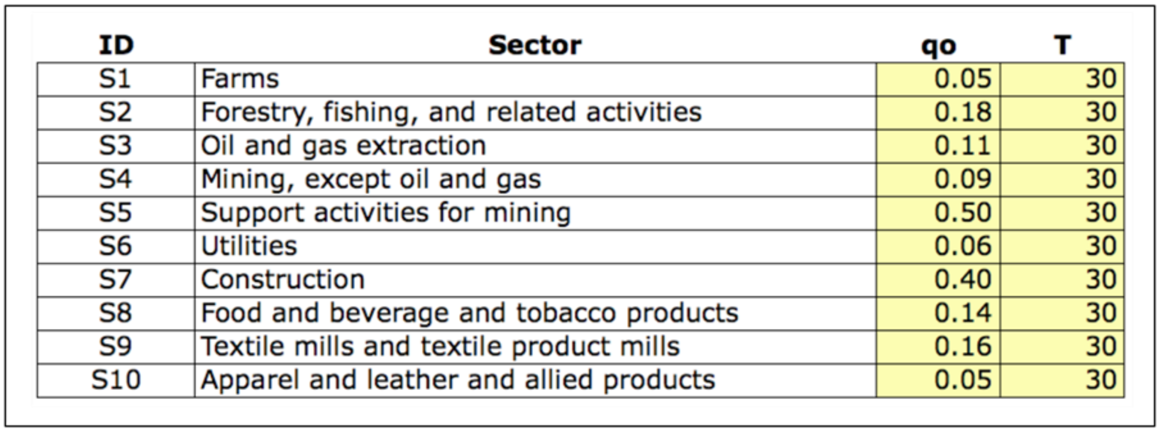
1. Scenario generation;
2. Computation;
3. Visualization;
4. Prioritization and sensitivity analysis; and
5. Data analysis.

These modules are described as follows:

9.3.1 Scenario Generation Module

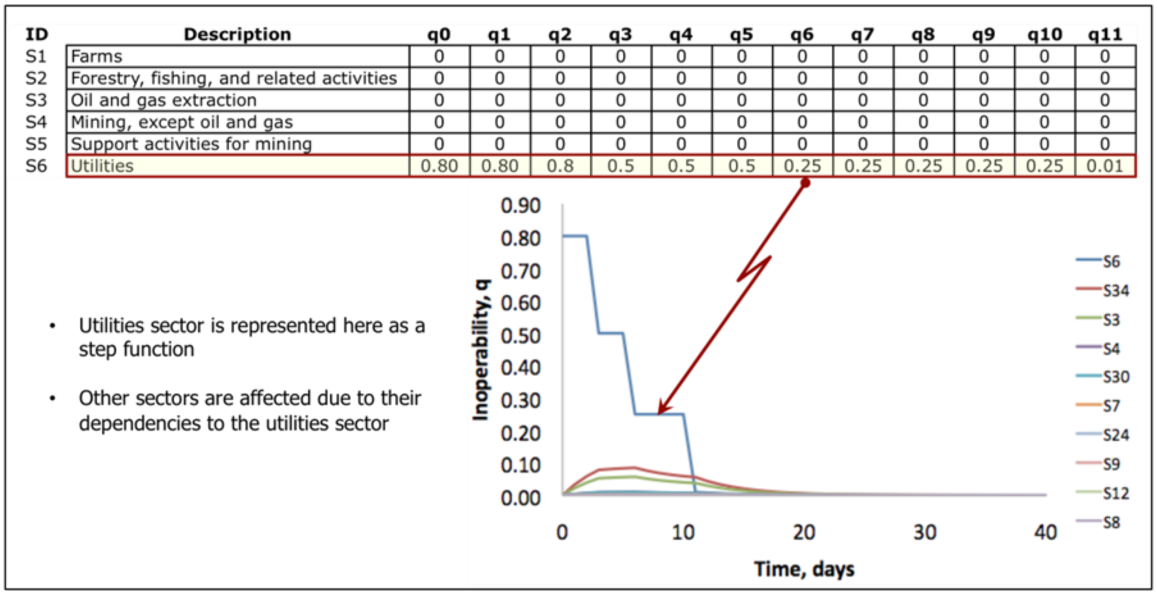
The scenario generation module enables the user to provide the model scenario inputs. The user is asked to enter the initial inoperability for each of the 65 sectors, as well as the time it takes to achieve full recovery. Initial inoperability (denoted by q_0) is a number between 0 and 1, which describes the extent to which a given sector's production capacity is initially affected (i.e., 0.1 means that 10% of the production capacity is rendered inoperable by a disaster). On the other hand, the time to recovery (denoted by T) is the time that it is expected to take a sector to recover to its pre-disaster production level. In the model, the time to recovery is measured in days. In the absence of recovery period data for some sectors, a similar value for a sector with known recovery period can be used. The reasoning behind this is that a given sector – even if it is not directly affected by a disaster – will match (or even exceed) the recovery period of a sector that it is coupled with. By the same token, a sector whose dependence on other sectors is minimal will virtually remain unaffected regardless of the assumed recovery period. *Figure 9.3* shows a partial screenshot of the scenario generation component with arbitrary parameter inputs.

In addition, an advanced feature of the model allows the user to enter not only the initial inoperability values (q_0), but the subsequent inoperability values across the recovery period as well (e.g., q_1, q_2, q_3, etc.). This is particularly useful for disaster scenarios with known inoperability and recovery trends, such as estimated in RR/SAP Phases 2 through 4. This advanced feature also allows users to perform inoperability adjustments whenever risk management actions are introduced within the



ID	Sector	qo	T
S1	Farms	0.05	30
S2	Forestry, fishing, and related activities	0.18	30
S3	Oil and gas extraction	0.11	30
S4	Mining, except oil and gas	0.09	30
S5	Support activities for mining	0.50	30
S6	Utilities	0.06	30
S7	Construction	0.40	30
S8	Food and beverage and tobacco products	0.14	30
S9	Textile mills and textile product mills	0.16	30
S10	Apparel and leather and allied products	0.05	30

Figure 9.3 **Screenshot of Scenario Definition GUI component**



ID	Description	q0	q1	q2	q3	q4	q5	q6	q7	q8	q9	q10	q11
S1	Farms	0	0	0	0	0	0	0	0	0	0	0	0
S2	Forestry, fishing, and related activities	0	0	0	0	0	0	0	0	0	0	0	0
S3	Oil and gas extraction	0	0	0	0	0	0	0	0	0	0	0	0
S4	Mining, except oil and gas	0	0	0	0	0	0	0	0	0	0	0	0
S5	Support activities for mining	0	0	0	0	0	0	0	0	0	0	0	0
S6	Utilities	0.80	0.80	0.8	0.5	0.5	0.5	0.25	0.25	0.25	0.25	0.25	0.01

- Utilities sector is represented here as a step function
- Other sectors are affected due to their dependencies to the utilities sector

Figure 9.4 **Screenshot of Scenario Definition GUI Component**

recovery period. The annotated diagram in *Figure 9.4* explains this advanced feature for a sector with a recovery trend similar to a step function.

9.3.2 Computation Module

This is the computing engine of the program containing the codes for the IIM. This module stores the simulation rules and algorithms needed for executing the IIM and its dynamic recovery model extensions. This module also includes the algorithms for visualizing the model results, namely the inoperability and economic loss for each sector and for each day within the recovery period.

In the computer tool, sector recovery is modeled as a time-varying function instead of static or predetermined value as formulated previously. The resilience coefficient (discussed in Section 9.2.2) for each sector represents the ability of a sector to recover from some level of inoperability to a final level of inoperability in a given period of time. As a regional economy and its associated sectors recover from a large-scale disruption, the nominal resilience coefficients are expected to fluctuate. The reasoning behind this is that as sectors utilize inventories and capital resources to recover and mitigate the impacts of a disaster, they deplete these resources and thus are less able to recover. The pace of recovery is further compounded by sector interdependencies – creating indirect effects that continue to disrupt regional productivity. The new formulation of the resilience coefficient includes a variety of factors, including the current inoperability value, previous inoperability values (giving measures of trends and duration) and nominal sector recovery rates to determine a baseline scenario.

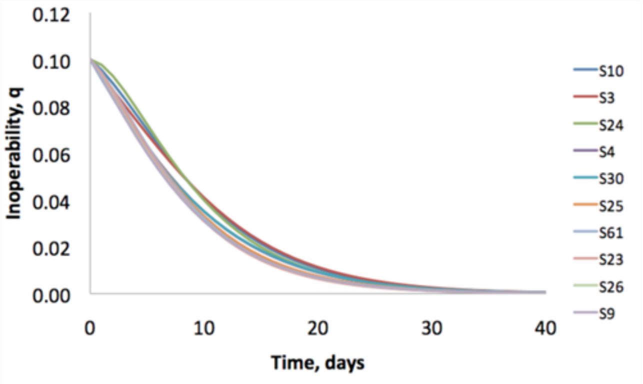
9.3.3 Visualization Module

The visualization module enables the user to view the recovery behaviors of the critical sectors given the parameter values entered in the scenario definition stage. The critical sectors are selected as the top 10 sectors (out of 65) with respect to the two primary metrics of the IIM, which are *inoperability* and *economic loss*. The rankings based on these two metrics are generally different, as explained in Section 9.2.2.

The following figures give sample visualizations of how inoperability and economic loss evolve across the recovery period. Although not directly included in the visualization, other important disaster consequence metrics are extrapolated from the economic loss estimates. These include tax loss, income loss, and equivalent number of jobs lost for the applicable recovery period. These loss estimates are provided in each of the scenarios explored in Section 9.4.

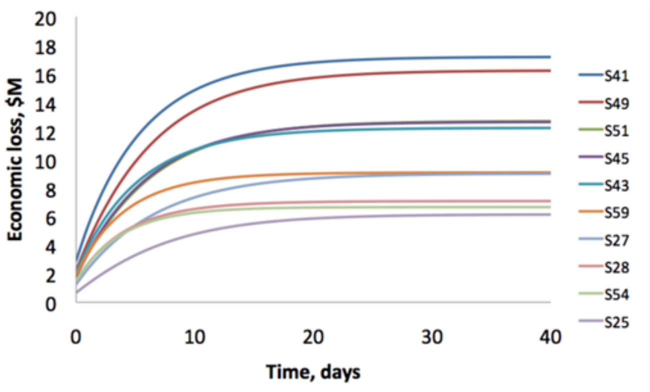
Figure 9.5 provides a sample depiction of the top 10 sectors with largest inoperability values. Inoperability rankings are based on magnitude of sector disruptions, normalized relative to sector total output. A uniform sector disruption scenario is applied to all 65 sectors to show the key sectors based on the inoperability metric. Inoperability metric highlights sectors that are tightly coupled with other sectors regardless of their economic values, such as: manufacturing (S10, S25, S23, S26, S9); oil and gas, mining (S3, S4); and transportation (S24, S30).

On the other hand, *Figure 9.6* depicts the associated top 10 sectors with largest economic losses. Economic loss rankings are based on cumulative economic losses incurred prior to full recovery. The same uniform initial disruption is applied to all 65 sectors to show the key sectors based on the economic loss metric. Economic loss metric highlights sectors that have higher production values, measured in monetary unit, such as: banks, insurance (S41, S43); computer systems (S49); administrative services (S51); real estate (S45); and trade (S27, S28).



S10	Apparel and leather and allied products
S3	Oil and gas extraction
S24	Other Transportation equipment
S4	Mining, except oil and gas
S30	Rail transportation
S25	Furniture and related products
S61	Other services, except government
S23	Motor vehicles, bodies and trailers, and parts
S26	Miscellaneous manufacturing
S9	Textile mills and textile product mills

Figure 9.5 **Top 10 sectors with largest inoperability**



S41	Federal Reserve banks and credit intermediation
S49	Computer systems design and related services
S51	Administrative and support services
S45	Real estate
S43	Insurance carriers and related activities
S59	Accommodation
S27	Wholesale trade
S28	Retail trade
S54	Ambulatory health care services
S25	Furniture and related products

Figure 9.6 **Top 10 sectors with largest inoperability**

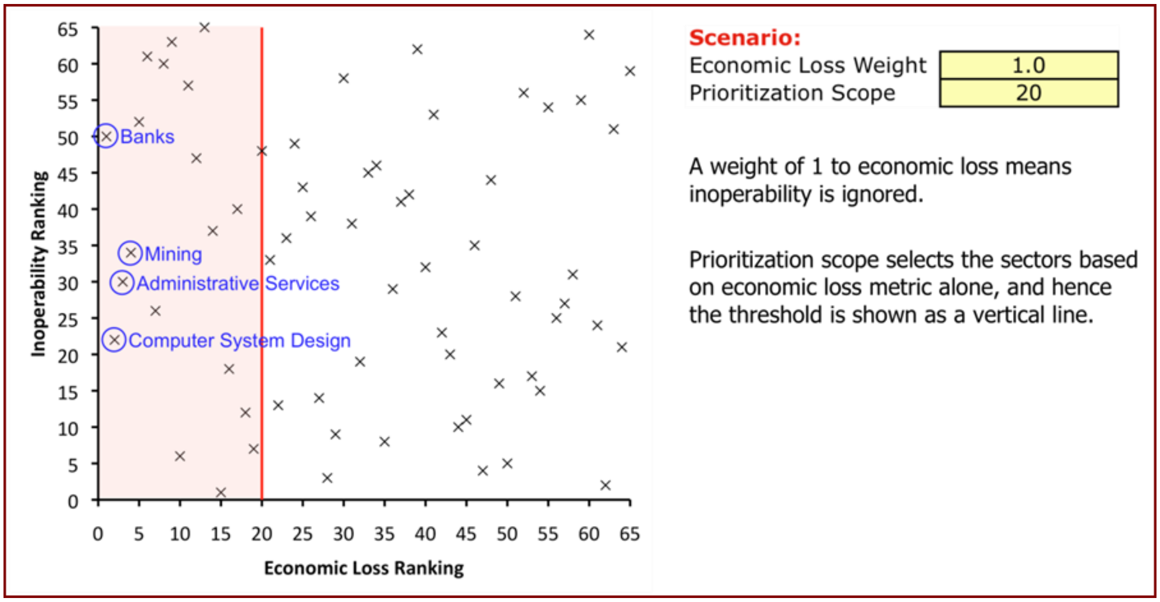
9.3.4 Prioritization Sensitivity Analysis Module

The tool is capable of visually searching for critical economic sectors that support two minimization objectives, which are economic loss and inoperability. We utilize the dynamic cross prioritization plot (DCPP) that uses more flexible threshold regions to capture critical sectors with varying preferences for the economic loss and inoperability objectives (Resurreccion and Santos, 2011). That is, the use of an arc orientation that captures more points closer to the x-axis (y-axis) to highlight the higher preference for the inoperability (economic loss) objective than the economic loss (inoperability) objective. Hence, the DCPP module can provide additional information on identifying and prioritizing the economic sectors that are expected to suffer the greatest consequences from a disaster scenario. These inoperability and economic loss consequences, as well as the extrapolated fiscal losses (i.e., tax loss, income loss, and equivalent number of jobs lost) can provide insights in planning for enhancements of regional resilience (e.g., backup capabilities, additional inventories, and production input substitutions, among others).

The prioritization sensitivity analysis module requires two categories of user inputs: (1) preference structure for economic loss and inoperability objectives; and (2) prioritization scope to determine the size of the prioritization filter. The user is asked for the economic loss weight, or the relative importance of the economic loss objective with respect to inoperability. A scale of 0 to 1 is used, with the following interpretations:

- A value of 1 means economic loss is the only objective that matters (see *Figure 9.7*);
- A value of 0.5 means economic loss is equally preferred to inoperability (see *Figure 9.8*); and
- A value of 0 means inoperability is the only objective that matters (see *Figure 9.9*).

In addition, the tool requires the user to enter a prioritization scope – a positive integer that can be adjusted to set the size of the prioritization area. This integer is increased when more sectors are to be prioritized, and decreased when fewer

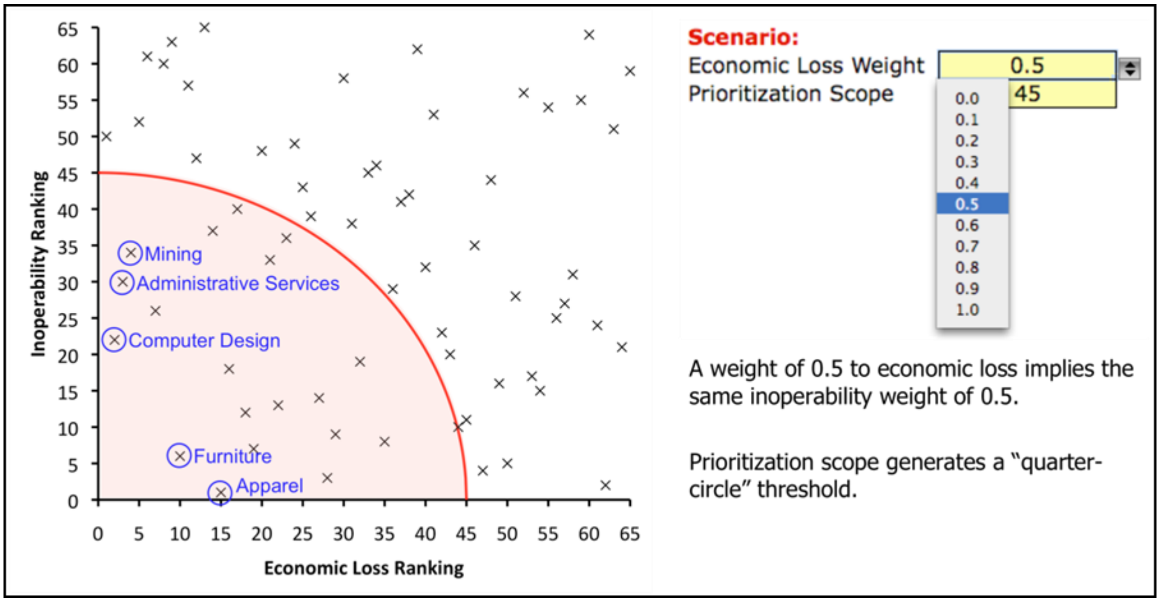


Scenario:
Economic Loss Weight 1.0
Prioritization Scope 20

A weight of 1 to economic loss means inoperability is ignored.

Prioritization scope selects the sectors based on economic loss metric alone, and hence the threshold is shown as a vertical line.

Figure 9.7 **Prioritization using economic loss objective only**

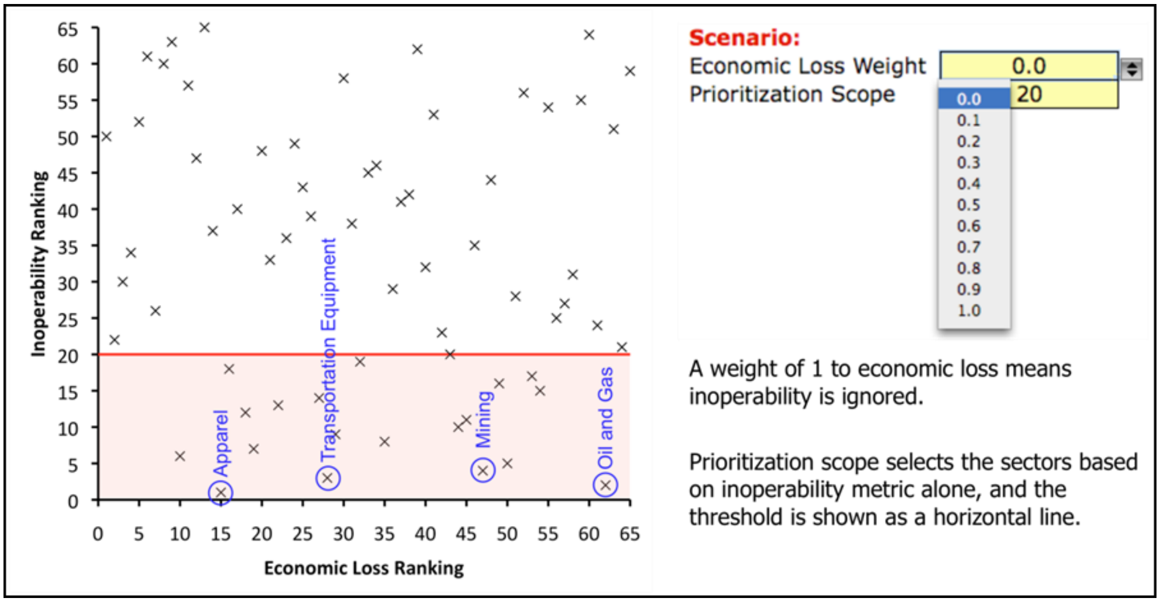


Scenario:
Economic Loss Weight 0.5
Prioritization Scope 45

A weight of 0.5 to economic loss implies the same inoperability weight of 0.5.

Prioritization scope generates a "quarter-circle" threshold.

Figure 9.8 **Prioritization with equal weights for economic loss and inoperability objectives**



Scenario:

Economic Loss Weight 0.0

Prioritization Scope 20

A weight of 1 to economic loss means inoperability is ignored.

Prioritization scope selects the sectors based on inoperability metric alone, and the threshold is shown as a horizontal line.

Figure 9.9 **Prioritization using inoperability objective only**

sectors can be prioritized (e.g., a budget constraint).

9.3.5. Data Module

The data module contains the relevant regional economic data. Examples of economic data that have been already described in *Section 9.2.3* are I-O matrices, GDP, LAPI and employment statistics. These data are specific to the Nashville metropolitan region. In addition to the foregoing data sets, the spreadsheet tool also houses data extrapolated from other sources. These extrapolated data sets are used for estimating regional fiscal losses such as tax opportunity losses, personal income losses and employment losses.

Tax Loss Estimation

Here, we assume that significant portions of the tax revenues collected at the county and state levels are pegged to the level of economic activity of the region. Examples of such tax categories include sales and use taxes, which are typically taken as percentages of the commodities and services sold locally. For the state of Tennessee (which encompasses Nashville), the sales tax rate for food is 5.5% and 7% for other merchandise. Rates for use taxes are the same as sale taxes. "It [use tax] is applied when merchandise (tangible personal property) is purchased from outside the state of Tennessee and imported into the state for use or consumption" (Tennessee Department of Revenue, 2011).

The following equation provides an estimate of sales and use tax losses for each sector *i*. Note that there are 65 sectors.

$$Tax\ Loss_i = (\ PCE_i \div x_i\ ) \times (\Delta x_i) \times (tax\ rate_i) \qquad Eq.\ 9.5$$

Where:

- **PCE$_i$** is the Personal Consumption Expenditure for sector *i*.
- **x$_i$** is the total output of sector *i* in the region.
- **Δx$_i$** is the economic loss of sector *i* for a given disaster scenario, as computed by the model.
- **tax rate$_i$** is the applicable sales tax rate for sector *i* in the region.

Because of the current capability of the I-O model to estimate production output losses, sales and use tax losses will be estimated based on the percentage of the PCE relative to regional output. Other tax categories include property, excise, licenses and fees, and income, among others.

Due to the current data module limitations on tax analysis, the computer tool is only capable of estimating losses from sales and use taxes.

Income Loss Estimation

Here, we focus our analysis on extrapolated data based on LAPI. As discussed previously, LAPI is available for each of the 65 sectors. For each sector *i*, we first compute the proportion of LAPI with respect to the total regional output. When this proportion is multiplied with the production output loss of a particular sector *i* (due to a disaster), this will provide an estimate of the income loss for sector *i* and is formulated as follows:

$$\textit{Income Loss}_i = (LAPI_i \div x_i) \times (\Delta x_i) \qquad \textit{Eq. 9.6}$$

Where:

- $\mathbf{LAPI}_i$ is the Local Area Personal Income for sector *i*.
- $\mathbf{x}_i$ is the total output of sector *i* in the region.
- $\mathbf{\Delta x}_i$ is the economic loss of sector *i* for a given disaster scenario, as computed by the model.

Note that the loss estimated in the above formulation pertains to the aggregated income losses suffered by the workforce in sector *i*. Computation of the corresponding income tax loss by the local government can be complex (i.e., considering the different income tax brackets, federal versus state distribution, disaster tax reliefs, etc.). Hence, extracting the associated income tax loss from the computed income loss is beyond the current scope of the current study.

Employment Losses

Tradition I-O employment multipliers analysis enables the computation of additional jobs created due to an increase in demand (and subsequently, production) of commodities and services for particular sectors. A similar concept is implemented here for estimating job losses that can stem disaster-induced income losses. The formulation for job losses[18] in each sector *i* is as follows:

$$\textit{Job Loss}_i = (\textit{Income Loss}_i \div LAPI_i) \times (\textit{Workers}_i) \qquad \textit{Eq. 9.7}$$

Where:

- $\mathbf{Job\ Loss}_i$ is the number of jobs lost in sector *i.*
- $\mathbf{Income}_i$ is the workforce income loss in sector *i.*
- $\mathbf{LAPI}_i$ is the local area personal income sector *i.*
- $\mathbf{Workers}_i$ is the number of workers in sector *i.*

9.4 Worked Examples with Screenshots

Disaster consequences encompass reductions in workforce productivity, loss of lives, and social disequilibrium. Workforce productivity losses can significantly decrease a sector's output regardless of the efficiency of other production factors. The objective of the case studies is to manage impacts of various disaster scenarios in Nashville using available economic and survey data. This section demonstrates the use of the IIM and its dynamic extensions to assess the impacts of disaster scenarios on the Nashville's economic sectors. Data sets assembled from various economic and census agencies include I-O matrices, GDP data, local area personal income data, and employment numbers, among others.

The following sections demonstrate the application of the IIM using different cases. Each case is introduced with scenario descriptions, as well as a summary of the different loss categories that could be of interest to regional policymakers. Recall that the two primary consequence categories provided by the IIM are *inoperability* and *economic loss*. The economic loss variable is denoted by Δx_i (see *Eqs. 9.5 and 9.6*) and is computed by the IIM for each of the 65 sectors. These economic loss

---

[18] Available data does not distinguish counts of full-time and part-time workers.

values serve as the basis for estimating different categories of regional losses, including:

- Tax loss;
- Income loss; and
- Equivalent number of jobs lost.

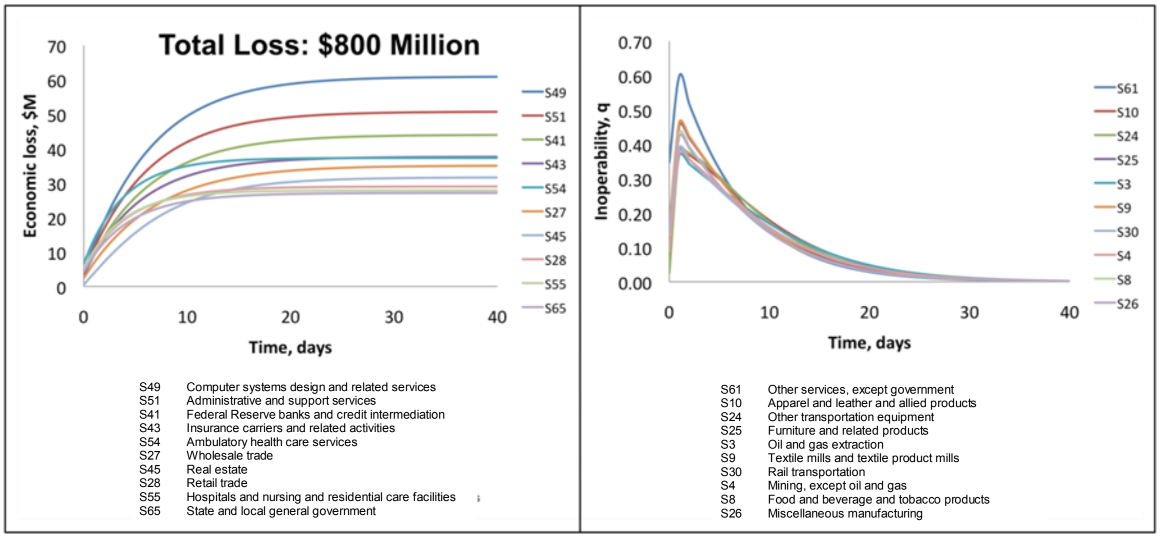
In addition, the rankings of the critical sectors according to the inoperability and economic loss metrics are shown, along with the associated visualization outputs of the IIM. The DCPP tool also provides sample prioritization of key sectors based on priority assignments to the inoperability and economic loss objectives. As discussed in *Section 9.3.4*, the DCPP results can identify the economic sectors that are expected to suffer the greatest consequences from a disaster scenario and can help in formulating policies for enhancing regional resilience.

9.4.1 Case 1 – Modeling Workforce Disruption

Consider a disaster that hits the Nashville region, causing an initial inoperability of 50% to all its workforce sectors. For this scenario, it is assumed that inoperability decreases exponentially and recovery is achieved over a 30-day horizon. The parameters that describe the initial effects of the disaster scenario are entered into the dynamic IIM and generate the economic loss and inoperability charts in *Figure 9.10*. The total economic loss for the simulated scenario is $800 million. From this economic loss, the following losses can be estimated based on the approaches discussed in *Section 9.3.5* (note that these losses are incurred only within the assumed recovery period of 30 days):

- Tax loss: $7,221,193
- Income loss: $108,013,667
- Equivalent number of jobs lost: 2,465 jobs

The top 10 sectors that suffer the highest economic losses (*Figure 9.10*, left panel) are: computer systems design and related services (S49); administrative and support services (S51); federal reserve banks and credit intermediation (S41); insurance carriers and related activities (S43); ambulatory health care services (S54); wholesale trade (S27); real estate (S45); retail trade (S28); hospitals and nursing and residential care facilities (S55); and state and local government (S65). The top 10 sectors account for 48% of the total regional economic loss. It can also be observed that the economic losses increase sharply in the first 10 days, and start to "flatten out" after approximately 20 days. The inoperability charts indicate that recovery is almost completely achieved in 30 days.



S49	Computer systems design and related services
S51	Administrative and support services
S41	Federal Reserve banks and credit intermediation
S43	Insurance carriers and related activities
S54	Ambulatory health care services
S27	Wholesale trade
S45	Real estate
S28	Retail trade
S55	Hospitals and nursing and residential care facilities
S65	State and local general government

S61	Other services, except government
S10	Apparel and leather and allied products
S24	Other transportation equipment
S25	Furniture and related products
S3	Oil and gas extraction
S9	Textile mills and textile product mills
S30	Rail transportation
S4	Mining, except oil and gas
S8	Food and beverage and tobacco products
S26	Miscellaneous manufacturing

Figure 9.10 **Top 10 critical sectors for Case 1 ranked according to: Economic loss (left) and Inoperability (right)**

For the same scenario, the top 10 sectors with highest inoperability values (*Figure 9.10*, right panel) are: other services, except government (S61); apparel and leather and allied products (S10); other transportation equipment (S24); furniture and related products (S25); oil and gas extraction (S3); textile mills and textile product mills (S9); rail transportation (S30); mining, except oil and gas (S4); food and beverage and tobacco products (S8); and miscellaneous manufacturing (S26).

The inoperability and economic loss rankings are different because the production outputs of the sectors could vary by orders of magnitude. As such, a sector that suffers a relatively low economic loss value can have a critical ranking in inoperability if its total production output is also lower relative to other sectors. By the same token, a sector with a relatively low inoperability value can have a critical ranking in economic loss if its total production output is significantly higher compared to the other sectors.

The DCPP tool enables the users to perform sensitivity analysis with respect to how they structure their preference between the economic loss and inoperability objectives. Two sample scenarios are presented in *Figure 9.11*. The vertical region corresponds to a preference strategy that gives importance to economic loss only, while the quarter-circle region corresponds to assigning equal weights to inoperability and economic loss objectives. For a purely economic loss-minimizing strategy, there is a risk to exclude sectors that have critical ranking with respect to inoperability (e.g., transportation equipment). For the equal weighting strategy, equal priority is allocated between economic loss and inoperability. Nevertheless, there is also a risk of excluding sectors with critical economic loss rankings in this equal weighting strategy (e.g., banking and insurance). Hence, prioritizing sectors for recovery need careful consideration of the balance between economic loss and inoperability.

9.4.2 *Case 2 – Infrastructure Disruption with "Flat" Recovery Function*

Suppose that Case 1 is expanded such that in addition to the 50% initial workforce inoperability, there is a constant 80% electric power outage[19] that persists for 10 days. These

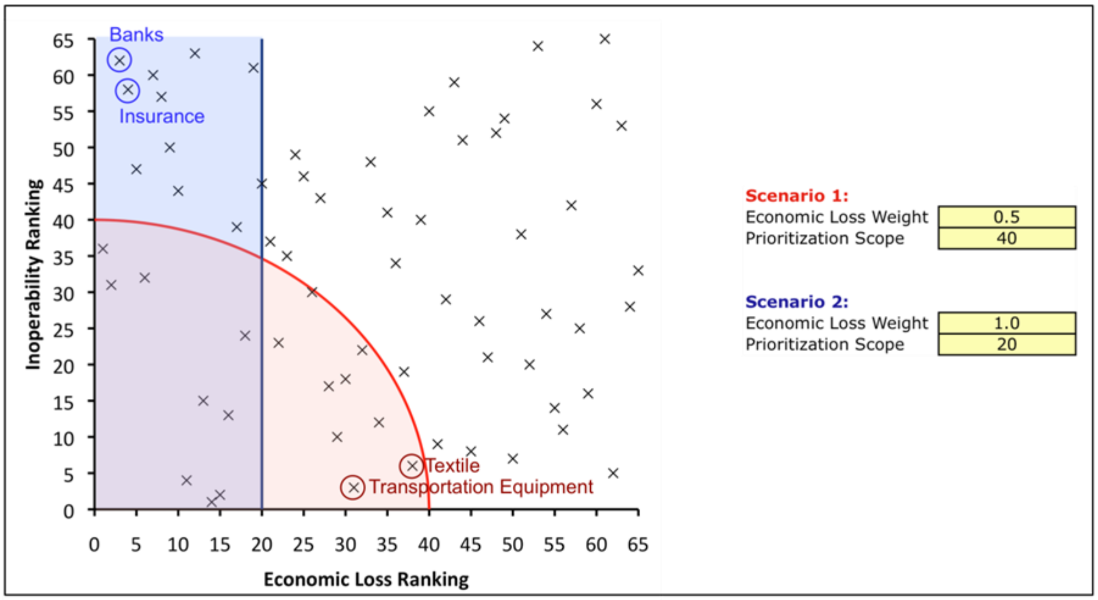


Figure 9.11 **DCPP for Case 1**

---

[19] Since regional I-O data typically lump electric power sector with the general "utility" sector, an approach to perform sector disaggregation is to pre-multiply the assumed "percent outage" with the ratio of electric power output relative to the total utility sector output.

combined disruption scenarios comprise Case 2, which is explored in this section. The scenario parameters that describe Case 2 are entered into the dynamic IIM and generated the economic loss and inoperability charts in *Figure 9.12*. The total economic loss for the simulated scenario is $816 million. From this economic loss, the following losses can be estimated based on the approaches discussed in *Section 9.3.5* (note that these losses are incurred only within the assumed recovery period of 30 days):

- Tax loss: $7,346,801
- Income loss: $108,831,472
- Equivalent number of jobs lost: 2,483

The top 10 sectors that suffer the highest economic losses (*Figure 9.12*, left panel) are: computer systems design and related services (S49); administrative and support services (S51); federal reserve banks and credit intermediation (S41); insurance carriers and related activities (S43); ambulatory health care services (S54); wholesale trade (S27); real estate (S45); retail trade (S28); hospitals and nursing and residential care facilities (S55); and state and local government (S65). The top 10 sectors account for 47% of the total economic loss.

In contrast, the top 10 sectors with highest inoperability values (*Figure 9.12*, right panel) are: utilities (S6); oil and gas extraction (S3); other services, except government (S61); pipeline transportation (S34); apparel and leather and allied products (S10); other transportation equipment (S24); mining, except oil and gas (S4); rail transportation (S30); textile mills and textile product mills (S9); and furniture and related products (S25). In the inoperability charts for Case 2, we can directly observe that the electric power disruption is modeled as a "utilities" sector disruption, which is flat for the first 10 days and completely restored thereafter.

The inoperability and economic loss rankings vary for the same reasons given earlier. The DCPP tool enables the user to perform sensitivity analysis with respect to how they structure their preference between the economic loss and inoperability objectives. The vertical region in *Figure 9.13* corresponds to a preference strategy that gives importance to economic loss only, while the quarter-circle region corresponds to assigning equal weights to inoperability and economic loss objectives. For a purely economic loss minimizing strategy, there is a risk to exclude sectors that have critical ranking with respect to inoperability (e.g., utilities, pipeline transportation). Nevertheless, there is also a risk

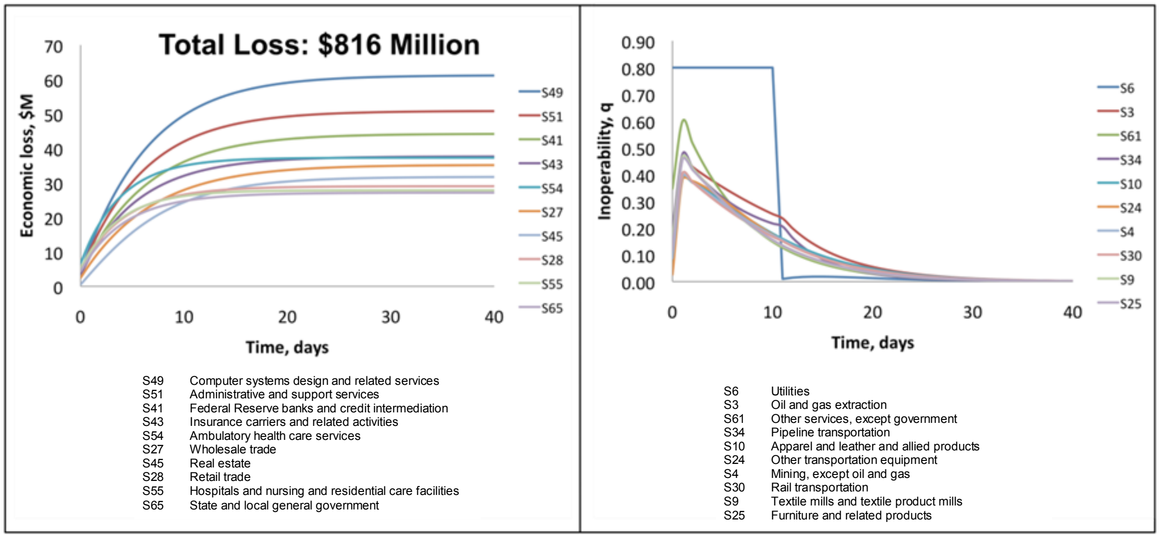


Figure 9.12 **Top 10 critical sectors for Case 2 ranked according to: Economic loss (left) and Inoperability (right)**

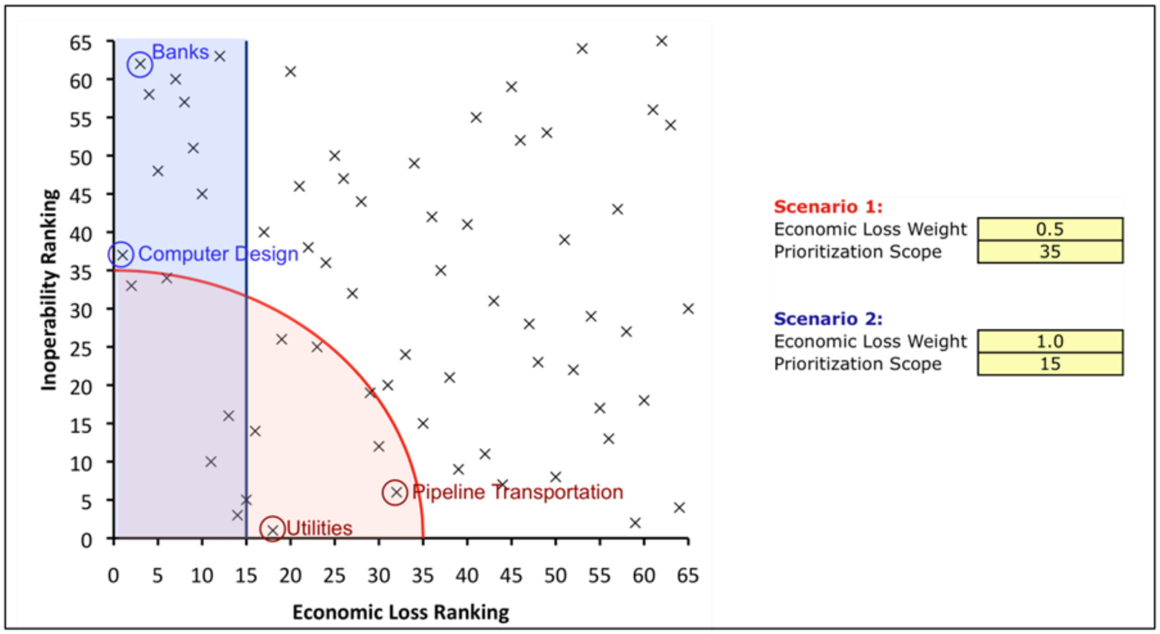


Figure 9.13 **DCPP for Case 2**

of excluding sectors with critical economic loss rankings (e.g., computer design, banking) when equal weights are allocated between economic loss and inoperability. Hence, prioritizing sectors for recovery need careful consideration of the balance between economic loss and inoperability.

9.4.3 Case 3 – Infrastructure Disruption with a "Step Function" Recovery

Suppose that Case 1 is expanded such that in addition to the 50% initial workforce inoperability, the electric power recovery is modeled as a step function with the following specifications:[20]

- 80% utility infrastructure disruption for Day 0 to Day 2
- 50% utility infrastructure disruption from Day 3 to Day 5
- 25% utility infrastructure disruption from Day 6 to Day 10

These combined disruption scenarios comprise Case 3, which is explored in this section. The scenario parameters that describe Case 3 are entered into the dynamic IIM and generated the economic loss and inoperability charts in *Figure 9.14*. The total economic loss for the simulated scenario is $809 million. From this economic loss, the following losses can be estimated based on the approaches discussed in *Section 9.3.5* (note these values encompass the losses incurred within the assumed recovery period of 30 days):

- Tax loss: $7,286,167
- Income loss: $108,475,569
- Equivalent number of jobs lost: 2,475

For Case 3, the top 10 sectors that suffer the highest economic losses (*Figure 9.14*, left panel) are: computer systems design and related services (S49); administrative and support services (S51); federal reserve banks and credit intermediation (S41); insurance carriers and related activities (S43); ambulatory health care services (S54); wholesale trade (S27); real estate (S45); retail trade (S28); hospitals and nursing and residential care facilities (S55); and state and local government (S65). The total economic loss for the simulated scenario is $809 million. The top 10 sectors account for 47% of this total economic loss, which is the same as Case 2.

---

[20] See explanatory notes in footnote 17.

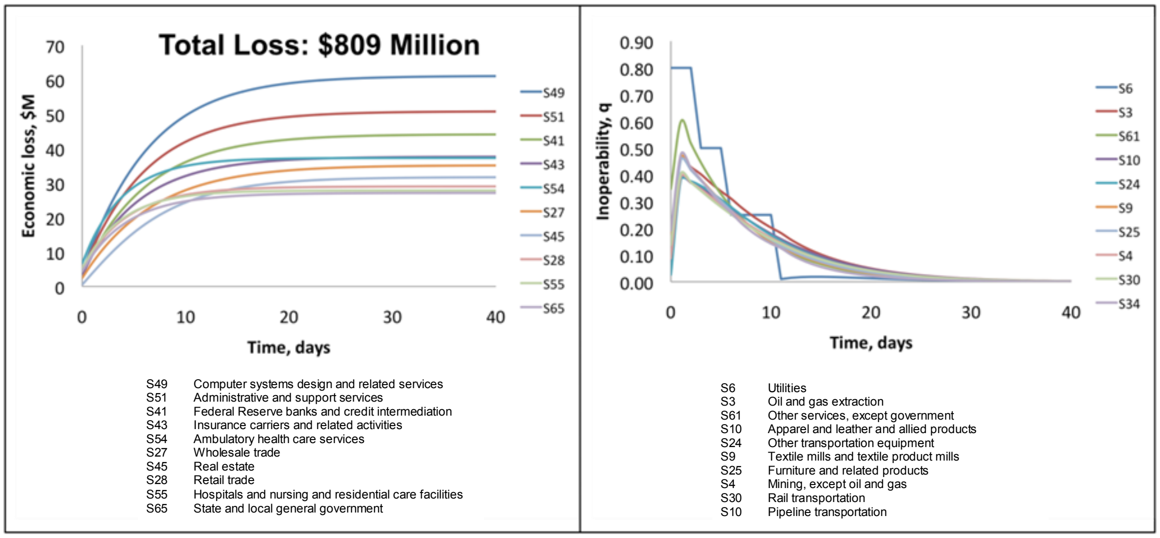


Figure 9.14 **Top 10 critical sectors for Case 3 ranked according to: Economic loss (left) and Inoperability right**

In contrast, the top 10 sectors with highest inoperability values (*Figure 9.14*, right panel) are: utilities (S6); oil and gas extraction (S3); other services, except government (S61); apparel and leather and allied products (S10); other transportation equipment (S24); textile mills and textile product mills (S9); furniture and related products (S25); mining, except oil and gas (S4); rail transportation (S30); and pipeline transportation (S34). In the inoperability charts for Case 3, we can directly observe that the electric power disruption is modeled as a "utilities" sector disruption, whose recovery is modeled similar to a step function. This type of flexible recovery adjustment is particularly useful for modeling risk management interventions to expedite recovery.

Just like in previous cases, the DCPP tool enables the user to perform sensitivity analysis with respect to how users or decision-makers would structure their preference between the economic loss and inoperability objectives. It should be noted that Case 3 is a slight variant of Case 2 (i.e., they only differ with respect to the shape of the recovery function for the "utilities" sector). Hence the DCPP chart is omitted for this case since the sector priorities are the same as the economic loss and inoperability rankings found in *Figure 9.13*.

9.4.4 IIM "Final" Scenario Results

Scenario Description

Table 9.1 shows the disruption scenarios previously estimated in Chapters Five and Six for the three infrastructure systems (power, wastewater, and water), expressed in terms of the daily losses (in thousand dollars).

Normalizing the daily loss of each infrastructure system with respect to the average daily revenue will result in the disruption scenarios in *Table 9.2*, in percent.

Table 9.1 **Average Daily Losses for Electric Power, Water and Wastewater**

Infrastructure	Ave. Daily Revenue ($K)	Daily Loss ($K): Days 0-10	Daily Loss ($K): Days 11-20	Daily Loss ($K): Days 21-30
Electric Power	2070	585	435	217
Wastewater	1251	579	579	159
Water	1724	346	346	125
Total	5045	1510	1360	501

Table 9.2 **Normalized Percentage Daily Loss for Three Infrastructures**

Infrastructure	Ave. Daily Revenue ($K)	Percent Loss: Days 0-10	Percent Loss: Days 11-20	Percent Loss: Days 21-30
Power	2070	585/2070 = 28%	435/2070 = 21%	217/2070 = 10%
Wastewater	1251	579/1251 = 46%	579/1251 = 46%	159/1251 = 13%
Water	1724	346/1724 = 20%	346/1724 = 20%	125/1724 = 7%
Total	5045	1510/5045= 30%	1360/5045= 27%	501/5045= 10%

In the current version of the IIM for Nashville, there is a "Utility" sector that encompasses the three infrastructure systems. With the above specifications for daily losses in each infrastructure system, the IIM model is capable of disaggregating the results in terms of economic loss and inoperability for each of the 3 infrastructure systems (power, wastewater, and water). The same codes for the economic sectors are used in the analysis (see Appendix for these sector codes). Utility sector is designated with an alphanumeric code of S6. With the decomposition process, Utility sector is now represented into three disaggregated sectors as follows:

- S6.1 Utilities - Power
- S6.2 Utilities - Water
- S6.3 Utilities - Wastewater

Results

The above scenario parameters are entered into the dynamic IIM and generated the economic loss and inoperability charts in *Figure 9.15*. The total regional economic loss for the simulated scenario is around $45 million. From this economic loss, the following losses can be estimated based on the approaches discussed in the IIM methodology chapter. Note that the following losses are incurred only within the assumed recovery period of 30 days (or approximately 1 month):

- Total regional economic loss: $44.8 Million
- Sales tax loss: $365,000
- Income loss: $2,238,000
- Equivalent number of jobs lost: 51

The top 10 sectors that suffer the highest economic losses (Figure 9.15, left panel) are: utilities – power (S6.1); utilities – water (S6.2); utilities – wastewater (S6.3); construction (S7);

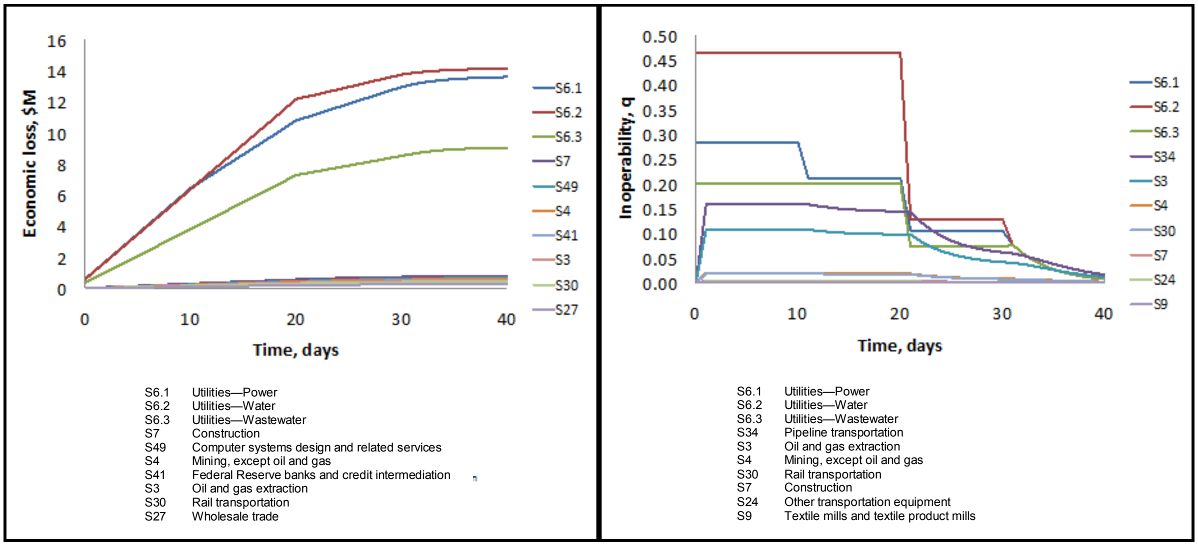


Figure 9.15 **Top-10 critical sectors for Case 2 ranked according to: Economic loss (left) and Inoperability (right)**

computer systems design and related services (S49); mining, except oil and gas (S4); federal reserve banks and credit intermediation (S41); oil and gas extraction (S3); rail transportation (S30); and wholesale trade (S27). All the losses for all 65 sectors are in Annex 9, at the end of this chapter.

In contrast, the top 10 sectors with highest inoperability values (*Figure 9.15*, right panel) are: utilities – power (S6.1); utilities – water (S6.2); utilities – wastewater (S6.3); pipeline transportation (S34); oil and gas extraction (S3); mining, except oil and gas (S4); rail transportation (S30); construction (S7); other transportation equipment (S24); and textile mills and textile product mills (S9).

9.5 Calculating the Key Indicators

These results are used directly in calculating several key indictors for the decision process. At the level of the total region, resilience is defined to be the same as the total regional economic risk, while the total regional risk is defined as the inclusive risk, i.e., the risk including the allowance for human casualties. The threat likelihood and vulnerability for these calculations are the same as estimated for the threat-asset pairs in Phase 2 (Chapter Four). Thus, for each threat-asset pair:

$$\begin{gathered}\textit{Total Regional Risk}_{ta} = \\ [\textit{Total Economic Loss}_{ta} + \\ (\$7.0\ \textit{mill.} \times \textit{Fatalities}_{ta}) + \\ (\$1.7\ \textit{moll.} \times \textit{Injuries})_{ta}] \times V_{ta} \times T_{ta}\end{gathered}$$

Eq. 9.8

$$\begin{gathered}\textit{Total Regional Resilience}_{ta} = \\ \textit{Total Economic Loss}_{ta} \times V_{ta} \times T_{ta}\end{gathered}$$

Eq. 9.9

$$\begin{gathered}\textit{Expected Job Loss}_{ta} = \\ \textit{Total Job Loss}_{ta} \times V_{ta} \times T_{ta}\end{gathered}$$

Eq. 9.10

$$\begin{gathered}\textit{Expected Lost Wages}_{ta} = \\ \textit{Total Lost Wages}_{ta} \times V_{ta} \times T_{ta}\end{gathered}$$

Eq. 9.11

$$\begin{gathered}\textit{Expected Sales Tax Loss}_{ta} = \\ \textit{Total Sales Tax Loss}_{ta} \times V_{ta} \times T_{ta}\end{gathered}$$

Eq. 9.12

Where:

Total Economic Loss$_{ta}$, Total Job Loss$_{ta}$, Total Lost Wages$_{ta}$, and Total Sales Tax Loss$_{ta}$ are as estimated in IIM for the threat-asset pair. The V_{ta} and T_{ta} are as estimated for the threat-asset pair in Phase 2 (Chapter Four).

Because these are expected values, they can be aggregated for all threat-asset pairs or any useful subset (e.g., all risks originating from a particular infrastructure, all natural hazard risk or all adversary risk) by simple addition.

In the RR/SAP assessment cycle, these help direct attention to the risk and resilience areas that pose the greatest challenges. In the evaluation cycle, they help select the options with the greatest benefits.

9.6 Conclusions and areas for future model improvements

Economic disruptions in the aftermath of a disasters can cascade across interdependent economic sectors, further delaying recovery. This chapter develops a recovery model to estimate sector inoperability and economic losses for a disaster scenario in the example region. Two primary IIM metrics for determining critical sectors are presented in this chapter – namely inoperability and economic loss. Inoperability measures the percentage reduction relative to the total output of the sector. Economic loss, on the other hand, corresponds to the decrease in the value of economic output due to the productivity disruptions. From the economic loss values computed by the IIM, other loss categories could be derived such as tax loss, income loss, and equivalent number of jobs lost. Sensitivity analysis of inoperability and loss reduction objectives can provide insights on identification and prioritization of critical sectors. Based on the simulated scenarios, the 10 most critically affected sectors (out of 65) suffer about half of the projected losses. This observation will be particularly useful in informing the regional decision-makers just who will bear the greatest losses.

To show the key features of the IIM tool, three cases are explored. These scenarios involve combinations of disruptions to workforce sectors and to the utility infrastructure sector. Since regional I-O data typically bundle electric power within the general utility sector, further analysis is needed to perform sector disaggregation to analyze direct impacts on the electric power sector. For example, it is possible to take the ratio of electric power output with respect to the total utility sector output. At the national level, utility sector is comprised of three subsectors, namely (1) electric power, (2) natural gas, and (3) water and sewerage systems. Such ratio can range from 60-70% based on national data archived by the BEA.[21] Hence, electric power is a significant component of the utility sector. A given value of electric power (percent) outage can be entered to the IIM as a utility sector disruption by applying such ratios.

Finally, the simulated scenarios for the example region showed that the majority of the top 10 sectors based on the economic loss metric are service-oriented. In contrast, the majority of the top 10 sectors based on the inoperability metric are manufacturing-related. Hence, a careful balance must be sought in prioritizing key sectors as different performance measures may indicate a different set of rankings. Given decision-maker preferences, there exists an opportunity to use the Analytic Hierarchy Process and other elicitation methods to guide in the prioritization of the key sectors. Although applied specifically to the example metro area, the same methodology can be implemented in other regions. The methodology and decision analysis tool developed in this chapter can be integrated with other critical infrastructure models.

---

[21] For examples, GDP and production output data that provide breakdowns of utility sector components are found in http://www.bea.gov/industry/gdpbyind_data.htm.

Annex 9

Itemized Economic Losses for the 65 Sectors of Nashville Region

Code	Description	Loss ($M)
S1	Farms	0.0018
S2	Forestry, fishing, and related activities	0.0129
S3	Oil and gas extraction	0.5367
S4	Mining, except oil and gas	0.6062
S5	Support activities for mining	0.0033
S6.1	Utilities – Power	13.64698
S6.2	Utilities – Wastewater	14.16832
S6.3	Utilities – Water	9.09162
S7	Construction	0.8063
S8	Wood products	0.0654
S9	Nonmetallic mineral products	0.0901
S10	Primary metals	0.1917
S11	Fabricated metal products	0.226
S12	Machinery	0.1469
S13	Computer and electronic products	0.0164
S14	Electrical equipment, appliances, and components	0.0767
S15	Motor vehicles, bodies and trailers, and parts	0.0545
S16	Other transportation equipment	0.0093
S17	Furniture and related products	0.0135
S18	Miscellaneous manufacturing	0.0128
S19	Food and beverage and tobacco products	0.0411
S20	Textile mills and textile product mills	0.0098
S21	Apparel and leather and allied products	0.0021
S22	Paper products	0.052
S23	Printing and related support activities	0.0347
S24	Petroleum and coal products	0.1977
S25	Chemical products	0.1585
S26	Plastics and rubber products	0.0919
S27	Wholesale trade	0.2925
S28	Retail trade	0.0616
S29	Air transportation	0.0211
S30	Rail transportation	0.4378
S31	Water transportation	0.0052
S32	Truck transportation	0.1439

Code	Description	Loss ($M)
S33	Transit and ground passenger transportation	0.0069
S34	Pipeline transportation	0.2919
S35	Other transportation and support activities	0.0938
S36	Warehousing and storage	0.0127
S37	Publishing industries (includes software)	0.0386
S38	Motion picture and sound recording industries	0.0103
S39	Broadcasting and telecommunications	0.0928
S40	Information and data processing services	0.0352
S41	Federal Reserve banks, credit intermediation, and related activities	0.5587
S42	Securities, commodity contracts, and investments	0.045
S43	Insurance carriers and related activities	0.1007
S44	Funds, trusts, and other financial vehicles	0.0014
S45	Real estate	0.2117
S46	Rental and leasing services and lessors of intangible assets	0.1336
S47	Legal services	0.1661
S48	Computer systems design and related services	0.0411
S49	Miscellaneous professional, scientific, and technical services	0.6879
S50	Management of companies and enterprises	0.0732
S51	Administrative and support services	0.2848
S52	Waste management and remediation services	0.0307
S53	Educational services	0.0043
S54	Ambulatory health care services	0.0004
S55	Hospitals and nursing and residential care facilities	0.0001
S56	Social assistance	0
S57	Performing arts, spectator sports, museums, and related activities	0.023
S58	Amusements, gambling, and recreation industries	0.0027
S59	Accommodation	0.0475
S60	Food services and drinking places	0.2146
S61	Other services, except government	0.1155
S62	Federal general government	0.0394
S63	Federal government enterprises	0.0176
S64	State and local general government	0.0121
S65	State and local government enterprises	0.0395

CHAPTER 10

RR/SAP Phase 6 – Decision-Makers' Choices & Plans And The RR/SAP Evaluation Cycle

10.1 Purposes of Phase 6 and the Evaluation Cycle: Decision-Making

Phase 6 of the Regional Resilience/Security Analysis Process (RR/SAP) is the decision-making phase. At the end of the RR/SAP Assessment Cycle, Phase 6 (*Figure 10.1*) reviews the results of the first five phases to determine which specific risks and resilience situations, at the level of threat-asset or threat-facility pairs, system or interdependency, warrant further work to examine what can be done to enhance security and resilience. This decision initiates the second RR/SAP cycle, the Mitigation Option Evaluation Cycle (or "evaluation cycle" for brevity), which:

- Refines the criteria of multi-attribute objective of value, if needed and sets priorities among the identified risk and resilience areas (Phase 1 of the Evaluation Cycle);
- Defines specific options to reduce risk and/or increase resilience and estimates their costs;
- Estimates how and how much the options would change one or more elements of risk or resilience – reduce consequences, likelihood of occurrence, vulnerability, service outage duration and severity – and the amount by which security and resilience are enhanced by revisiting Phases 2-5 and noting the differences;
- Evaluates the value (relative score on the multi-attribute objective), value/dollar, benefits to the owner, the owner's benefit/cost ratio, the benefit to the regional public, and then the public's benefit/cost ratio and displays them for the decision-makers;
- Decides which *set* or portfolio of options will be selected for implementation by the owners, which set by authorities representing the regional public, which require collaboration and which will be deferred (Phase 6); and
- Implements and oversees the operations of the selected options and manages their effectiveness.

The similarity of this chapter to the seventh step of RAMCAP, Risk/Resilience Management as sketched in Chapter Four, is not accidental. The work of this phase would be the same as Step 7 if

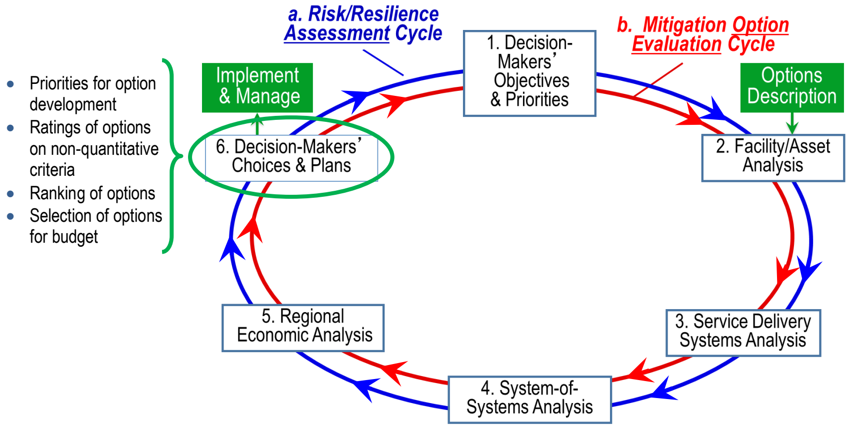


Figure 10.1 **RR/SAP Phase 6: Decision-Makers' Choices & Plans**

only one organization were conducting the analysis and with it limited to the static facilities and assets, without consideration of the system's operations or system-of-systems dependencies.

This chapter describes Phase 6 and the full Evaluation Cycle, culminating in the decisions that determine the new additions to the portfolios of the participating organizations.

10.2 Overview

RR/SAP Phase 6 of the Evaluation Cycle is *the decision-making that actually reduces risk and enhances resilience.* Risk and resilience management is the deliberate course of deciding upon and implementing *options* (e.g., establishing or improving security countermeasures, improving consequence mitigation tactics, building in resilience and redundancy by design, entering into mutual aid pacts, creating emergency response and business continuity plans, training and conducting exercises in business continuity) to achieve an acceptable level of risk and resilience at an acceptable cost to the organization and the regional public. The initial risk and resilience analysis of the RR/SAP Assessment Cycle is based on the existing conditions at the time of the analysis. The value added relative to the multi-attribute objective, the reduction in risk and the increase in resilience are the benefits of the option, which can be compared to the cost of implementing it and to the benefits of other options.

The first five phases of the RR/SAP Assessment Cycle developed information that is collated in the sixth phase to estimate the level of risk and resilience that each critical facility, system and system-of-systems exhibits *with its current level of security and resilience measures* – a baseline for comparison with improvement options. Phase 6 of the Assessment Phase determines which areas of risk and resilience are significant enough, either to the owner or the regional public, to justify additional time and effort to develop and evaluate improvement options. The Evaluation Cycle accomplishes the work to do this by prioritizing the areas of concern and re-analyzing the same set of threat-asset pairs under the assumption that a specific option has been implemented. Unless there are mandated legal or regulatory actions to consider, the option of taking no action – the baseline option – should always be included considered. *Improvements over this baseline define the benefits of the options.* Alternatives to doing nothing are broadly classified as either *countermeasures* or *consequence-mitigation options*. Countermeasures, also called "protective measures," can be viewed as reducing threat likelihood and/or vulnerability, while consequence-mitigation actions are intended to reduce consequences.

A special, but extremely important, case of consequence mitigation is *resilience enhancement:* the ability to withstand a disruptive incident and reduction of service downtime between an incident and acceptable restoration of service if it cannot be withstood. Especially in the "lifeline" infrastructures upon which the very viability of a community depends, resilience enhancements can minimize the loss of region-wide economic activity and major public health and safety consequences. Consequence-mitigation can also have an effect on threat likelihood by reducing the attractiveness of the asset target.

Once these analyses are complete, Phase 6 of the Evaluation Cycle is fundamentally concerned with optimizing resource allocation – selection of investment options in support of increasing security and resilience to natural hazards, terrorist threats and dependency/proximity hazards – and implementing those decisions in the most effective way given the limitations on resources. This is not a simple ranking problem because:

- The several systems have their respective owners, each with their own resource limits and priorities;
- Governments and civil society organizations have their distinctive responsibilities to represent the regional

public, so have different interests, priorities and resource constraints; and

- Public-private partnerships are often formed to deal with issues affecting both public and private interests, so will have their own priorities and constraints.

Further, these decisions have multiple dimensions of value and cost, which is the reason the RR/SAP began with the articulation and prioritizing of the multi-attribute objective. The purpose of Assessment Cycle Phase 6 is to review the results of the preceding phases and to provide a defined scope for the Evaluation Cycle.

The Evaluation Cycle, in turn, then proceeds through nine tasks that collectively constitute the cycle, culminating in the decisions that select the portfolio additions for each of the respective organizations and implementing and managing the chosen options. In overview, these tasks are:

Task 10.1 Decide what risk/resilience issues to analyze further. Determine the security and resilience areas, such as threat-asset pairs, facilities, subsystems, and dependencies, , that warrant further consideration based on the Assessment Cycle results (Assessment Cycle Phase 6).

Task 10.2 Set or refine priorities for the Evaluation Cycle. Rank the threat risk and resilience areas of continuing concern so that analytical resources can be judiciously applied (Evaluation Cycle Phase 1).

Task 10.3 Define options. Prepare conceptual designs for countermeasures and mitigation/ resilience options and estimate their investment and operating costs.

Task 10.4 Evaluate each option. Evaluate the options by analyzing the system, facility or asset under the assumption that the option has been implemented – revisiting RR/SAP Phases Steps 2 through 5 to re-estimate the risk and resilience levels to the owner and to the public, and determine the estimated benefits of the option (Evaluation Cycle Phases 2-5).

Task 10.5 Adjust and accumulate the benefits of each option. Adjust the benefits from each threat-asset pair for which the option reduces risk or enhances resilience. Many options reduce risk for more than the particular threat-asset pair for which it was initially designed. Conversely, some options combinations may be alternatives to other options, so their respective benefits could be double counted. Both types of adjustments must be made for a true allocation of benefits (Evaluation Cycle Phase 6, as are all the remaining tasks).

Task 10.6 Estimate net benefits and marginal value of each option. Estimate the (a) multi-attribute value score and value score per dollar; (b) the owner's net benefit and benefit/cost ratio (and/or other criteria relevant in the organization's resource decision-making, e.g., return on investment); and (c) the net benefit and benefit/cost ratio to the regional public.

Task 10.7 Choose and allocate resources to options. Select among the options considering all criteria from the perspectives of the owners of each system and of the regional public based on the full set of criteria and constraints – the risks of fatalities and serious injuries, financial losses to the owner, economic losses to the community, resilience levels, and qualitative factors under the constraints of available resources and prior commitments, etc. – and allocate sufficient resources to these options to initiate the appropriate next step.

Task 10.8 Manage the options. Implement, manage, monitor and evaluate the performance of the selected options, doing whatever "mid-course corrections" are necessary for each to achieve its specific objective.

Task 10.9 Repeat the Regional Resilience/ Security Analysis Process. Conduct additional risk assessments to monitor progress, adapt to changing conditions and support continuous improvement, usually through a periodic repetition of the RR/SAP, supplemented by special analysis on an as-needed basis.

Each of these tasks is discussed in more depth in the next section.

10.3 Tasks in Moving from Analysis to Enhanced Resilience and Security

10.3.1 (Task 10.1) Decide what risk/resilience issues to analyze further

The first set of decisions is to determine which issues to analyze further based on the results to date. Ideally, this would start with deciding what risk and resilience levels are acceptable to the decision-makers by examining the estimated results of the first five phases for each threat-asset pair, facility, system, or dependency. In many organizations and forums, stating acceptance criteria may prove problematic for public relations and legal liability reasons. For this reason, the issues for further attention are designated and the others deferred until time and resources are available.

In general, the designated issues are those threat-asset pairs, facilities, systems or dependencies that pose the greatest risk and/or expected outage – the resilience indicator. For those that are deferred, document the decision. For those that are designated for further analysis, proceed to the next steps. Not all risks and resilience levels justify actions. This step allows the decision-makers to decide whether they can accept deferring the existing risk and resilience and where they want to consider improvements. Designating an issue does not imply that something will – or even can be done about it – just that it will be included in the next step of the analysis.

To reach these decisions, it is useful for the analysts to display a summary of the situation such as shown in *Table 10.1*. This displays only the system totals from the perspectives of the system owners and the regional public and includes only the most significant indicators. Decision-makers evaluate which systems exhibit

Table 10.1 **Summary of Risk and Resilience at Current Conditions: Region and Major Systems**

Metric	Owner's Perspective	Regional Public's Perspective
1. Total Region		
a. Expected Fatalities		
b. Total Expected Casualties		
c. Financial/Economic Risk		
d. Inclusive Risk (includes casualties at VSL)		
e. Resilience Index		
2. Wastewater System Total		
a. Expected Fatalities		
b. Total Expected Casualties		
c. Financial/Economic Risk		
d. Inclusive Risk (includes casualties at VSL)		
e. Resilience Index		
3. Water System Total		
a.		
b.		
4. Electric Power System Total		
Etc.		

values on these indicators that are not acceptable on their face.

Once the systems of concern are selected, a series of "drill-downs", such as in *Table 10.2*, allow the decision-makers to identify the specific risk and resilience areas and issues of greatest concern. The information allows them to trace the risk and resilience issues from the high-level total system to lower levels – facility totals, asset totals and threat-asset pairs. As they drill down, they indicate which subsystems, facilities assets or threat-asset pairs they designate for additional analysis. In some particularly large analyses, decision-makers may elect to set thresholds for each of the key indicators and let the analysts sort them out for further attention.

Deciding which risk/resilience areas to analyze further can be difficult for owners and top executives. Making these critical decisions explicit will direct the entire Evaluation Cycle. Threat-asset pairs can usefully be divided into four groups:

1. *Acceptable business risks* – Some specific risks and resilience levels are obviously acceptable to the organization. In a sense, the organization self-insures that it can bear the consequences of the event without breaching trust with the public or the stakeholders of the organization.
2. *Unacceptable, but insurable risks* – Some risks are sufficiently predictable to allow insurance companies to write policies that make the owner of the asset partially or fully whole if the incident occurs. Storm and flood insurance are of this sort. Note that this insurance protects owners from economic losses, but *does not protect the community that depends on the asset or system's functioning.*

Table 10.2 **Typical "Drill-Down" Table for A Specific System**

Metric	Owner's Perspective	Regional Public's Perspective
1. Wastewater System Total		
a. Expected Fatalities		
b. Total Expected Casualties		
c. Financial/Economic Risk		
d. Inclusive Risk (includes casualties at VSL)		
e. Resilience Index		
1.1 Control Center		
a. Expected Fatalities		
b. Total Expected Casualties		
c. Financial/Economic Risk		
d. Inclusive Risk (includes casualties at VSL)		
e. Resilience Index		
1.1.1 Threat-Asset Pair (1.1.1)		
a.		
b.		
1.1.2 Threat-Asset Pair (1.1.2)		
1.2 Treatment Plant		
. 1.2.1 Chlorine Storage		
1.1.2.1 Threat-Chlorine Pair		
Etc.		

3. *Survival and mission-critical risks* – Other risks have consequences that are so threatening to the organization's survival and most critical mission(s) that management is simply compelled to examine them further for means of enhancing security and resilience.
4. *Potentially manageable risks* – In between these last two groups are those for which senior decision-makers would like to examine the benefits and costs, with an eye to selecting security or resilience options if they are not too costly.

The risk/resilience areas in groups 3 and 4 are subjected to the RR/SAP Evaluation Cycle, which begins in the next task. With both the owners and those representing the regional public, it is useful to include the estimates from both the owners' and the public's perspectives. This allows both parties to identify the stakes each faces in examining these risk/resilience areas.

10.3.2 (Task 10.2) Set or refine priorities for the Evaluation Cycle

Once the initial sorting of these categories is accomplished, it behooves management to review the implicit criteria to make these distinctions and the boundaries of the resulting three groups. Explicit examination of the implicit criteria allows management to challenge, discuss, refine and communicate them, at least internally. This task can identify inconsistencies and clarify the priorities of the organization regarding risk and resilience. These discussions may lead to refinements of the initial set of objectives, priorities, and metrics, based on an update of the Analytic Hierarchy Process (AHP) completed in Phase 1 of the Assessment Cycle (discussed in Chapter Three).

In light of these considerations, rank the risk and resilience areas and issues of continuing concern so that analytical resources can be judiciously applied (Evaluation Cycle Phase 1).

10.3.3 (Task 10.3) Define Countermeasures and Mitigation/Resilience Options

This task defines countermeasure and mitigation options for those risk/resilience areas that fall into the third and fourth groups from Task 10.2. Developing these alternative options addresses specific threat-asset pairs of threat-facility pairs. Analysts should consider the principles of devalue, deter, detect, delay, and response to reduce consequences and enhance resilience, e.g., redundant or contingent capabilities, continuity of operations plans, "hardening" facilities, accelerated recovery. Examination of the earlier estimates of consequence, vulnerability, and resilience for ways to improve them is a useful way to develop options. The following questions illustrate this concept:

- How can consequences be reduced?
- How can an adversary be deterred from selecting this asset or facility?
- How can the asset be made less vulnerable?
- How can the service outage be made less severe or shorter?

Countermeasures and consequence-mitigation actions are developed for each threat-asset pair, threat-facility pair or threat-system pair. Later, options addressing multiple threat-asset pairs, etc., are considered. For efficiency, it is preferable to address the highest-risk pairs first. Often, options designed for these high-risk pairs will also reduce risks for lower risk pairs as well. Alternative actions or strategies should be developed in a way that directly compares their projected effectiveness at reducing risks and enhancing resilience.

During the foregoing risk analysis for a particular threat or hazard to a specific asset, facility, site or system, estimates of current vulnerabilities were made, *given* the effectiveness and reliability of the existing countermeasures and mitigation plans against each threat or hazard. For the third and fourth categories of threat-asset pairs, enhanced countermeasures should be considered that improve the existing security systems.

Countermeasures. Examples of protective measures or countermeasures include the following:

- Physical security, including extension of security perimeter beyond the limits of facility to create a buffer zone;
- Roving security inspections;
- Sensors or closed-circuit television at key points;
- Access control;
- Background checks for employees, temporary workers, contractors, subcontractors, security force and potential first responders;
- Loss prevention, material control and inventory management;
- Delivery service verification, e.g., request delivery worker identity card;
- Control-room security;
- Policies and procedures;
- Cyber security;
- Training on security plans;
- Drills involving employees, contractors, public and media;
- Crisis management and emergency response, including incident command system; and
- Communication of hazards by asset owners to public sector protection forces.

Security enhancements at a facility can include one or more of the following strategies:

- "Devalue, deter, detect and delay" principles;
- Physical or cyber "layers of protection" and "rings of protection;"
- Procedures and administrative controls; and
- Inherently safer systems from the environmental perspective.

One of the classic approaches for countermeasures is to *devalue, deter, detect* and *delay* the adversary. This approach is often used in the protection of a fixed facility and involves accepted methodologies of conventional security in the form of physical restraints, uniformed guards, warning systems, detection and identification systems and delaying tactics. More specifically, they are defined as follows:

- **Devalue** is a countermeasure intended to make the asset less attractive to the adversary as a target for attack. Many devaluation countermeasures are designed to increase the terrorists' estimation of the costs of attacking, reduce their estimates of the chances of success or achieving the public relations value of the attack. Examples would be the more conspicuous forms of hardening, demonstration of determination to resume functioning, and forms of deterrence.

- **Deterrence** is a countermeasure strategy intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Examples of deterrence countermeasures include physical security systems, such as warning signs, lights, uniformed/armed guards, dogs, cameras and bars across windows or other access points.

- **Detection** is a countermeasure strategy intended to identify an adversary attempting to commit a security breach or other criminal activity. Detection may involve real-time observation, e.g., using video-surveillance equipment, motion detectors, or security personnel, as well as post-incident analysis of the activities to determine the identity of the adversary.

- **Delay** is a countermeasure strategy intended to provide various barriers to slow the progress of an adversary from entering or exiting a site. An example is the positioning of "jersey" barriers to preclude direct line-of-sight vehicle access to an asset.

Consequence-mitigation and resilience enhancement. Selection of consequence-mitigation strategies, like countermeasures, is highly dependent upon the asset or target and the threats to which they are exposed. Countermeasures can be seen as one form of mitigation measure: if the threat is thwarted, there are few or no consequences. In general, the term "mitigation" refers to reducing consequences of an event, given that it occurs.

A special form of consequence-mitigation is resilience enhancement. While consequence-mitigation refers to reducing any or all negative consequences, resilience options are specifically designed to reduce the duration or severity of denial of service to the community served by the infrastructure. For example, a mutual aid plan between neighboring water utilities would provide for one utility to share its peak capacity to assist another whose base load capacity is damaged. This would result in consequence-mitigation or resilience to the community. In practice, the distinction between consequence-mitigation and resilience enhancement options is merely semantic. The RAMCAP approach considers them together.

Elements of a consequence-mitigation strategy may include the following:

- Well-developed and well-exercised continuity of operations and continuity of government plans;
- Remote back-up of vital data;
- Automatic equipment responses, such as actuation of fire-suppression equipment or actuation of an emergency source of electrical power;
- Physical mitigation systems, which limit the effects of an attack (e.g., structural elements designed to withstand temperature and pressure effects of specified loads);
- State and federal resources for evacuation management or cleanup of toxic material;
- Early detection so that first responders can be mobilized and mitigation programs activated;
- On-site first responders (e.g., employees who can shut down situations that are out of control, provide immediate first aid to casualties and activate continuity of operations or continuity of government plans) taking immediate action to minimize the consequences;
- Emergency responders (local police, fire and emergency medical) trained in the appropriate initial steps to control or shut down out-of-control situations (when possible) and treatment of casualties for injuries that might occur at the facility, especially if they involve unusual materials, e.g., heavier-than-air toxic gases, burning chemicals;
- Pre-positioning spare parts, tools and transportation for rapid dispatch to damaged areas of the distributed facilities or network;
- Preparation of the public to respond appropriately in the aftermath of an attack by developing and exercising evacuation plans for neighboring residences and businesses, encouraging private stockpiling of water, food, medical supplies, etc., for at least 72 hours (e.g., www.ready.gov);
- Developing and exercising mutual aid agreements among neighboring utilities and competitors to restore service as rapidly as possible;
- Investing in back-up capabilities to meet service denial during crises, such as emergency generators (with ample fuel supplies), water storage tanks or towers, and enlarged inventories of critical raw and semi-finished materials to continue operations; and
- Developing significant levels of flexibility in networked systems, so damaged areas can be quickly isolated and bypassed to maintain service in as much of the system as possible while the damaged portion is being repaired.

For each countermeasure and mitigation/ resilience option, the effect on each element of risk and resilience is defined carefully. To reduce risk or enhance resilience, it is necessary to improve one or more of threat likelihood, vulnerability, consequences, or time to resume functioning. These are the key variables for the next step.

Consequence-mitigation and resilience enhancement options can often be more robust than countermeasures because many countermeasures address only one of a small number of threats, whereas mitigation and resilience options address numerous and highly diverse threats. This difference in robustness frequently translates into greater cost-effectiveness. This is a major motivation for the continuity and resilience movements that have become more and more prominent in many industries and communities.

In addition, for each option it is necessary to estimate the investment and operating costs. The costs should all follow the principle of forward costing only, i.e., no previous outlays ("sunk" costs) are to be included. The only exception to this is where the user is a taxable organization and unused depreciation can affect forward tax liabilities.

Estimate the effective life of each option and its investment and operating costs, being sure to include regular maintenance and periodic overhaul if expected. Adjust future costs to discounted present value.

Figure 10.2 shows how Decision Lens accumulates the estimates of option costs. It also recognizes the distinction among budgeting "pools," in our case, between operating and capital budgets, but potentially among others. The total money available for each pool is also determined and entered into the analysis at this point in the process.

10.3.4 (Task 10.4) Evaluate Each Countermeasure and Mitigation/ Resilience Option

This task assesses the options by analyzing the facility or asset under the assumption that the option has been implemented. This entails defining specifically how the options change the consequences, vulnerability, threat likelihood, outage severity or duration. Then, the threat-asset pair is re-evaluated with the option in place in RR/SAP Phases 2, 3, 4, and 5 to estimate the *new* risk and resilience levels. These are subtracted from the original risk and resilience estimates to calculate the benefits of the option, i.e., the difference between the risk and resilience levels without the option and those with the option in place.

Figure 10.2 **Accumulation of Option Cost Estimates, Funds Available and Budget Pool Eligibility**

Define Constraints

Resource: Investment

Scenario: Default

Period: Base Year

Total Budget: 43.870

☐ Only Fully Fund

Pool Name	Budget
Operating Budget (in millions)	9.87
Captial Budget (in millions)	34.00

Alternative Name	Value	Request	Funding Pool		Minimum
Option A	0.3	2.800	Captial Budget (in milli	S	0.400
Option B	0.374	1.100	Operating Budget (in m	S	1.100
Option C	0.411	12.000	Captial Budget (in milli	S	4.000
Option D	0.362	1.700	Operating Budget (in m	F	0.700
Combo Options A & C	0.394	12.400	Captial Budget (in milli	S	4.000
Combo Options B and D	0.337	1.900	Captial Budget (in milli	H	0.500
Option E	0.335	2.100	Operating Budget (in m	S	0.700
Options F1	0.33	1.200	Operating Budget (in m	S	0.700
Option F2	0.394	0.900	Operating Budget (in m	H	0.300
Totals		97.700			34.000

Courtesy of Decision Lens Inc.

The baseline for comparison is the "existing conditions" option. The benefits are the expected value of the avoided losses for risk reduction and the reduction of the expected value of the duration-severity product for resilience improvement. Each option is also rated on the multi-attribute objectives that call for ordinal judgments.

Evaluating the options for reducing risk and enhancing resilience requires metrics generally accepted as indicating value added and costs incurred. The reduction of expected loss (risk reduction, security enhancement) and/or expected outage (resilience enhancement, reducing the resilience indicator) are both benefits that add value to the organization or public. The "value score" on the multi-attribute objective is a broader indicator that includes risk reduction and resilience enhancement.

Net benefits (benefits minus costs, the gain in well-being) and benefit/cost ratios (a measure of efficiency, the marginal gain per dollar of cost) are widely used in public and non-profit organizations to evaluate options promising positive results for the organization and/or its stakeholders. Public executives are advised to invest in options with the greatest net benefits and/or the highest benefit/cost ratios. Three major benefits are most important in valuing options – the overall value score, inclusive risk reduction and resilience improvement to the owner and to the regional public, respectively.

The principle is to capture the greatest value possible given constrained budgets. The benefits are those incurred by the organization or public served and, in theory, are estimated on the basis of their "willingness to pay" for these outcomes. In principle, fatalities and injuries are "monetized" by setting dollar values (the value of a statistical life" discussed in Chapter Four) on each and including them with the economic benefits, called here the "inclusive risk." At higher levels of government, costs are estimated as "opportunity costs," or the value of other benefits, public and private, forgone by using resources for the present option. Willingness to pay and opportunity costs are very difficult to estimate, so this section evaluates public benefits as avoided fatalities, serious injuries, community economic losses and budgetary cash outlays to implement the option. This definition of costs is used almost universally by private businesses, non-profit utilities, and local and state governments.

For-profit businesses and many non-profit utilities use seemingly different metrics to evaluate the merits of investment and expenditure options. They may use the same estimates of fatalities and injuries as the public sector analysis. They may also use the direct cash liabilities for fatalities and injuries, after insurance adjustments. They use the financial losses to the owner as the primary economic metric. These include such metrics as maximizing net earnings (akin to net benefits) and/or return on investment or internal rate of return (both akin to benefit/cost ratios.) The private benefits are revenues and avoided losses and the private costs are the cash outlays of the organization to acquire those benefits.

While the respective conventions use different definitions of who pays and who benefits and the metrics seem to be very different, they share fundamental principles (e.g., net present expected value of both benefits and costs, after taxes and side-payments, if any). Except for the "who-benefits/who-pays" issue, it is little more than a simple algebra exercise to convert one to another. For taxable organizations, the calculations should be done on an after-tax cash flow basis. This section uses the language and methods of benefit-cost analysis, because it is a bit more intuitive than business accounting terms.

Evaluating countermeasures and mitigation/ resilience options requires re-estimating the terms in the risk and resilience equations changed by the option and re-calculating the level of risk and resilience.

- Risk-reduction benefits of the option are the amount that risk (= C * V * T) is reduced – by reducing any or all of likelihood of the hazard's occurrence, the asset's vulnerability or the consequences of the hazard – and is measured by the difference in the risk with and without the option.

- Resilience benefits are the amount that the duration and/or severity of service denial is reduced and can be valued by the economic losses to the community that are weighted by the possibly revised likelihood of the hazard and vulnerability. They are measured by the difference in weighted community losses with and without the option.[22]

Making these estimates entails serious consideration of which of the elements of risk and resilience is changed by the option and returning to one or more of Steps 1 through 6 of RAMCAP in RR/SAP Phase 2 and then extending that analysis through Phases 3 through 5 to estimate the systems and regional system-of-systems benefits of accepting the option.

In addition to estimating the risk and resilience results for each option, they also must be rated for the multi-attribute value score on the metrics that are not generated as part of the risk analysis per se. *Figure 10.3* shows how the AHP (as implemented by Decision Lens) supports estimation of the extent to which options advance objectives for which ordinal metrics are being used. These include opinion issues and potentially quantitative issues for which the approach does not yet supply appropriate quantitative tools. Both of the issues in the figure – attractiveness to industry and adequacy of infrastructure could be measured by surveys of public opinion or development of measurement tools, but are here treated by using ordinal scale judgments.

10.3.5 (Task 10.5) Adjust and Accumulate the Benefits of Each Option

Once the benefits of each option of the individual threat-asset pairs are adjusted and added, the options are arrayed together and examined for instances of:

- Robustness – one option (or design variation) reduces the risks or enhances the resilience of threat-asset pairs in addition to the one it was originally conceived to improve; and
- Synergies (positive or negative) – where options taken in combination generate benefits that are less than or greater than the sum of their individual benefits, a critical step in optimizing the ending portfolio.

Rate: 1. Option A
in terms of: Enhance Equity

User	(1) Excellen...	(2) Very goo...	(3) Good	(4) Moderate	(5) Poor
Brashear, Jerry					
Schott, Laurie				✓	
Rahman, Rasheq			✓		
Hamilton, Ted				✓	
Krimgold, Fred			✓		
Creel, James				✓	

Group Average: 0.355 5 out of 5 votes cast Voting On Alternative 1 out of 18

Rate: 2. Option B
in terms of: Enhance Equity

User	(1) Excellen...	(2) Very goo...	(3) Good	(4) Moderate	(5) Poor
Brashear, Jerry			✓		
Schott, Laurie			✓		
Rahman, Rasheq				✓	
Hamilton, Ted				✓	
Krimgold, Fred				✓	
Creel, James		✓			

Group Average: 0.438 6 out of 5 votes cast Voting On Alternative 2 out of 18

Figure 10.3 **Rating Options Relative to the objectives Not Calculated in RR/SAP**

Courtesy of Decision Lens Inc.

---

[22] Algebraically, risk-reduction benefits of an option = $(C*V*T)_{\text{no option}} - (C*V*T)_{\text{with option}}$; and resilience-enhancement benefits of an option = $(\text{Regional economic loss}*V*T)_{\text{no option}} - (\text{Regional economic loss}*V*T)_{\text{with option}}$.

This task identifies such robust and synergistic options and adjusting their evaluations accordingly.

To identify and carry out these adjustments, a matrix for *each* of the key decision metrics is prepared, such as the example in *Table 10.3*. For the region, the key decision metrics are:

1. Multi-attribute value score;
2. Expected casualties avoided;
3. Regional inclusive direct risk;
4. Regional direct resilience indicator reduction; and
5. Total regional risk/resilience indicator reduction.

For the owner, the key metrics are:

1. The inclusive owner's risk reduction and
2. Owner's resilience indicator reduction. Each of these is judged also as the ratio to the present value costs. Additional key metrics may be included if needed for the organization's standard budgeting processes.

These matrices can help identify robust and synergistic options. The matrix is constructed by listing all threat-asset pairs deemed unacceptable risks as rows, generally in the order of highest risk first, and the options as columns. Because the table only includes threat-asset pairs with risk larger than is acceptable, every threat-asset pair has at least one benefit (from the option designed for it), so the cells on the diagonal in the table all have entries. An option may also create benefits of *other* threat-asset pairs, as Option A does for threat-asset pair 2.2. For example, if a higher fence reduces the vulnerability to an attack by one assailant as well as an attack by two to four,

Table 10.3 **Example Identification of Robust and Synergistic Options: Owner's Risk-Reduction Benefits**

(Entries are gross benefits, based on owner's inclusive risk, except as marked.)

Threat-Asset Pairs	**Options**					
	Option A	Option B	Option C	Option D	Option B&D	Option …
1.1	579			339	339	
1.2		290			290	
1.3			209		74	
2.1				267	987	
2.2	440					
2.3		175			175	
…				407	407	
Total Gross Benefits	1,019	1,099	209	1,013	2,112	
Est. Effective Life of Option (Yr.)	3	1	20	5	1	
Present Value (@7%) of Gross Benefits for Life of Option	3,451	1,099	2,213	4,153	2,112	
Present Value Cost of Option	350	893	482	1,350	304	
Net Benefits	3,451-350= 3,101	1,099-893= 206	2,213-482= 1,731	4,153-1,350= 2,802	2,112-304= 1,808	
Net Benefit/Cost Ratio	3,101/350= 8.86	206/893= 0.23	1,731/482= 3.59	2,802/1,350= 2.08	1,808/304= 5.95	

the benefits of the two threat-asset pairs should be added together as the benefit of the option.

Each option is reviewed to determine whether it would also reduce (increase) risk or increase (reduce) resilience for any other threat-asset pairs, wholly or in part. Where there are synergies among the options (i.e., the total benefit of the combined options is greater than (or less than) the sum of their individual benefits), special note should be taken and the synergistic options considered as a combined option, as well as individually, as exemplified in the *Table 10.3* entry "Option B & D." Such synergistic options are treated as separate, new options with their unique benefits. For these robust options, the benefits are added together and costs are adjusted accordingly. For synergistic options, the benefits must be sorted out individually, possibly by re-analyzing the combination through the earlier analytic phases.

Option B&D is the combination of Options B and D. It exhibits two types of positive synergies: benefits of the combination exceed the sum of the two options taken singly, and cost efficiencies – the combined option costs less than the sum of options B and D individually. The process to this point will have identified and evaluated at least one option for each threat-asset pair with apparently positive net benefits. This creates the shaded diagonal in the figure.

In some instances, by contrast, the options may *reduce* the benefits when taken in combinations. This occurs when the options are fully or partly alternatives to one another, even if this was not the original intent. For example, the benefits of hardening a door to a facility might show the benefits of reducing vulnerability, but if this is done in the context of the high fence, the vulnerability is already reduced by the fence, so a portion of the benefits of the door, in conjunction with the fence, are double-counted. In this case, the combined options should be listed and treated as a single option, to be compared with two original options and all the others under consideration. This accumulates the total benefits of each option. After these adjustments are made, the columns are totaled for each option.

Because of the way the analysis is structured, we have estimated the annual risk and resilience, because we used the annual threat likelihoods. While some options have only annual effect (e.g., insurance policies), many are durable in the sense that their contributions to resilience and security last for as long as the option is in place and the threats and assets do not change. For these, it is necessary to estimate the option's useful life. If the option is a design feature in construction or major rehabilitation, the life could be the life of the asset it protects. A the effects of a training and exercise program, by contrast will last only as staff turnover and human memories permit. To account for such variable useful lives, the analysts estimate the number of years the option will be effective – the future "stream of benefits, as in an annuity – and calculates the present value of that stream using the organization's discount rate.

Of course, certain options will decline in effectiveness over time and other conditions may change. In a more sophisticated, multi-year analysis, these situations could be modeled explicitly, but for the present purposes, this adjustment is sufficient.

10.3.6 (Task 10.6) Estimate net benefits and marginal value of each option

This task continues the calculations shown above in *Table 10.3*. It calculates the net benefits and benefit/cost ratio to estimate the total value and risk-reduction efficiency (benefit/cost ratio) of each option. For risk, net benefit equals gross benefits (loss avoided) minus the present value of the costs. The benefit/cost ratio equals net benefits divided by the present value of the costs. The net benefits are the total value that each option adds, while the ratio is a direct measure of the amount of risk reduction per dollar of cost, an efficiency comparison. No option should be considered further on the risk-reduction metric if the net benefits calculation is not positive. There may be cases, such as Option B in the table where the benefit/cost ratio is less than unity, or one, where the option should be considered. The ratio simply means that the option is inefficient relative to the others, but it still produces significant benefits. However, for the other metrics, casualties, resilience and multi-attribute value score, there are no obvious threshold levels. Investment in an option may be justified by its results relative to *any* of the key decision metrics.

At this point, a sensitivity analysis of the leading candidate options for selection should be considered. By systematically examining the uncertainties in the benefit and cost estimates, the analyst can help the decision-maker understand the true range of values the selected options might bring. Some options that appear to yield high benefits may also have very high uncertainty. In this case, the benefits can be factored down to reflect the uncertain outcomes of the option.

For the multi-attribute objective value score, the data are entered into Decision Lens where they are aggregated for display such as in *Figures 10.4* and *10.5*, using a different set of options.

10.3.7 (Task 10.7) Choose and Allocate Resources to Options

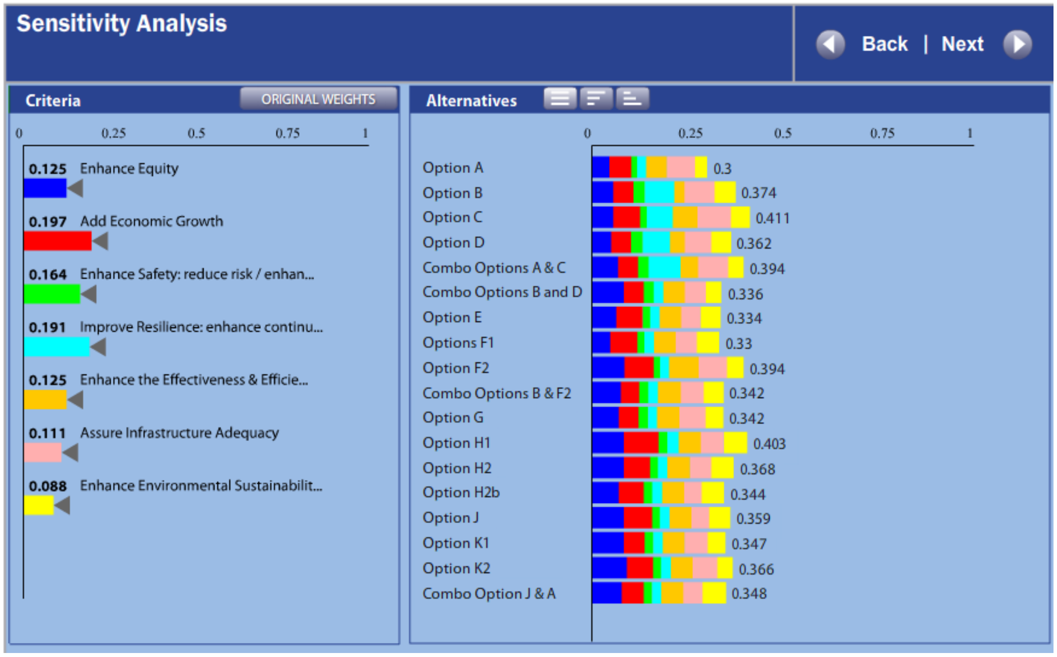
This task reviews the options considering all the key decision metrics to select among the options and allocate resources to the ones selected. To support these decisions, the options are displayed as in *Table 10.4*. Decision-makers should favor the options that have the highest multi-attribute value score, the greatest net benefits and benefit/cost ratios, the most expected casualties avoided, and the greatest reduction in the resilience indicators. Because the metrics are not necessarily correlated, decision-makers must use judgment to make the needed trade-offs and determine the resources – financial, human, and other – needed to operate the selected options. This 13-column table with all key indicators arrayed for each option and combination of options facilitates comparisons through iterative rankings by the respective metrics. These displays might be augmented by graphic displays such as shown in *Figure 10.4*, which also shows which major objectives contribute to the overall score.

As discussed earlier, both relevant perspectives of the decision-makers, that of the owner of the asset and that of the regional community, are displayed to both sets of decision-makers to promote shared understanding of the situation and the options to be considered. To the owner, risk is the consequence (threat- and vulnerability-weighted) incurred by the owner. Resilience for the owner is a rapid return to full function to minimize lost revenue, restore a reputation for reliability, etc. From the community's perspective, the risk is more inclusive and resilience is indicated by the lost economic activity (threat- and vulnerability-weighted) due to service denial.

Table 10.4 **Display of Key Decision Metrics for the Respective Options**

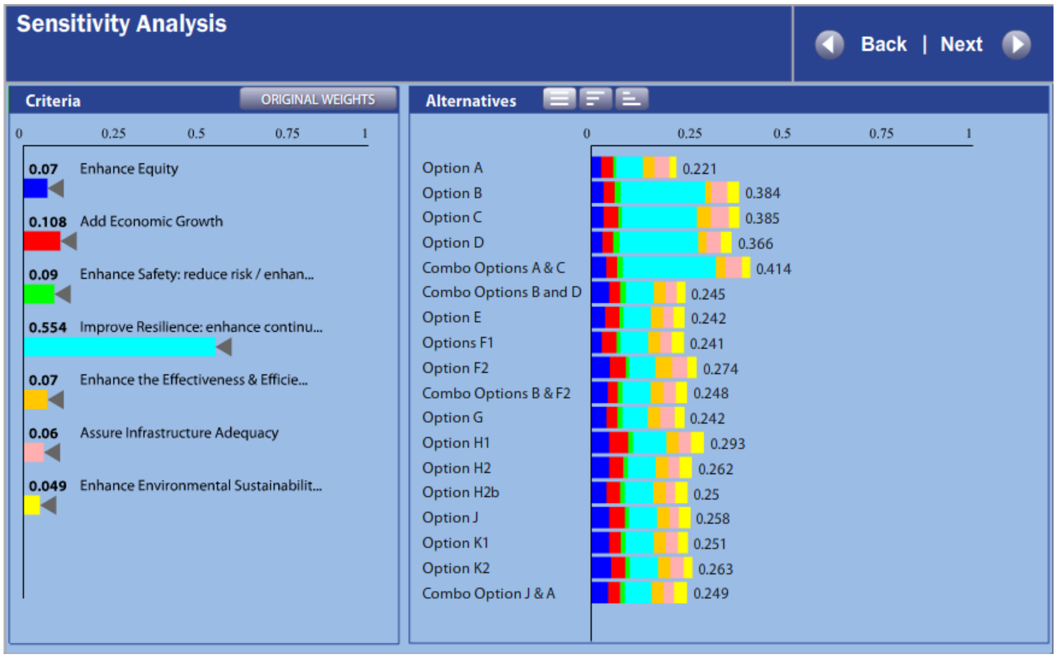
	Regional Community										Owner			
Benefit Metrics	Multi-Attribute Objective Value		Expected Casualties Avoided		Inclusive Direct Risk Reduction		Direct Resilience Indicator Reduction		Total Regional Risk/Resil. Improvement		Inclusive Risk Reduction		Resilience Indicator Reduction	
Option Descriptions	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $	No.	Per $
A														
B														
C														
D														
E														
Etc.														

Figure 10.4 **Options Ranked by Multi-Attribute Objective Value Score**



Courtesy of Decision Lens Inc.

Figure 10.5 **Multi-Attribute Scores with Higher Priority on Resilience**



Courtesy of Decision Lens Inc.

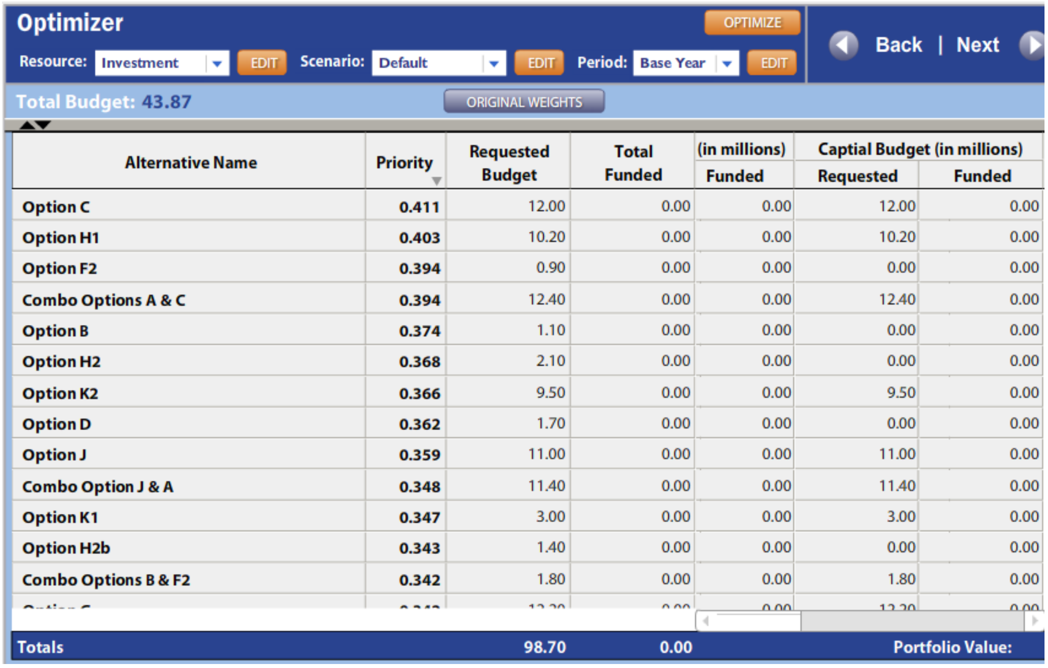
The welfare economics and public policy literatures have long used the consequences to the public (or – synonyms to economists – "society" or "the economy") while the business and micro-economic literatures have stressed the consequences to the owner/operator and his stakeholders. Because the RR/SAP is designed to support decision-makers in both public and private sectors and at both single-agency and oversight levels, both perspectives are included as separate metrics. Decision-makers in both sectors can gain insights by examining both metrics. The owner makes decisions to maximize the value for the stakeholders, while recognizing a civic duty; a public official or members of a public-private partnership are more interested in maximizing the value to the regional community, but need to know whether a case can be made for private investment in options that also benefit the public.

Sensitivity analysis can be performed on the aggregated multi-attribute value scores by varying the priorities assigned to the respective attributes of value. *Figure 10.5* shows the same information as in *Figure 10.4*, but with substantially greater weight assigned to the resilience objective. Note that the order of preference among the options changes as the priorities change.

Regardless of the perspective of the decision-maker, the method for selecting options to be included in the budget is the same. It relies on ranking based on the estimated net benefits, with adjustments "at the margin" – among the last-chosen options. The specific metrics are carefully explained to the decision-makers, so they fully understand the estimates before them.

The most effective way to develop a final ranking of options that falls within the budgetary constraints is to *tentatively* accept all options as they are ranked by net benefits until their cumulative cost reaches the available budget. This list includes a number of the options that ranked high on the benefit/cost ratio ranking. Those are clearly accepted. The remaining unselected options with the greatest benefit/cost ratios are compared with the option(s) that are lowest-ranked by net benefit but still included within the budget constraint. Judgment is required to make the trade-offs among large-benefit options and high-efficiency options, but

Figure 10.6 **Resource Allocation by Multi-Attribute Objective Value Score Per Dollar**



Resource: Investment Scenario: Default Period: Base Year

Total Budget: 43.87

Alternative Name	Priority	Requested Budget	Total Funded	(in millions)	Captial Budget (in millions)	
				Funded	Requested	Funded
Option C	0.411	12.00	0.00	0.00	12.00	0.00
Option H1	0.403	10.20	0.00	0.00	10.20	0.00
Option F2	0.394	0.90	0.00	0.00	0.00	0.00
Combo Options A & C	0.394	12.40	0.00	0.00	12.40	0.00
Option B	0.374	1.10	0.00	0.00	0.00	0.00
Option H2	0.368	2.10	0.00	0.00	0.00	0.00
Option K2	0.366	9.50	0.00	0.00	9.50	0.00
Option D	0.362	1.70	0.00	0.00	0.00	0.00
Option J	0.359	11.00	0.00	0.00	11.00	0.00
Combo Option J & A	0.348	11.40	0.00	0.00	11.40	0.00
Option K1	0.347	3.00	0.00	0.00	3.00	0.00
Option H2b	0.343	1.40	0.00	0.00	0.00	0.00
Combo Options B & F2	0.342	1.80	0.00	0.00	1.80	0.00
Totals		98.70	0.00		Portfolio Value:	

Courtesy of Decision Lens Inc.

this need only be done near the cut-off point, i.e., at the margin. The approach is repeated until all the highest benefit-cost options have been considered with all the lowest net benefit options still within the budget. Use of this method forces the trade-offs to be only at the margin, the last few options selected.

If the options are roughly comparable in the scale of net benefits, the benefit/cost ratios or the value score/dollar may be used to select options. *Figure 10.6* shows the Decision Lens solution based on multi-attribute value score/dollar. Three of the options with the highest scores were not funded because their value per dollar fell below many other options. It is also notable that, while less than half of the requested funding was available, the project selection using this method produced 70% of the value if all the options had been funded (the "Portfolio Value" in the lower right corner).

Judgment is also required to weigh the respective consequence metrics – multi-attribute objective score, reduced casualties, financial losses to the asset's owner, lost economic activity to the community and the qualitative consequences, such as public confidence, military readiness, etc.

Many decision-makers prefer to see all the key metrics so they can make additional marginal trade-offs. These choices are perfectly reasonable, especially made at this point, when the actual trade-offs are determined as adjustments to enhance a numerically near-optimal selection.

Finally, as the selection process approaches its conclusion, certain practical considerations also play a role, including:

- Are there risks the option might not work as planned? What is the "track record" with this option?Are there any non-financial constraints the option violates?
- Will the option accord with the organization's core technology, values, culture and public image?
- Will any of the organization's stakeholders be offended by the option?

At this point, the collection of options selected constitutes a tentative security and resilience portfolio in proper form for inclusion in the larger budget process. A review of the selected options *as a portfolio* will further improve the selection of options. In reviewing the selection of options, it is important to consider whether some options may interact with others in ways not identified in the robustness test in Task 10.5. For example, if the owner installs a double security fence with dogs or patrols between, hardening a door inside the second fence may have significantly less benefit than without the fences. Similarly, there may be trade-offs between risk-reduction and resilience-enhancement options.

Increasing the security of a facility alone may improve resilience by reducing the likelihood of an unwanted event or the vulnerability to the event. In such cases, the benefit estimates should be corrected for the context of the portfolio in which they appear. In this sense, an option may have somewhat different benefits depending on what other options are in its portfolio. Failure to look for these adjustments may lead to missed opportunities or over-valued options. The final choice of options should, for this reason, be as a portfolio of options, not simply a list.

The final decision step is to consider security and resilience options as elements in the organization's overall portfolio of investments and operations. Few organizations have the capacity to undertake this review, but added benefits and efficiencies await those who do. Enterprise risk management and asset portfolio optimization are being implemented by increasing numbers of organizations in both public and private sectors.

10.3.8 (Task 10.8) Manage the Selected Options

This task consists of implementing, monitoring and evaluating the performance of the selected options. Once the portfolio for enhancing security and resilience has been selected, it must be implemented with the same management direction and oversight as other important activities – these elements were selected expressly because they address important aspects of the vitality of the organization and the community. They must be planned in detail and implemented in an orderly manner, with the effectiveness of their implementation assured at the beginning and the effectiveness of their operation periodically evaluated. "Mid-course corrections" may be required, especially if the options contain novel elements. Implementation of some major infrastructure projects may consist of developing more detailed designs and engineering plans and revising the cost and delivery schedules. The fact that an option was selected through the risk analysis does not mean it goes forward without further question. Rather, such a project would be re-evaluated relative to the conditions, constraints and alternatives available in each stage of design, engineering and construction.

10.3.9 (Task 10.9) Repeat the Regional Resilience/Security Analysis Process

Risk and resilience management is a continuous process. New risk and resilience assessments should be undertaken periodically for a variety of reasons, including:

- A way to measure progress and accountability in reducing and enhancing resilience, based on previously implemented programs;
- As part of the organization's commitment to continuous improvement; and
- To update the security and resilience posture to address new or emerging conditions, e.g., climate change, new intelligence on terrorists' plans, and new threats, such as pandemics.

Generally, organizations find it useful to revise and update their risk and resilience assessments on a periodic basis, often annually or biennially, as coordinated with their internal budgeting. Some also establish standards by which any new capital proposal must be accompanied by a full risk/resilience assessment of the proposed asset or facility. The RR/SAP approach is objective and quantitative enough to measure progress and accountability of the implemented options. Because it is relatively inexpensive and non-disruptive to apply, annual updates are feasible, but most organizations schedule the most complete, full double-cycle process for every second or third year, with interim updates as conditions warrant. Many organizations use the "off-years" to analyze the higher ranking threat-asset pairs that were deferred in the early prioritizing in the Assessment Cycle's Phase 2.

10.4 Conclusions

The overall RR/SAP has been developed to the present as an in-depth prototype to demonstrate the feasibility of the logic of the business process. It is clearly feasible and serves a critically important function that no other known process does. It is not at this time, however, a fully developed and integrated tool, ready to be disseminated. Each of the basic phases needs additional development work and field-testing to make it efficient and effective at performing its specific role in the process. First, the basic set-up work of acquiring the right organizational, GIS and operating information about the region and its major infrastructure, governmental and economic entities could be reduced to simple, automated questionnaires and standard processes for collecting the data and synthesizing it into a viable understanding of the region. The RAMCAP process should be automated to reduce the time to administer it and expedite the calculations. Developing simple, yet effective models of the processes of each system are essential and could be a program of research in itself. In addition, the respective phases need to be aligned and smoothly integrated. And, finally, all aspects of the process need to be automated, with solid, decision-oriented interfaces that directly support both the analytic decisions made during the analysis and the final selection of a "near-optimal" portfolio for value, security and resilience.

If this work is carried out and the RR/SAP is disseminated to the state, local and federal field agencies and private corporations that provide infrastructure services, American infrastructure will have the chance to be more resilient, effective and cost-effective. The RR/SAP could provide the basis for a national program to enhance resilience through grants, loans and loan guarantees. The proposed infrastructure bank and/or DHS programs could take the lead in initiating this program. The benefits would be those sketched at the end of Chapter One.

BIBLIOGRAPHY

Abraham, J.E. and J.D. Hunt. 1999. Policy analysis using the Sacramento MEPLAN land use-transportation interaction model. *Transportation Research Record*, 1685: 199–208.

American Petroleum Institute and the National Petrochemical and Refiners Association. October 2004. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries,* Second Edition (includes reporting form templates).

Anderson, C.W., J.R. Santos, and Y.Y. Haimes. 2007. A risk-based input-output methodology for measuring the effects of the August 2003 Northeast Blackout. *Economic Systems Research*, 19(2): 183-204.

ANSI/ASME-ITI/AWWA. 2010. J100-10 Risk Analysis and Management for Critical Asset Protection (RAMCAP) Standard for Risk and Resilience Management of Water and Wastewater Systems, an American National Standard.

Arnold, R., De Sa, J., Gronniger, T., Percy, A., Somers, J. 2006. A Potential Influenza Pandemic: Possible Macroeconomic Effects and Policy Issues. Congressional Budget Office.

ASCE. 2009. 2009 Report Card for America's Infrastructure. American Society of Civil Engineers. http://www.infrastructurereportcard.org/sites/default/files/RC2009_full_report.pdf

ASME-ITI. 2004. Risk Analysis and Management for Critical Asset Protection: General Guidance.

ASME-ITI. 2005a. Introduction to Risk Analysis and Management for Critical Asset Protection.

ASME-ITI. 2005b. Risk Analysis and Management for Critical Asset Protection (RAMCAP) Applied to Terrorism and Homeland Security.

ASME-ITI. 2005c. Sector-Specific Guidance: Nuclear Power Plants.

ASME-ITI. 2005d. Sector-Specific Guidance: Spent Fuel Transportation and Storage.

ASME-ITI. 2005e. Sector-Specific Guidance: Petroleum Refining.

ASME-ITI. 2005f. Sector-Specific Guidance: Chemical Manufacturing.

ASME-ITI. 2005g. Sector-Specific Guidance: Liquefied Natural Gas Off-Loading Ports.

ASME-ITI. 2006. RAMCAP Framework©, Version 2.0.

ASME-ITI. 2007a. Sector-Specific Guidance: Dams and Navigational Locks.

ASME-ITI. 2007b. Sector-Specific Guidance: Water and Wastewater Systems.

ASME-ITI. 2008. Sector-Specific Guidance: Risk Management for Higher Education.

ASME-ITI. 2009. All-Hazards Risk and Resilience: Prioritizing Critical Infrastructure Using the RAMCAP Plus Approach.

ASME-ITI/ANSI. 2010. Higher Education Risk to Natural and Manmade Hazards. An American National Standard.

Baker, Arnold, et al. 2002. A Scalable Systems Approach for Critical Infrastructure Security. Sandia National Laboratories. SAND 2002-0877, www.sandia.gov/scada/documents/020877.pdf.

Barker, K.A., Santos, J.R. 2010. Measuring the efficacy of inventory with a dynamic input–output model. *International Journal of Production Economics*, 126(1): 130-143

Bernstein, P. L. 1998. *Against the Gods: The Remarkable Story of Risk.* John Wiley & Sons, New York.

BICE. 2009. *Sustainable Critical Infrastructure Systems – a Framework for Meeting 21st Century Imperatives*. Board on Infrastructure and the Constructed Environment, Division on Engineering and Physical Sciences.

Brealey, R. and Myers, S. 2000. *Principles of Corporate Finance.* Sixth Edition, Boston, MA: Irwin McGraw-Hill.

Brigham, E., L. Gapenski and M. Ehrhardt. 1999. *Financial Management: Theory and Practice.* Ninth Edition, Fort Worth, TX: The Dryden Press.

Building America's Future. 2011. Transportation Infrastructure Report 2011: Falling Apart and Falling Behind. http://www.bafuture.org/sites/default/files/Report_0.pdf

Bureau of Economic Analysis. 2008. Local Area Personal Income. <http://www.bea.gov/bea/regional/reis/>

Bureau of Economic Analysis. 2011. Glossary G and L. Available online: http://www.bea.gov/glossary/glossary.cfm?letter=L and http://www.bea.gov/glossary/glossary.cfm?letter=G

Bureau of Economic Analysis. 2011. Table 3.7ES, Investment in Private Fixed Assets by Industry. http://www.bea.gov/iTable/iTable.cfm?ReqID=10&step=1

Bureau of Transportation Statistics. 2008. Commodity Flow Survey. Available online: <http://www.bts.gov/programs/commodity_flow_survey/>

Burrus, R.T., C.F. Dumas, C.H. Farrell and W.W. Hall. 2002. The Impacts of Low-Intensity Hurricanes on Regional Economic Activity. *Natural Hazards Review*, 3(3):118-125.

Center for Chemical Process Safety. 1995. Tools for Making Acute Risk Decisions: with Chemical Process Safety Applications. American Institute of Chemical Engineers.

Center for Risk and Economic Analysis of Terrorism Events, University of Southern California, http://create.usc.edu/ (contains terrorism risk analysis papers from various CREATE symposia).

Corbett, John. Ian McHarg. 2001. Overlay Maps and the Evaluation of Social and Environmental Costs of Land Use Change. http://www.csiss.org/classics/content/23.

Crowther, K.G., Y.Y. Haimes, G. Taub. 2007. Systemic Valuation of Strategic Preparedness with Illustrations from Hurricane Katrina. *Risk Analysis*, 27(5): 1345–1364.

CSIS. 2006. *Guiding Principles for Strengthening America's Infrastructure*. Center for Strategic and International Studies, Commission on Public Infrastructure.

Decision Lens 2009. Analytic Hierarchy Process. http://www.decisionlens.com/products/process/.

de la Barra T. 1995. *Integrated Land Use and Transport Modeling: Decision Chains and Hierarchies*. Cambridge University Press, New York, NY.

Department of Homeland Security. 2003. Homeland Security Presidential Directive-5: Management of Domestic Incidents. Available online: <http://www.fas.org/irp/offdocs/nspd/hspd-5.html>

Department of Homeland Security. 2009. National Infrastructure Protection Plan (NIPP). Available online: <http://www.dhs.gov/files/programs/editorial_0827.shtm>

Department of Homeland Security. 2008. National Response Framework (NRF). Available online: <http://www.fema.gov/NRF>

Department of Homeland Security. 2003. Presidential Directive-7: Critical Infrastructure Identification, Prioritization, and Protection. Available online: <http://www.fas.org/irp/offdocs/nspd/hspd-7.html>

Dietzenbacher E. and M.L. Lahr. *Wassily Leontief and Input-Output Economics*, Cambridge University Press, Cambridge, UK, 2004.

Dyer, J. S. 1990. Remarks on the analytic hierarchy process. *Management Science*, 36(3) 249-258.

Echenique, M.H. 1985. The use of integrated land use transportation planning models: The cases of Sao Paolo, Brazil and Bilbao, Spain. *The Practice of Transportation Planning*, The Elsevier, Hague.

Environmental Protection Agency. 2000. Guidelines for Preparing Economic Analyses. EPA 240-R-00-003.

Environmental Protection Agency. 2004. Risk Management Plan (RMP) COMP^{TM}. www.epa.gov/emergencies/rmp.

Environmental Protection Agency. 2010. Valuing Mortality Risk Reductions for Environmental Policy: A White Paper (Draft). National Center for Environmental Economics.

Firestone, D. 2003. Power Failure Reveals a Creaky System, Energy Experts Believe. *The New York*

Times, August 15, 2003. http://www.nytimes.com/2003/08/15/nyregion/15GRID.html

Fishhoff, B. 2002. Assessing and Communicating the Risks of Terrorism. *Science and Technology in a Vulnerable World*.

Fleming, S. 2009. E&Y Ranks Top 10 Business Risks for Commercial Real Estate. *National Real Estate Investor*. http://nreionline.com/finance/news/ernest_young_ranks_0408/

Food and Drug Administration. 2011. Food Labeling: Nutritional Labeling. Docket No. FDA-2011-F-0172.

Forman, E.H. and S.I Gass. The analytical hierarchy process – an exposition. *Operations Research 49.4 (July-August 2001): 469(18)*

Forrester, Jay W. 1961. Industrial Dynamics. Pegasus Communications. ISBN 1883823366.

Forrester, Jay W. 1969. Urban Dynamics. Pegasus Communications. ISBN 1883823390.

GMU/CIP. 2005. "Critical Infrastructure Protection in the National Capital Region: Risk-Based Foundations for Resilience and Sustainability."

Gass, S.I. 2005. Model World: The Great Debate – MAUT Versus AHP. *Interfaces*, Vol. 35, No. 4, July-August, pp. 308-312.

Grove, John M. de. 1965. Review: [untitled]. *The Yale Law Journal* 74 (3) (January 1): 588-593. doi:10.2307/794677.

Haggerty, M., J.R. Santos, and Y.Y. Haimes. 2008. A Transportation-Based Framework for Deriving Perturbations to the Inoperability Input-Output Model. *Journal of Infrastructure Systems*, 14(4): 293-304.

Haimes, Y.Y. and P. Jiang. 2001. Leontief-Based Model of Risk in Complex Interconnected Infrastructures. *Journal of Infrastructure Systems*, 7(1): 1-12.

Haimes, Y.Y., B.M. Horowitz, J.H. Lambert, J.R. Santos, K. Crowther, and C. Lian. 2005. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. *Journal of Infrastructure Systems*, 11(2): 67-79.

Holling, C. 1973. Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, 4: 1–23.

Howe, D. 2005. National Planning Scenarios. Available online: <http://media.washingtonpost.com/ wp-srv/nation/nationalsecurity/earlywarning/ NationalPlanningScenariosApril2005.pdf>

Huddleston, J. R. 2005. An Introduction to Local Government Budgets: A Guide for Planners. *Materials prepared for the Workshop on Curriculum for Graduate Planning Programs: The Nuts and Bolts of Development Finance. Cambridge: Lincoln Institute of Land Policy*.

Hunt, J.D. and D.C. Simmonds. 1993. Theory and application of an integrated land-use and transport modeling framework. *Environment and Planning B*, **20:** 221–244.

Hutchinson, Harry. 2005. Calculating Risks: Can the Science that Judges the Safety of Nuclear Plants Secure the Infrastructure of a Nation. *Mechanical Engineering.*

Isard, W. 1960. *Methods of Regional Analysis: An Introduction to Regional Science*. MIT Press, Cambridge, MA.

Jordan, M. 2003. Punctuations and agendas: A new look at local government budget expenditures. *Journal of Policy Analysis and Management* 22 (3) (June 1): 345-360. doi:10.1002/pam.10136.

Keeney, R. L., H. Raiffa. 1976. *Decisions with Multiple Objectives: Preference and Value Tradeoffs*. John Wiley & Sons, New York.

Kendrick J. and D. Saaty. 2007. Use Analytic Hierarchy Process for Project Selection. Decision Lens Inc., 2007.

Kirkwood, Craig W. 1997. *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*. Wadsworth Publishing Co., New York.

Kusnetzky, Dan. 2010. What is “Big Data?” ZDNet. http://www.zdnet.com/blog/virtualization/what-is-big-data/1708.

Leontief, W. 1936. Quantitative input and output relations in the economic system of the United States. *Review of Economics and Statistics*, 18(3): 105-125.

Leontief, W.W. 1951. Input-Output Economics. *Scientific American*, pp. 15-21, October.

Leontief, W.W. 1951. *The Structure of the American Economy, 1919-1939, Second Edition.* Oxford University Press, New York.

Lian, C. and Y.Y. Haimes. 2006. Managing the Risk of Terrorism to Interdependent Infrastructure Systems Through the Dynamic Inoperability Input-Output Model. *Systems Engineering*, 9(3): 241-258.

Lian C., Santos, J.R., Y. Y. Haimes. 2007. Extreme Risk Analysis of Interdependent Economic and Infrastructure Sectors. *Risk Analysis, an International Journal*, 27(4): 1053-1064.

LMSRA. 2009. *Building America’s Future National Survey of Registered Voters*. Luntz Maslansky Strategic Research Analysis.

Lowrance, W.W. 1976. *Of Acceptable Risk: Science and the Determination of Safety*. Kaufmann, Los Altos, CA.

Lowry, I.S. 1964. *Model of Metropolis* (RM-4035-RC), RAND Corporation, Santa Monica, CA.

Luce, R.D., H. Raiffa. 1957. *Games and Decisions,* John Wiley and Sons, New York.

Markowitz, H. M. 1952. Portfolio Selection. *J. Finance* 7 (1): pp. 77-91.

McCarthy, J. A., and J. Brashear. 2005. *Critical Infrastructure Protection in the National Capital Region: Risk-Based Foundations for Resilience and Sustainability.* University Consortium for Infrastructure Protection, Critical Infrastructure Program, George Mason University School of Law, Arlington, Virginia.

Miller R.E. and P.D. Blair, 2009. *Input-output Analysis: Foundations and Extensions, 2nd ed.* University Press, Cambridge, UK.

Minnesota IMPLAN Group. 2008. Impact Analysis for Planning (IMPLAN). Available Online: <http://www.implan.com/>

Moe, T. M. 1984. "The new economics of organization." *American Journal of Political Science*: 739–777.

Morgenstern, O. and Von-Neumann, J. 1944. *Theory of Games and Economic Behavior*. Princeton University Press.

Moteff, John. September 2, 2004. "Risk Management and Critical Infrastructure Protection: Assessing, Integrating and Managing Threats, Vulnerabilities, and Consequences," Congressional Research Service, Library of Congress (order code RL32561).

Multihazard Mitigation Council. December 2005. *Natural Hazard Mitigation Saves: Independent Study to Assess the Future Benefits of Hazard Mitigation Activities*, *Volume 2 - Study Documentation.* Prepared for the Federal Emergency Management Agency of the U.S. Department of Homeland Security by the Applied Technology Council under contract to the Multihazard Mitigation Council of the National Institute of Building Sciences, Washington, D.C.

MWCOG, 2011. Metropolitan Washington Council of Governments, accessed at http://www.mwcog.org/transportation/activities/models/4step/4_step.asp on December 14, 2011.

NASBO. 1999. *Capital Budgeting in the States*. National Association of State Budget Officers.

National Cooperative Highway Research Program (NCHRP), 2001. *Report 456: Guidebook for Assessing the Social and Economic Effects of Transportation Projects*. National Academies Press, Washington, DC.

National Oceanic and Atmospheric Administration. 1999. Hurricane Return Period Database. http://www.nhc.noaa.gov/HAW2/english/basics/return_printer.shtml

National Research Council. 2002. "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," The National Academic Press, Washington, D.C. (esp. Chapter 10, with its extensive bibliography).

Office of Management and Budget (OMB), 2003. OMB Circular No. A-4, "Regulatory Analysis."

Orszag, P. 2008. "Investing in Infrastructure," Testimony before the Committee on Finance, U.S. Senate, July 10, 2008. http://www.cbo.gov/ftpdocs/95xx/MainText.1.2.shtml, accessed June 22, 2009.

Perrings, C. 2001. Resilience and Sustainability. In H. Folmer, H. L. Gabel, S. Gerking, A. Rose (Eds.), *Frontiers of Environmental Economics*. Cheltenham, pp. 319–41. U.K.: Edward Elgar.

Resurreccion JZ, Santos JR, 2011. Developing an Inventory-Based Prioritization Methodology for Assessing Inoperability and Economic Loss in Interdependent Sectors, *IEEE Proceedings of Systems and Information Engineering Design Symposium*, pp. 176-181.

Rose, A. 2004. "Economic Principles, Issues, and Research Priorities in Natural Hazard Loss Estimation" in Okuyama Y. and Chang S. (eds.), *Modeling the Spatial Economic Impacts of Natural Hazards,* Heidelberg: Springer, 2004, pp.13-36.

Rose, A. 2006. "Economic Resilience to Disasters: Toward a Consistent and Comprehensive Formulation," in Paton D. and Johnston D. (eds.), *Disaster Resilience: An Integrated Approach*, Springfield, IL: Charles C. Thomas, 2006, pp. 226-48.

Rose, A. 2007. "Macroeconomic Modeling of Catastrophic Events," in Quigley J. and Rosenthal L. (eds.), *Real Estate, Catastrophic Risk, and Public Policy,* Berkeley, CA: Berkeley Public Policy Press, forthcoming.

Rose, A. and Liao, S., 2005. "Modeling Regional Economic Resilience to Disasters: A Computable General Equilibrium Analysis of Water Service Disruptions," *Journal of Regional Science,* Vol. 45, No. 1, 2005, pp. 75-112.

Rose, A., Oladosu G., and Liao S., 2007. "Business Interruption Impacts of a Terrorist Attack on the Water System of Los Angeles: Customer Resilience to a Total Blackout," in Richardson, H., Gordon, P., and Moore, J. (eds.), *Economic Costs and Consequences of Terrorist Attacks*, Cheltenham, UK, pp. 291-316.

Ruiz-Juri, N. and Kockelman, K.M., 2006. Evaluation of the Trans-Texas Corridor Proposal: Application and Enhancements of the Random-Utility-Based Multiregional Input-Output Model, *Journal of Transportation Engineering*, 132 (7): 531-539.

Saaty, T. L. 1980. The Analytic Hierarchy Process. McGraw-Hill Book Co., New York.

Saaty, T.L. and Vargas, L. 1982. *The Logic of Priorities: Applications in Business, Energy, Health and Transportation,* Kluwer-Nijhoff Publishing, Boston.

Saaty, T.L. and Alexander J. 1989. *Conflict Resolution: The Analytic Hierarchy Approach,* Praeger, New York.

Santos, J.R., 2006. Inoperability Input-Output Modeling of Disruptions to Interdependent Economic Systems. *Systems Engineering*, 9(1): 20-34.

Santos, J. R., 2008. Inoperability Input-Output Model (IIM) with Multiple Probabilistic Sector Inputs, *Journal of Industrial Management and Optimization*, 4(3): 489-510.

Santos, J.R. and Haimes, Y.Y., 2004. Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures, *Risk Analysis* 24(6):1437-1451.

Santos, J.R., Y. Y. Haimes, and C. Lian, 2007. A Framework for Linking Cyber Security Metrics to the Modeling of Macroeconomic Interdependencies, *Risk Analysis: An International Journal*, 27(4): 1283-1297.

Santos, J.R., K. Barker, and P. Zelinke, 2008. Sequential Decision-making in Interdependent Sectors with Multiobjective Inoperability Decision Trees, *Economic Systems Research*, 20(1): 29-56.

Savage, L.J. 1954. The Foundations of Statistics. Wiley: New York.

Snowden, D. 2002. “Complex acts of knowing: paradox and descriptive self-awareness.” Journal of knowledge management 6 (2): 100–111.

Springer, D., and G. Dierkers. 2009. *An Infrastructure Vision for the 21st Century: Strengthening our Infrastructure for a Sustainable Future*. National Governors Association.

Stevens, S. S., 1946. “On the Theory of Scales of Measurement,” *Science*, June 7, Vol.103, No. 2684: 677–680.

Steyaert, Patrick, and Janice Jiggins. 2007. “Governance of complex environmental situations through social learning: a synthesis of SLIM’s lessons for research, policy and practice.” Environmental Science & Policy 10 (6) (October): 575-586. doi:10.1016/j.envsci.2007.01.011.

Teich, S. D. Nelson, and S. J. Lita (eds.), AAAS, Washington, D.C., pp. 51-64.

Tennessee Department of Revenue, State of Tennessee. http://www.tn.gov/revenue/tntaxes/salesanduse.htm, (accessed 31 October 2011).

The Infrastructure Security Partnership (TISP), 2006. Regional Disaster Resilience: A guide for developing an action plan. American Society of Civil Engineers, Reston, VA. Available online: <www.llis.gov>, document #19458.

The White House, July 15, 1996. Executive Order 13010: *Establishing the President’s Commission on Critical Infrastructure Protection (PCCIP)*. Available online: <http://www.fas.org/irp/offdocs eo13010.htm>

Tyler, C., and J. Willand. 1997. “Public budgeting in America: A twentieth century retrospective.” *Public budgeting and financial management,* 9: 31.

ULI. 2009. *Infrastructure 2009: Pivot Point*. The Urban Land Institute and Ernst & Young.

URISA. GIS Hall of Fame - Ian McHarg | URISA. http://www.urisa.org/node/394.

US Census Bureau, 2007. *Journey to Work and Place of Work*. Available Online: <http://www.census.gov/population/www/socdemo/journey.html>

U.S. Census Bureau. 2011. Table 437, State and Local Government - Capital Outlays: 1990 to 2008.

US Department of Commerce. 1997. Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System, Washington, DC: U.S. Government Printing Office.

U.S. Department of Commerce. 2006. National Institute of Standards and Technology. *Ninth Annual Report on Federal Agency Use of Voluntary Consensus Standards and Conformity Assessment*. Washington, D.C.: Government Printing Office.

U. S. Department of Homeland Security. 2004. "DHS Interim Rule on Procedures Associated with Sharing and Handling of Information Designated as Critical Infrastructure Information." *Federal Register*, Vol. 69, No. 34, pp. 8074-8089.

U.S. Department of Homeland Security. 2006. National Infrastructure Protection Plan.

U.S. Department of Homeland Security. 2009. National Infrastructure Protection Plan. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

U.S. Department of Homeland Security. 2010. DHS Risk Lexicon, 2010 Edition.

U.S. Department of Transportation. 2009. Land Use Compendium, DOT-T-99-03: Enhancement of DVRPC's Travel Simulation Models Task 12: Review of Land Use Models and Recommended Model for DVRPC. Available online: <http://tmip.fhwa.dot.gov/clearinghouse/docs/landuse/compendium/intro.stm>

U.S. Department of Transportation. 2003. U.S. Department of Transportation, "Revised Departmental Guidance Valuation of Travel Time in Economic Analysis," signed 2-11-03.

U.S. Department of Transportation. 2011. Trottenberg and Rivkin, "Economic Value of a Statistical Life."

U.S. Government Accountability Office. October 12, 2001. "Homeland Security: Key Elements of a Risk Management Approach," GAO-02-150T.

U.S. Government Printing Office. 2007. "Historical Tables: Budget of the United States Government." ISN 978-0-16-077509-3.

U.S. Nuclear Regulatory Commission, November 1995, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission," Final Report, NUREG/BR-0058, Revision 2

Wallenius et al., 2008. Multiple Criteria Decision Making and Multi-attribute Utility Theory Management Science 54(7), pp. 1336–1349.

Wildavsky, A. B. 1964. *The politics of the budgetary process*. Little, Brown Boston.

Zhao, Y. and K.M. Kockelman, 2004. The Random-Utility-Based Multiregional Input-Output Model: Solution Existence and Uniqueness, *Transportation Research B,* 38(9): 789-807.

GLOSSARY

Note: Wherever possible, the U.S. Department of Homeland Security's *DHS Risk Lexicon* (DHS, 2010) has been used to advance the common use of risk analysis terms. Where the Lexicon's definition is used verbatim, it is shown in italics. Otherwise, these definitions conform to the ANSI/ASME-ITI/AWWA Standard J100 (2010).

1. ***Acceptable Risk*** *– Level of risk at which, given costs and benefits associated with risk reduction measures, no action is deemed to be warranted at a given point in time.*
2. ***Adversary*** *– An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.* Adversaries may include intelligence services of host nations or third party nations, political and malevolent groups, criminals, rogue employees and private interests. *Adversaries* can include site insiders, site outsiders, or the two acting in collusion.
3. ***Analytic Hierarchy Process*** – A decision methodology used for systematically addressing multi-criterion decisions or multi-attribute evaluations in a consistent manner.
4. ***Asset*** *– A person, structure, facility, information, material, or process that has value. Includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources, personnel, intelligence, technology, or physical infrastructure, or anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned; from an intelligence standpoint, includes any resource – person, group, relationship, instrument, installation, or supply – at the disposal of an intelligence organization for use in an operational or support role.*

   In the context of critical infrastructure, an asset is something of importance or value that, if targeted, exploited, destroyed, or incapacitated, could result in injury, death, economic damage to the owner of the asset or to the community it serves, destruction of property, or could profoundly damage a nation's prestige and confidence. Assets may include physical elements (tangible property), cyber elements (information and communication systems), and human or living elements (critical knowledge and functions of people).

   4.1 Critical asset – An asset whose absence or unavailability would significantly degrade the ability of an organization to carry out its mission or would have unacceptable financial, political or environmental consequences for the owner or the community.
5. ***Baseline Risk*** *– Current level of risk that takes into account existing risk mitigation measures.*
6. ***Bayesian Probability*** *– The process of evaluating the probability of a hypothesis through 1) the specification of a prior probability and 2) modification of the prior probability by incorporation of observed information to create an updated posterior probability.*
7. ***Consequence*** *– Effect of an event, incident, or occurrence. Consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.* The immediate, short- and long-term effects of a malevolent event or natural incident. These effects include losses suffered by the owner of the asset and by the community served by that asset. They include human and property losses, environmental damages and lifeline interruptions. Property damage and losses from interruption of operations are expressed in monetary units. Consequences involving loss of life, injury, loss of lifelines and environmental damage may be measured in either or both of two ways: (1) natural units reported and considered individually (e.g., fatalities, number of serious injuries, losses in dollars); or (2)

converted to a single, summary economic value, reported and considered as a single loss indicator (See Section A-4.7.6).

8. ***Consequence Mitigation*** – A series of planned and coordinated actions or system features designed to: reduce or minimize the damage caused by events (consequences of an event); support and complement emergency forces (first responders); facilitate field-investigation and crisis management; and facilitate rapid recovery and reconstitution. These may also include actions taken to reduce short- and long-term consequences, such as providing alternative sources of supply for critical goods and services. Mitigation actions and strategies are intended to reduce the consequences of an incident, whereas countermeasures are intended to reduce the probability that an event will occur or will reduce the probability of failure or significant damage if the event occurs.
9. ***Benefit/Cost Ratio*** *– Analytic technique used to compare alternatives according to the relative costs incurred and the relative benefits gained.*
10. ***Countermeasure*** – *An action, measure, or device intended to reduce an identified risk. A countermeasure can reduce any component of risk – threat [likelihood], vulnerability, or consequence.* Countermeasures may be directed at providing detection, deterrence, devaluation, delay, or response. These are often used in conjunction with other security actions to create a more comprehensive and holistic security system and may incorporate consequence mitigation (above), i.e.,
    - ***10.1 Detect*** – Use of security countermeasures to discover an adversary's intention to attack an asset or exploit an asset's vulnerability. Detection does not by itself seek to prevent an attack, but rather to recognize it and to trigger other types of security actions.
    - ***10.2 Deter*** – Actions to cause potential adversaries to perceive that the risk of failure is greater than that which they find acceptable, e.g., restricted access, vehicle checkpoints, enhanced police presence.
    - ***10.3 Devalue*** **–** Actions to reduce the adversary’s incentive by reducing the target’s value, e.g., developing redundancies and maintaining backup systems or key personnel.
    - ***10.4 Delay*** – The use of security countermeasures to slow the actions of an adversary to the point that a successful attack takes long enough to be interdicted or longer than expected or desired by the adversary.
    - ***10.5 Respond*** – The reactive use of emergency response capabilities to deal with the immediate consequences of an incident or attack.
11. ***Crisis Management*** – For the private sector, crisis management is that transition from normal business decision-making processes to a highly streamlined process aimed at containing the initiating event, maintaining essential operations and recovery of normal business conditions as quickly as possible.
12. ***Critical asset*** – See *asset.*
13. ***Decision Analysis*** *– The techniques, body of knowledge, and professional practice used to provide analytical support for making decisions through a formalized structure.*
14. ***Criticality*** **–** *Importance to a mission or function, or continuity of operations.*
15. ***Dependency*** – The reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to perform mission objectives.
16. ***Dependency hazard*** – A dependency the denial of which has the potential to disrupt the function of the asset, system, etc.

17. ***Deterrent –*** *Measure that discourages, complicates, or delays an adversary's action or occurrence by instilling fear, doubt, or anxiety.*
18. ***Emergency Response*** – A response to emergencies, including both natural disasters, *e.g.,* hurricanes, floods, earthquakes, etc., and human-induced events, *e.g.*, civil commotion, adversary attacks, etc., in order to protect lives and limit damage to property and impact on operations.
19. ***Enterprise Risk Management*** *– A comprehensive approach to risk management that engages organizational systems and processes together to improve the quality of decision-making for managing risks that may hinder an organization's ability to achieve its objectives.*
20. ***Event Tree (also called "Failure Tree")*** *– A graphical tool used to illustrate the range and probabilities of possible outcomes that arise from an initiating event.* A graphical "tree" construct to analyze the logical sequence of the occurrence of events in, or states of, a system following an initiating event (often called the "top event"); inductive analysis of events between the initiation of an incident and the terminal event is described as a branching tree, where each "branch" is assigned a probability of occurrence, while all potential branches at a node have occurrence probabilities that sum to unity (1.0). In vulnerability analysis, the product (?) of the probabilities of all branches on any sequential path which the incident follows results in the estimated consequences is the vulnerability estimate.
21. ***Event Tree Analysis*** – An inductive analysis process that utilizes a graphical "tree" constructed to analyze the logical sequence of the occurrence of events in, or states of, a system following an initiating event.
22. ***Facility*** – This term is commonly used to describe a fixed manufacturing or operating site or installation. However, the more general term "asset" as used in this document includes "facilities" as well as other types of assets. Assets may also be constituent elements of a facility.
23. ***Failure Mode*** – A way that failure can occur, described by the means or underlying physics by which element or component failures must occur to cause loss of the subsystem or system function.
24. ***Fault Tree –*** *A graphical tool used to illustrate the range, probability, and interaction of causal occurrences that lead to a final outcome.* A deductive logic diagram that depicts how a particular undesired event can occur as a logical combination of other undesired events.
25. ***First Due Zone –*** The primary service area for Emergency Medical Services (EMS) or Fire Suppression (FS).
26. ***Frequency*** *– A number of occurrences of an event per defined period of time or number of trials.* The rate of occurrence that is measured by the number of events per unit time, in this context, usually one year unless otherwise specified, or in a particular number of iterations, e.g., one defect per million products.
27. ***Game Theory –*** *A branch of applied mathematics that models interactions among agents where an agent's choice and subsequent success depend on the choices of other agents that are simultaneously acting to maximize their own results or minimize their losses.*
28. ***Hazard*** *– A natural or man-made source or cause of harm or difficulty. A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed. A hazard can be actual or potential.* Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.
29. ***Incident*** *– An occurrence, caused by either human action or natural phenomena that may cause harm and that may require action. Homeland security incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, law enforcement encounters*

and other occurrences requiring a mitigating [or emergency] response. Harm can include human casualties, destruction of property, adverse economic impact, and/or damage to natural resources.

30. ***Initiating Event*** – An event that appears at the beginning of a chain of events or a sequence of events, such as in an event tree or failure tree. In this context, generally includes malevolent events, accidents, natural hazards, failure of key dependencies or disruption of a hazardous neighboring site.
31. ***Insider Threat*** – One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.
32. ***Intent*** – *A state of mind or desire to achieve an objective. Adversary intent is the desire or design to conduct a type of attack or to attack a type of target. Adversary intent is one of two elements, along with adversary capability, that is commonly considered when estimating the likelihood of terrorist attacks and often refers to the likelihood that an adversary will execute a chosen course of action or attempt a particular type of attack.*
33. ***Likelihood*** – see **Probability**
34. ***Mitigation*** – *Ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident. Actions may be implemented prior to, during, or after an incident occurrence. Mitigation measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury. Technical measures can include the development of technologies that result in mitigation and can be used to support mitigation strategy.*
35. ***Model*** – *Approximation, representation, or idealization of selected aspects of the structure, behavior, operation, or other characteristics of a real-world process, concept, or system.*
36. ***Natural Hazard*** – *A source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena.* Incidents that are not human-caused are considered natural hazards.
37. ***Operational Risk*** – *Risk that has the potential to impede the successful execution of operations.*
38. ***Preparedness*** – A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during the incident response and recovery, including continuity of operations plans, continuity of government plans, and preparation of resources for rapid restoration of function.
39. ***Probability*** – A measure of the likelihood, degree of belief, frequency or chance that a particular event will occur in a period of time (usually one year) or number of iterations or trials. This is usually expressed quantitatively as a value between 0 and 1, a range of values between 0 and 1, a distribution (density function), or the mean of such a distribution. Probability can also be expressed in qualitative terms, *e.g.* low, moderate, or high, if there is a common understanding of the meaning of the qualitative terms.
40. ***Proximity Hazard*** – A threat that arises from being near another facility that is or could be hazardous.
41. ***Qualitative Risk Analysis*** – An appraisal of risk that uses linguistic terms and measurements to characterize the factors of risk. Whenever possible, qualitative analyses should be couched in terms of a consistent measure that allows comparisons between assets. Qualitative measures can be linguistic, *e.g.*, high, medium, low, or quantified, *e.g.*, a scale of 1 to 10).
42. ***Qualitative Risk Assessment Methodology*** – *Set of methods, principles, or rules for assessing risk based on non-numerical categories or levels.*

43. ***Quantitative Risk Assessment Methodology*** *– Set of methods, principles, or rules for assessing risk based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.*
44. ***Redundancy*** *– Additional or alternative systems, subsystems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, subsystem, asset, or process.*
45. ***Reference Threat*** – A particular event specified in terms of intensity or magnitude, mode and medium of delivery, to be used in a consistent fashion across numerous assets to facilitate direct comparisons. It is not to be confused with "design basis threat," which is the type and intensity of threat that a facility is designed to withstand.
46. ***Residual Risk*** – *risk that remains after risk management measures have been implemented.* The residual reflects the impact of threats that are not deterred, consequences that are not avoided and vulnerabilities that are not reduced through other countermeasures. The concept can also include the risks from threats that have not been included in a risk analysis.
47. ***Resilience*** – *The ability to adapt to changing conditions and prepare for, withstand and rapidly recover from disruption.* The ability of an asset or system to withstand an event or natural hazard without interruption of asset performance or system function or, if the function is interrupted, the ability to restore the function rapidly.
48. ***Resilience Management*** **–** The deliberate process of understanding resilience both as a function of loss of infrastructure components and the ability of the community to cope with the loss and recover in the shortest practical time. Resilience management includes the ability to model the interdependencies of infrastructure components and decide upon and implement actions that will increase the resilience of the community given the loss of a subset of infrastructure.
49. ***Respond*** – **See Countermeasures**
50. ***Return on Investment*** **–** The calculation of the value of risk reduction measures in the context of the cost of developing and implementing those measures.
51. ***Risk*** – *The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.* A function of consequences, hazard frequency, or likelihood, and vulnerability which, with point estimates, is the product of the terms. It is the expected value of the consequences of an initiating event weighted by the likelihood of the event's occurrence and the likelihood that the event will result in the consequences, given that it occurs. Risk can be based on identified events or event scenarios.
52. ***Risk Analysis*** – *A systematic examination of the components and characteristics of risk.* ***In*** *practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk.* Risk analysis provides the processes for identifying threats, hazards or hazard scenarios, event-probability estimation, vulnerability assessment and consequence estimation. The risk analysis process answers three basic questions: (1) What can go wrong and how it can happen? (2) What is the likelihood that it will go wrong? (3) What are the consequences if it does go wrong?
53. ***Risk Assessment*** – **see Risk Analysis**
54. ***Risk Indicator*** **–** *A measure that signals the potential for an unwanted outcome as determined by qualitative or quantitative analysis.*
55. ***Risk Management*** – *The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated*

costs and benefits of any actions taken. Effective risk management improves the quality of decision making. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to control risk. The deliberate, cyclical process of understanding risk based on a risk analysis and deciding upon, implementing and managing actions, e.g., security countermeasures or consequence mitigation features, to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by identifying, measuring, estimating and controlling risks to a level commensurate with an assigned or accepted value; monitoring and evaluating the effectiveness of implementation and operation of the selected options (with corrective actions as needed); and periodic repetition of the full risk management cycle.

56. ***Risk Reduction*** – *A decrease in risk through risk avoidance, risk control, risk transfer*, or risk management.
57. ***Scenario*** **–** *A hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate. A scenario can be created and used for the purposes of training, exercise, analysis, or modeling as well as for other purposes. A scenario that has occurred or is occurring is an incident.* A scenario defines a suite of circumstances of interest in a risk assessment. In the present context, a scenario includes at least a specific threat (man-made or natural hazard) to a specific asset, with the associated probabilities and consequences**.**
58. ***Sensitivity Analysis*** – *A process to determine how outputs of a methodology differ in response to variation of the inputs or conditions.*
59. ***Subject Matter Expert*** – An individual with in-depth knowledge in a specific area or field.
60. ***System*** – *Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.* A group of interacting, interrelated, or interdependent elements, such as people, property, materials, environment, and/or processes for a single purpose or defined set of purposes. The elements together form a complex whole that can be a physical structure, process, or procedure of some attributes of interest.
61. ***Target*** – *Asset, network, system or geographic area chosen by an adversary to be impacted by an attack..*
62. ***Terrorism*** **–** Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience. (Derived from Title 22 of the United States Code, Section 2656f(d)).
63. ***Terrorist*** – An agent of a sub-national group who uses premeditated, politically motivated violence against non-combatant targets, usually intended to influence an audience (derived from Title 22 of the United States Code, Section 2656f(d)).
64. ***Threat*** – *A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Threat as defined refers to an individual, entity, action, or occurrence; however, for the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that a hazard will manifest.*
65. ***Threat Analysis*** – The study or analysis of threats including adversary capability, intent and incidents that may be indicators of adversary activities.
66. ***Threat Likelihood*** **–** The probability that an undesirable event will occur. With natural hazards, the threat likelihood is the historical frequency of similar events unless there is a belief that the future will differ from the past. With malevolent threats, the likelihood is a function of available

intelligence, the objectives and capabilities of the adversary, and the attractiveness, symbolic or fear-inducing value of the asset as a target.

67. ***Unacceptable Risk*** *– Level of risk at which, given costs and benefits associated with further risk reduction measures, action is deemed to be warranted at a given point in time.*

68. ***Value of Statistical Life*** *– Amount of people are willing to pay to reduce risk so that on average one less person is expected to die from the risk. Most VSL estimates are based on studies of the wage compensation for occupational hazards or studies that elicit people's willingness to pay for mortality risk reduction directly.*

69. ***Vulnerability*** *– A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.* An inherent state of a system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary or impacted by a natural hazard to cause harm or damage. Such weaknesses can occur in building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings or operational and personnel practices. Vulnerability is expressed as the likelihood of an event's having the estimated consequences, given that the event occurs.

70. ***Vulnerability Analysis / Vulnerability Assessment*** *– A product or process of identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards. Vulnerability assessments can produce comparable estimates of vulnerabilities across a variety of hazards or assets, systems, or networks.* A systematic examination of the ability of an asset to withstand a specific threat or undesired event, including current security and emergency preparedness procedures and controls. A vulnerability assessment often suggests countermeasures, mitigation measures, and other security improvements.

71. ***Vulnerability Estimate*** – The probability, given the incident occurs, that a threat event will cause specifically estimated consequences.

72. ***Vulnerability Logic Diagram (VLD)*** – The flow of events from the time an adversary approaches the facility to the terminal event in which the attack is foiled or succeeds, considering the obstacles and countermeasures that must be surmounted, with each terminal event associated with a specific vulnerability "bin." This is frequently complemented by time estimates for each segment and compared with an estimate of the reaction time of a counterforce once the event has been detected. In many of the RAMCAP Sector-Specific Guidance documents, VLDs are prepared in advance as a heuristic to guide the team in making its analysis.

73. ***Worst Reasonable Case*** – An operating assumption for estimating consequence values that utilizes the most severe but reasonable and credible consequences for a specific hazard but does not combine unlikely coincidences. If an adversarial event, it directly reflects the assumption that an adversary is knowledgeable about the asset to be attacked and adaptive given emergent conditions.

ASME INNOVATIVE
TECHNOLOGIES
INSTITUTE, LLC