Standard Title Page - Report on Federally Funded Project

1. Report No.
FHWA/VTRC 02-CR5

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle
A Risk Assessment Methodology for Critical Transportation Infrastructure

5. Report Date
March 2002

6. Performing Organization Code

7. Author(s)
Y. Y. Haimes, J. H. Lambert, S. Kaplan, I. Pikus, and F. Leung

8. Performing Organization Report No.
VTRC 02-CR5

9. Performing Organization and Address

Virginia Transportation Research Council
530 Edgemont Road
Charlottesville, VA 22903

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
UPC 00056078-6940

12. Sponsoring Agencies' Name and Address

Virginia Department of Transportation	FHWA
1401 E. Broad Street	P.O. Box 10249
Richmond, VA 23219	Richmond, VA 23240

13. Type of Report and Period Covered
Final Contract Report

14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Infrastructure protection typifies a problem of risk assessment and management in a large-scale system. This study offers a methodological framework to identify, prioritize, assess, and manage risks. It includes the following major considerations: (1) a holistic approach to risk identification; (2) prioritization of a large number of risks or risk scenarios; (3) structured solicitation and effective integration of expert judgment into qualitative and quantitative analyses to supplement limited data availability; (4) extreme and catastrophic event analysis; and (5) use of multiobjective framework to evaluate management options (i.e., analyzing trade-offs among noncommensurate, conflicting objectives such as risk and cost). The methodology was illustrated using five case studies of selected transportation infrastructures in the Commonwealth of Virginia.

17 Key Words
Risk, assessment, protection, critical infrastructure

18. Distribution Statement
No restrictions. This document is available to the public through NTIS, Springfield, VA 22161.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 48	22. Price

Reproduction of completed page authorized

FINAL CONTRACT REPORT

A RISK ASSESSMENT METHODOLOGY FOR CRITICAL TRANSPORTATION INFRASTRUCTURE

Y. Y. Haimes, J. H. Lambert, S. Kaplan, I. Pikus, and F. Leung
Center for Risk Management of Engineering Systems
University of Virginia

Project Monitors
Wayne S. Ferguson, Virginia Transportation Research Council
Steve Mondul, Virginia Department of Transportation

Contract Research Sponsored by
Virginia Transportation Research Council

Virginia Research Transportation Council
(A Cooperative Organization Sponsored Jointly by the
Virginia Department of Transportation and
the University of Virginia)

Charlottesville, Virginia

March 2002
VTRC 02-CR5

NOTICE

The project that is the subject of this report was done under contract for the Virginia Department of Transportation, Virginia Transportation Research Council. The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the Virginia Department of Transportation, the Commonwealth Transportation Board, or the Federal Highway Administration. This report does not constitute a standard, specification, or regulation.

Each contract report is peer reviewed and accepted for publication by Research Council staff with expertise in related technical areas. Final editing and proofreading of the report are performed by the contractor.

PROJECT TEAM

Advisory Committee

Members of Virginia Governor's Domestic Preparedness Working Group

Michael M. Cline	Virginia Department of Emergency Management
Col. Michael J. Coleman	Virginia National Guard
George W. Foresman	Virginia Department of Emergency Services
Don Harrison	Office of Secretary of Public Safety, Virginia
Dr. Suzanne Jenkins	Virginia Department of Health
Troy H. Lapetina	Virginia Department of Fire Programs
Col. Gerald H. Massengill	Virginia State Police
Steve Mondul	Virginia Department of Transportation
Bruce C. Morris	Office of Secretary of Public Safety, Virginia
Peter C. Sherertz	Virginia Department of Health
LTC Darrel Stilwell	Virginia State Police
Donna Wells	Office of Secretary of Public Safety, Virginia

Steering Committee

Ralph Jones	Virginia Department of Emergency Management
Lt. Len Terry	Virginia State Police
Col. Michael J. Coleman	Virginia National Guard

Representatives from Virginia Department of Transportation (VDOT)

Steve Mondul	VDOT-Central Office
Perry Cogburn	VDOT-Central Office
J.R. Robinson	VDOT-Central Office
Dan Liston	VDOT-Central Office
Arthur N. Isley	VDOT-Central Office
Ken W. Wester	VDOT-Northern Virginia District
Robert W. Alexander	VDOT-Richmond District
Tom A. Hawthorne	VDOT-Richmond District
Jim Smith	VDOT-Richmond District
Ray Khoury	VDOT-Suffolk District
Bruce J. Wilkerson	VDOT-Suffolk District
Quinton D. Elliott	VDOT-Williamsburg Residency

Virginia Transportation Research Council (VTRC)
Wayne Ferguson

Center for Risk Management of Engineering Systems (CRMES)

Faculty
Yacov Y. Haimes
James H. Lambert
Stan Kaplan (Visiting Professor)
Irwin Pikus (Visiting Professor)

Students
Felicia Leung
Matthew Dombroski
Scott Crenshaw
Krista Moses
Zach Slagel
Jason Wynegar

TABLE OF CONTENTS

ABSTRACT

The U.S. transportation system is vulnerable and "open" to many risks, which can be categorized broadly as natural, accidental, and willful. The system traditionally has been protected against natural and accidental events but not against willful hazard. With the exception of civil aviation and the port system, few measures are currently in place in the transportation system to counter threats of terrorism (President's Commission on Critical Infrastructure Protection 1997; National Research Council 1999).

Infrastructure protection typifies a problem of risk assessment and management in a large-scale system. This study offers a methodological framework to identify, prioritize, assess, and manage risks. It includes the following major considerations: (1) a holistic approach to risk identification; (2) prioritization of a large number of risks or risk scenarios; (3) structured solicitation and effective integration of expert judgment into qualitative and quantitative analyses to supplement limited data availability; (4) extreme and catastrophic event analysis; and (5) use of multiobjective framework to evaluate management options (i.e., analyzing trade-offs among noncommensurate, conflicting objectives such as risk and cost). The methodology was illustrated using five case studies of selected transportation infrastructures in the Commonwealth of Virginia.

INTRODUCTION

The transportation system framework is highly complex, composed as it is of a wide array of infrastructures such as terminal facilities, travelways, transportation fleets, and information systems. There is no single organization responsible for controlling all of these infrastructures, most of which are owned by various private entities and state and local governments. It is inherently decentralized and open. Although these provide for easy and reliable access to its many users, as a result, the system is exposed to many risks.

Past incidents show that the transportation system is highly resilient to many risks. For example, the Loma Prieta earthquake in 1989 resulted in the collapse of a section of the Bay Bridge in San Francisco, making it completely inoperable for a period of time. During this period, affected commuters resorted to the use of the ferry service and the Bay Area Rapid Transit system (National Research Council 1999). There exist many redundancies in the system, preventing any large-scale impact of a failure event by providing alternative services in terms of routes or transportation modes. However, this is currently threatened by the growing trend toward integration and intermodalism in the transportation industry. This results in increased interconnectedness and interdependencies and thus compromising system redundancies. For instance, railroad companies are merging their assets and operations aiming to increase efficiency at the cost of reducing system redundancies (President's Commission on Critical Infrastructure Protection 1997). Moreover, the extensive application of information technology designed to improve efficiency and interconnectedness makes the system vulnerable to cyber attack, which has a potential to result in a more widespread damage than a physical attack.

Willful hazard poses a real and increasingly dangerous threat to the transportation system. A transportation infrastructure is an attractive target for intentional harmful attacks. It is highly visible, carries large number of commuters, and is easily accessed. Domestically, the proportion of attacks aimed against the transit systems (e.g., rails) has increased from 20% in 1991 to nearly 40% in 1998 (Federal Transit Administration 1999). Worldwide, transportation infrastructures had been the target of 58% of terrorist attacks in 1998 (FTA 2001b). This emerging threat warrants serious consideration since the US transportation systems traditionally have been protected against natural hazards and accidental failures, and not so much against willful hazards (NRC 1999).

On July 15, 1996, President Clinton issued Executive Order 13010 which included the transportation system among the nation's most critical infrastructures. The other critical infrastructures identified were: banking and finance, continuity of government, electrical power systems, emergency services, gas and oil storage/ transportation, telecommunication, transportation, and water supply systems. The following quotation from Executive Order 13010 helps illustrate the importance of these infrastructures.

> America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructure.

Presidential Decision Directive 63 was issued on May 28, 1998, and follows up on the recommendations from Executive Order 13010. It reinforces the vision of security for the critical infrastructures. The vision for transportation infrastructure assurance is stated as follows in the National Transportation Science and Technology Strategy (National Science and Technology Council (NSTC) 1999): "A transportation infrastructure that is secure from acts of terrorism and crime and that adapts rapidly to natural and intentional disruptions."

Unfortunately, with the exception of civil aviation and the port system, few measures are currently in place in the transportation system to counter threats of terrorism (PCCIP 1997; NRC 1999). And even with these institutionalized measures, not all willful hazards can be prevented. Dissident parties continually probe and attempt to overcome these measures with newer technology or back-to-basic strategies. The challenge of protecting critical infrastructures is not static; it is evolving and continuously adapting to the nature of emerging threats.

PURPOSE

The importance of protecting the nation's transportation infrastructure is readily apparent; the question, then, is how does one go about protecting them?

This study seeks to develop a comprehensive principle-based methodological framework able to identify and assess risks to Virginia's transportation infrastructures and to develop risk management options specifically to deal with the risks identified. Case studies were conducted for different types of transportation assets to demonstrate the use of the framework. These case studies are not presented in detail in this report to avoid discussion of any sensitive information; instead, a general example of the application of methodology is presented. The case studies may be obtained upon request, from the authors.

SCOPE AND LIMITATION

The term *transportation* denotes a wide array of travelways, which includes airports, airways, ports, inland waterways, railroads, and networks of highways. However, in this study, the terms *transportation*, *transportation system* and *transportation infrastructure* pertain to the surface transportation system and specifically to assets that fall within the control of the Virginia Department of Transportation (VDOT). These assets include:

1. The physical assets[1] consist of state-maintained highways, bridges, toll facilities, ferry services, rest areas and commuter parking facilities.
2. Cyber assets include all hardware, software, data used to support the information systems of VDOT.
3. Organizational assets include personnel, leadership value, standard operating procedures, and facilities used in business operations.

[1] List of VDOT physical assets can be found in their website at http://www.vdot.state.va.us/info/welcome.html.

The study focuses on five VDOT assets selected as case studies. Assets considered were limited to those within the Hampton Roads District[2]. These case study sites were selected by the project's steering committee as being among the most critical VDOT assets in the area. They compose a set of diverse assets in terms of size and functionality, thereby offering varied examples of VDOT transportation infrastructures. The case study sites[3] are as follows:

1. Traffic Management System (TMS) center
2. Major bridge
3. Major bridge/tunnels
4. Major interchange between interstates
5. Major interchange between a major highway and vital urban road.

METHODOLOGY

This study integrates a knowledge base gathered from a significant body of literature on infrastructure protection, risk assessment and management principles, and actual case studies, as described below.

1. *Review of literature on critical infrastructure protection.* This entails review of open source materials on different areas of infrastructure protection, including policies, current initiatives, threat assessments, security (physical and cyber), and emergency response among others. The scope is not limited to literature focused on surface transportation but generally covers all critical infrastructure protection materials. Similarities among infrastructures are exploited and adapted to this study, avoiding unnecessary duplications.

2. *Application of risk assessment and management principles.* The development of the framework for assessment of critical infrastructure is based on the principles of risk assessment and management principles. Current tools and methodologies were surveyed to ascertain what could be effectively applied to the problem of infrastructure protection.

3. *Conduct of case studies.* Sites were selected and studied. Contact persons for the sites were identified (see Appendix A). Understanding of the system, data collection, and judgment solicitation were accomplished through site visits, interviews, and electronic communications.

4. *Transfer of knowledge.* A workshop was conducted for VDOT personnel on risk assessment and management principles. Presentations were made by the research proponents to various steering committee and advisory committee meetings to report the results of the study.

[2] The transportation infrastructure in Hampton Roads, Virginia, is one of the most vital systems on the U.S. mid-Atlantic coast. It contains major east/west connectors for travelers in the mid-Atlantic region, the world's largest naval base, the Port of Virginia, and the second most complex system of underwater tunnels and bridges in the world. On top of the numerous physical structures that move traffic in the area, an advanced traffic system monitors the traffic flows and feeds information to commuters.

[3] General references were used to name case study sites throughout the report to protect sensitive information.

LITERATURE REVIEW

Critical infrastructure protection is among the U.S. Department of Transportation's (DOT) flagship initiatives (US DOT 1999b). The new emphasis on transportation security is reflected by the creation of the national security strategic goal in the DOT Strategic Plan in 1997 (US DOT 2000a). Prior to 1997, the security has been addressed under transportation safety.

Worldwide, transportation has been the target of 58% of terrorist attacks in 1998 (FTA 2001b). Domestically, the number of attacks against the transit systems (includes rail, bus, and ferry systems) has increased from 20% in 1991 to nearly 40% in 1998 (FTA 1999). Transportation infrastructures make for attractive targets since large number of people can be affected by a single attack, attacks and threats are immediately newsworthy, there is a high probability that the attacker will escape, and attacks can be associated with clearly identifiable national symbols, empowering attackers to embarrass or influence a particular government.

The effort to protect the transportation infrastructures is part of an overall effort in securing all critical infrastructures. Considerable knowledge could be gained from experiences of other agencies or documentation of past failure events and best practices. Some of these initiatives and resources in risk assessment for transportation infrastructure protection are as follows:

Information System Protection:

- U.S. DOT has issued a comprehensive set of guidelines for establishing an information system program (US DOT 1999a). This covers an overview of risk management processes, which include the following elements:
-
    1. Information Systems Security Plan
    2. Risk Assessment
    3. Continuity of Operations
    4. Certification and Accreditations
    5. Incident Handling
    6. Personnel Security
    7. Physical/Environmental Security
    8. Information System Security Awareness, Training and Education

  There are supplemental documents that detail each of these elements. These documents can be retrieved online at http://cio.ost.dot.gov/it_security/security_guidance.html. The documents can be easily adopted because the details and language are specifically applied to transportation information system.

- The Critical Infrastructure Assurance Office (CIAO) (2000) issued a guide to federal agencies for developing and implementing security policy. This document provided a survey, developed in association with Booz-Allen and Hamilton, Inc., for highlighting critical physical and cyber assets according to PDD 63.

- The National Security Telecommunications Advisory Committee (NSTAC) (1999) conducted an assessment of transportation information infrastructure at the national level. This study covers all subsystems of the transportation infrastructure, identifying risks derived from dependence on information technology and public networks. It raises the issue of growing vulnerabilities of information security, especially to insider attacks, resulting from trends on globalization, consolidation and intermodalism. To conduct the risk assessment, it used a methodology developed by the joint Government and NSTAC Network Security Information Exchanges.

Physical System Protection:

- A study by the U.S. General Accounting Office in 1988 looked into risks to the rail transit system (US GAO 1988). This methodology measured criticality of asset components in terms of impact on people and system operation and vulnerability to attack.

- All transit agencies are required to prepare and implement a System Security Program Plan (SSPP) by the FTA by January 1998 (Boyd and Sullivan 1997). The plan contains the activities necessary to provide security in the rail transit system, including counterterrorism programs. Continuing its efforts, the FTA is exploring innovative security measures for creating a safe environment for transit systems users. An example would be the development of advanced multi-sensor system using a network of urban chemical release detector (UCRD) to be installed in transit facilities (FTA 2001a).

- In 1998, the NRC established a diverse committee to examine the surface transportation system and suggest national responses for research and development strategies. The effort followed-up on a classified DOT vulnerability assessment study (US DOT 2001) of surface transportation in 1998. The committee emphasized the need to view security as part of a broader picture, i.e., to accomplish security goals in relation with other transportation goals (NRC 1999).

Formulating a comprehensive plan and response capability involves the efforts of multiple stakeholders—both private organizations and public agencies at the federal, state, and local levels. A significant initiative on information sharing was conducted in New Mexico (O'Neill 2000). The New Mexico Critical Infrastructure Assurance Council (NMCIAC) is the country's first all-volunteer, statewide organization devoted to critical infrastructure protection (CIP). This cooperative organization is a result of a summit meeting held in 1998 on CIP attended by various sectors including commerce, industry, state government, academia, military installations, and research laboratories, among others. They adapted a model of linking a state-regional-local information sharing and analysis center (ISAC) that is not subject to an upper-level coordinating agency, such as a federal agency. In particular, the summit established goals of rapid communication, private-public collaboration, identifying critical infrastructures, and triggering local response. The summit focused private organizations on establishing an ISAC. While other initiatives may be on the horizon in other states, NMCIAC currently serves as the model for other states to follow in effective infrastructure protection.

There is an extensive body of work on CIP by many agencies, which includes vulnerability assessments, documentation of past failure events, and best practices. What was discussed previously constitutes only a small sample of the available materials on infrastructure protection. However, information gathering, coordination, and sharing pose a major challenge for all agencies involved in the protection of critical infrastructure. There is no centralized point for collecting and processing this information. The wide array of federal programs and available materials can be confusing, presenting disjointedness efforts in CIP, which often result in overlapping assessments and programs (Freedberg 2001).

As part of an initial effort to consolidate information, an html-based navigational tool was developed that links a user to a collection of references on different areas of critical infrastructure protection. The html-based navigational tool is available in compact disc from the authors. The areas are as follows: (1) UVaCRMES, referring to materials by the Center for Risk Management of Engineering Systems; (2) Organization, containing a list of agencies (federal, state/local, and private) that are involved in infrastructure protection; (3) Critical Infrastructures, referring to materials with general applicability to any critical infrastructure such as EO 13010 and its amendments, PDD 63, presidential committee reports, and other similar materials; (4) Security and Hardening; (5) Information Security; (6) Information Assurance; (7) Emergency Response; (8)Research and Development; (9) Terrorism; and (10) Cases/Case Studies/Best Practices. Figure 1 shows the tool's interface. This system is continuously being updated.

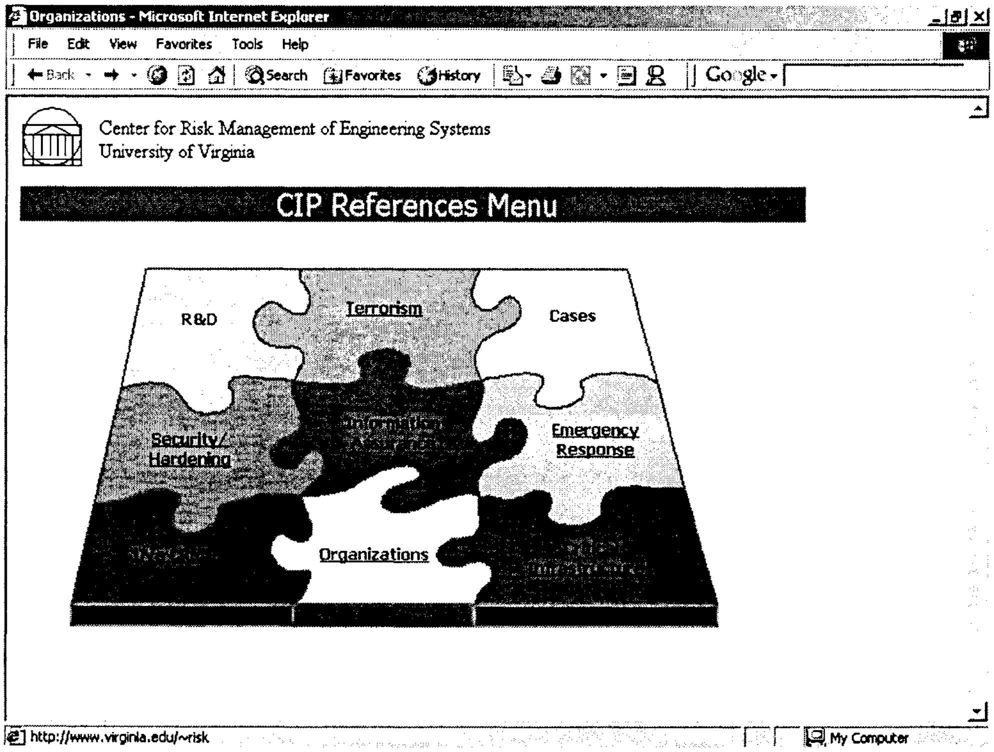


Figure 1. Html-based navigational tool linking to a collection of CIP references

RISK ASSESSMENT METHODOLOGY

Any risk analysis and management endeavor adheres to the same basic principles captured by six questions. In risk assessment, we ask: (1) What can go wrong?, (2) What is the likelihood that it would go wrong?, and (3) What are the consequences? (Kaplan and Garrick 1981). Risk management, on the other hand, answers the following three questions: (4) What can be done and what options are available?, (5) What are their associated trade-offs in terms of all costs, benefits, and risks?, and (6) What are the impacts of current management decisions on future options? (Haimes 1991, 1998). Risk assessment performs risk identification, quantification, and measurement while risk management involves the creative identification and meaningful evaluation of risk mitigation options to address the risks effectively.

Overview of Risk Filtering, Ranking, and Management Methodology

Haimes, Kaplan, and Lambert (2002) offer a methodological framework that identifies, prioritizes, assesses and manages risks to complex, large-scale systems. The risk filtering, ranking, and management (RFRM) methodology captures all six questions of risk assessment and management, thereby ensuring a comprehensive risk analysis process. The RFRM method involves eight phases:

Phase I. Scenario Identification through Hierarchical Holographic Modeling
Phase II. Scenario Filtering
Phase III. Bi-Criteria Filtering and Ranking
Phase IV. Multi-Criteria Evaluation
Phase V. Quantitative Ranking
Phase VI. Risk Management
Phase VII. Safeguarding Against Missing Critical Items
Phase VIII. Operational Feedback

It builds on the hierarchical holographic modeling to identify risks. It then filters and ranks the many sources of risks, enabling decision makers to focus on the most critical. The prioritized risks are further evaluated in the risk management phase, which offers options and strategies of actions. Finally, it incorporates a process for reviewing and improving the method.

Mapping the RFRM Method to other Risk Assessment Methodologies Applied to Transportation

The RFRM methodology is compared to other risk assessment methodologies employed by key agencies in identifying risks to critical infrastructures. Three methodologies are presented:

1. DOT risk assessment process for information system protection (US DOT 1999a)
2. The National Security Information Exchanges (NSIE) methodology used to assess risks to security of public networks (NSTAC 1999)

3. Vulnerability/Impact Assessment Methodology employed by DOT's Research and Special Programs Administration and Office of Intelligence and Security in surface transportation assessment (US DOT 2001).

Table 1 shows the mapping of the RFRM method against these risk assessment methodologies. Except for the evaluation of likelihood of occurrence of a risk scenario, all four methodologies map well against each other. There are inherent challenges in determining the likelihood estimates for various risk scenarios; among them is a lack of data. Aside from the difficulties in accessing information through various databases, there is also the question of the lack of it. Many risk scenarios considered are for predicted events and thus have not occurred yet. There is no historical data to form a basis for the computation of probabilities.

In the RFRM method, the process of determining likelihood, even for many scenarios, was facilitated with the initial qualitative approach using mainly expert judgment in the initial filtering. Experts, in this case, VDOT contact persons, were asked to assess the likelihood of occurrence of a specific scenario based on their knowledge and experience. This approach was continued even for quantitative estimate of likelihood, supplementing the lack of data on many risk scenarios. There are many issues involved in the proper use of expert judgment. Kaplan (1992) and Meyer and Booker (1991) provide guidelines.

Detailed Discussion of the RFRM Eight Phases

Phase I: Scenario Identification

Hierarchical Holographic Modeling

When modeling large-scale, complex systems such as the transportation system, more than one mathematical or conceptual model is likely to emerge. For instance, the transportation infrastructure can be modeled according to modal travelways, in which case the decomposition would be in terms of land, rail, water, and air. Other commonly used modeling perspectives are spatial and functional. For example, VDOT uses regional decompositions based on geographic boundaries to define responsibilities for highway maintenance and construction (VDOT 2000). Although these regional decompositions will likely be adopted for planning, other perspectives can be employed such as temporal (e.g., short, medium and long term) or functional (e.g., operations, maintenance, R&D). The ability to view the system exhaustively from many perspectives, instead of being limited to one, facilitates the identification of a more comprehensive set of sources of risk. Hierarchical holographic modeling (Haimes 1981) allows simultaneous modeling of these multiple perspectives.

The HHM can be described as a diagram that categorizes multiple perspectives of a system capturing various sources of risk to the system. The objective is to identify all possible sources of risks. An HHM results from a complete specification of the underlying system into a hierarchy of subsystems, which together display a holistic view of the large-scale system.

Table 1. Mapping of RFRM to other risk assessment methodologies

6 Questions	RFRM	US DOT (1999a)	NSTAC (1999)	US DOT (2001)
1. What can go wrong?	Phase I Scenario Identification	– Identifying Assets; – Identifying Threats	– Threat Identification	– Asset Identification – Threat Identification – Formulation of Scenarios
	Phases II Decision maker Filtering	**	**	**
2. What is the likelihood? 3. What are the consequences?	Prioritize III Qualitative Filtering	– Loss Categories – Threat-Loss Pairing	▨	– Key Asset Selection – Assessment of Impacts
	Phase IV Multi-criteria Evaluation	– Identifying Vulnerabilities	– Vulnerability Identification	– Vulnerability Assessment* – Vulnerability / Impact Rating
	Phase V Quantitative Ranking	▨	▨	▨
4. What can be done? 5. What are the trade-offs? 6. What are the impacts to future options?	Phase VI Risk Management	– Identifying Existing Control – Determining Cost-Effective Safeguards	– Deterrents (to threats) and protection measure (to vulnerabilities)	– Identification of potential counter-measures
	Phase VII-VIII Feedback and Improvement	– Reporting Results	**	**

* *The DOT vulnerability assessment measured a different likelihood value from that of RFRM.RFRM measures likelihood of occurrence of risk scenario, whereas DOT's quantification is on determining the likelihood of success of risk scenario (implying the likelihood of resulting consequence) given that the risk scenario occurs.** There is no specific step defined in the methodology; however, the task is conducted implicitly and therefore is mapped to the corresponding RFRM phase*

Risk Scenario Generation

From the HHM, a list of risk scenarios (i.e., a specific failure event in the system) is generated through decomposition. This process commonly leads to the identification of a significant number of risk scenarios and it is impractical to address each one. Consequently, there is a need to prioritize these scenarios. The next phases of the process (Phases II to IV) filter these scenarios, identifying the most critical ones.

Phase II: Scenario Filtering Based on Scope, Temporal Domain, and Level of Decision Making

Phase II limits the set of risks according to the interests and responsibilities of decision maker(s). Since not all of the scenarios are of immediate and concurrent concern for the decision maker(s), these are filtered based on scope, temporal domain, or level of decision-making.

A sample classification of decision makers among VDOT personnel based on these factors is given in Table 2. The classification could facilitate the filtering process by presenting an initial set of relevant risk scenarios which could be validated by the decision maker. *Note that classifying the VDOT decision-making structure is not a trivial task.* The decision-making process of VDOT and the associated responsibilities of its personnel should be studied in depth in order to make a meaningful and relevant classification.

Table 2. Example classification of decision makers for risk filtering

Levels of Decisions	Description	Example of Decision Body in Transportation	Example of Relevant Risk Sources
(a) Strategic	Decisions concerns general direction, long-term goals; Relies on collective, multidisciplinary perspective on which to base decision	Transportation Board, Secretary of Transportation, Commissioner, Functional Heads	Terrorism Environmental impact Interdependencies
(b) Operational	This supports strategic decisions involving decisions that are at medium range, moderate consequences.	Functional Heads, District Administrators, District personnel, Residency personnel	Resource allocation
(c) Tactical	Everyday decisions; structured decisions. Impact is immediate, short-term, minimal consequence.	District personnel, Residency Personnel	Daily maintenance Local snow removal

Phase III: Bi-Criteria Filtering and Ranking

Phase III uses likelihood and consequences to filter risks. Each risk scenario is characterized using qualitative severity-scales of consequence and likelihood. Severity of risk scenario is assessed using both consequence and likelihood measures.

Risk Impact/Consequence

A listing of the possible qualitative severity-scale consequences is given in Table 3. More aspects of risk impact can possibly be added to the list such as economic and social impact of risk.

Table 3. Qualititative risk consequences (adapted from U.S. Department of Energy (DOE) Risk-Based Priority Setting Process (US DOE 1998))

A. **Safety and Health**
- A1. Catastrophic level in terms of number of deaths
- A2. Moderate number of deaths
- A3. Small number of deaths
- A4. Excessive injury
- A5. Moderate to low injury

B. **Direct Functional (Mission) Impact**
- B1. 100% inoperability – long term
- B2. 100% inoperability – moderate to short term
- B3. Loss of capability with compromise of operation
- B4. Loss of capability with no effect on operation
- B5. No effect

C. **Functional (Mission) Impact to Interdependent Systems**
- C1. 100% inoperability – long term
- C2. 100% inoperability – moderate to short term
- C3. Loss of capability with compromise of operation
- C4. Loss of capability with no effect on operation
- C5. No effect

D. **Environmental Impact**
- D1. Catastrophic damage to the environment
- D2. Significant damage to environment
- D3. Moderate to minor damage (localized and short-term effects)

Likelihood

An ordinal scale of likelihood is used to assess how often a risk scenario occurs (as in cases of occurring threat) or the potential for its occurrence (as in cases of emerging threats). At this phase, subjective language is used to describe the likelihood of occurrence of a risk scenario, relying on expert judgment or assessment. The scale is given as *unlikely*, *seldom*, *occasional*, *likely*, and *frequent*.

Risk Severity

The filtered risk scenarios are then evaluated to a risk severity level, based on the dual of consequence and likelihood. Risk severity is classified into *extremely high*, *high*, *moderate*, and *low* level of severity. Table 4 gives a brief description of these severity levels.

Table 4. Definition of risk severity level

Risk Severity Level	Consequence-Likelihood Combination
Extremely High Risk	Characterized by high likelihood and severe consequences; Cells in the upper RH side of the matrix would typically fall in this category.
High Risk	Characterized by HIGH consequences and MODERATE to HIGH likelihood.
Moderate Risk	Characterized by a combination of: HIGH consequence – LOW likelihood; or MOD consequence – MODERATE to LOW likelihood; or LOW consequence – HIGH likelihood
Low Risk	Characterized by low consequences, with little effect of likelihood. Even though the likelihood is MOD HIGH but if consequence is relatively low, then the risk severity can be categorized as low.

Risk Matrix

Each risk scenario is mapped in the severity matrix, adapted from Military Standard (MIL-STD) 882, US DoD (Roland and Moriarty 1990) shown in Figure 2. Filtering is accomplished based on the severity scale. Usually, the threshold is set such that scenarios with *low* and *moderate* severity levels are set aside for later consideration, while giving attention to those with *high* and *extremely high* risk severity.

Effect	Likelihood				
	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of life	**EH**	**EH**	**EH**	**EH**	**EH**
B. 100% inoperability	**H**	**H**	**H**	**H**	**EH**
C. Partial inoperability	**M**	**M**	**M**	**H**	**H**
D. Partial failure but no effect on operation	**L**	**L**	**M**	**M**	**M**
E. No effect	**L**	**L**	**L**	**L**	**L**

EH: Extremely high risk, **H**: High risk, **M**: Moderate risk, **L**: Low risk

Figure 2. Sample Risk severity matrix for RFRM Phase III

Phase IV: Multi-Criteria Evaluation

Defensive properties of the system are classified in terms of redundancy, robustness and resilience (3Rs) defined as follows:

1. Redundancy refers to ability of extra components of a system to assume the function of failed components.
2. Rebustness refers to insensitivity of system performance to external stresses.
3. Resilience refers to ability of a system to recover following a failure.

Specific criteria are defined for each of these system properties. Eleven criteria are defined in Table 5. The mapping of these 11 criteria to the 3Rs is shown in Figure 3. Each scenario is evaluated as *high*, *medium*, or *low* against these criteria.

This phase does not filter risk scenarios but aid in the audit of system's weaknesses in terms of the 3Rs. This evaluation is significant in developing options for managing risks (Phase VI). System criteria that are easily compromised by a risk scenario should be addressed.

Table 5. Eleven criteria of the defenses of the system against risk (Haimes, Kaplan, and Lambert 2002)

Criteria	Definition
1. Undetectability	refers to the components and redundancy of models by which the initial events of a scenario can be discovered before harm occurs to the system
2. Uncontrollability	refers to the redundancy of controlling models by which it is possible to take action or make an adjustment to prevent harm to the system
3. Multiple paths to failure	indicates that there are multiple and possibly unknown ways for the events of a scenario to harm the system, such as circumventing safety devices
4. Irreversibility	indicates a scenario in which the adverse condition cannot be returned to the initial, operational (pre-event) condition
5. Duration of effects	indicates a scenario which would have a long duration of adverse consequences
6. Cascading effects	indicates a scenario where the effects of an adverse condition readily propagate to other systems or subsystems, i.e., cannot be contained
7. Operating environment	indicates a scenario that results from external stressors

Table 5 *(cont'd)*. Eleven criteria of the defenses of the system against risk

Criteria	Definition
8. Wear and tear	indicates a scenario that results from use, leading to degraded performance
9. Hardware, Software, Human, and Organizational (HW/SW/HU/OR) interfaces	indicates a scenario in which the adverse outcome is sensitive to interfaces among diverse subsystems (e.g., human and hardware)
10. Complexity/emergent behaviors	indicates a scenario in which there is a potential for system-level behaviors that are not anticipated from a knowledge of components and the laws of their interactions
11. Design immaturity	indicates a scenario in which the adverse conditions are related to newness of a design or other lack of concept proof

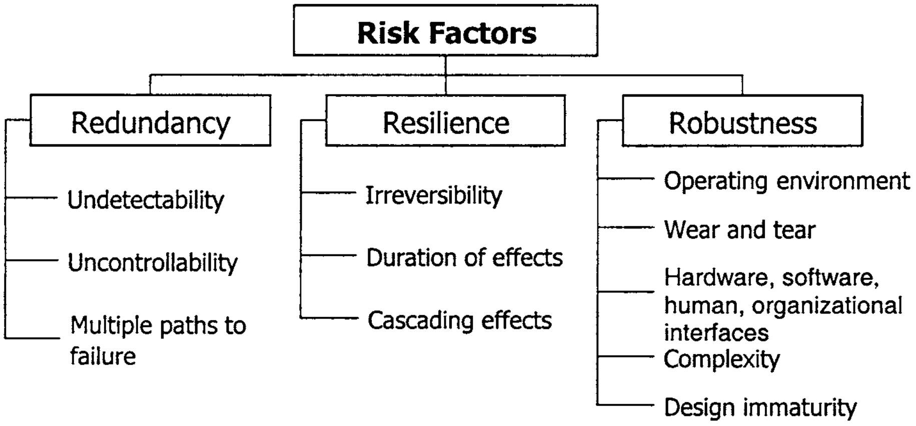


Figure 3. Eleven criteria of the defenses of the system against a scenario, used in RFRM Phase IV

Phase V: Quantitative Ranking

Phase V uses the diagram similar to Figure 2, except that quantitative probabilities are used instead of qualitative probabilities (as shown in Figure 4). Calculating quantitative likelihoods is accomplished by using available evidences, either in terms of historical data or expert judgment.

The remaining sources of risk are applied to this scale and are ranked in terms of severity as in Phase III. Upon completion of this phase, a manageable number of risks should result for further consideration.

Effect	Likelihood				
	$0 < P < .01$	$.01 \le Pr < .02$	$.02 \le Pr < .10$	$.10 \le Pr < .50$	$.50 \le Pr < 1$
A. Loss of life	**EH**	**EH**	**EH**	**EH**	**EH**
B. 100% inoperability	**H**	**H**	**H**	**H**	**EH**
C. Partial inoperability	**M**	**M**	**M**	**H**	**H**
D. Partial failure but no effect on operation	**L**	**L**	**M**	**M**	**M**
E. No effect	**L**	**L**	**L**	**L**	**L**

EH: Extremely high risk, **H**: High risk, **M**: Moderate risk, **L**: Low risk

Figure 4. Sample Risk severity matrix with cardinal likelihood scale used in Phase V

Phase VI: Risk Management

Management options that ask the questions, what can be done, what should be done, and what are the trade-offs of the options, are applied to the final set of most critical risk scenarios. Looking at the numerous possibilities for managing the risks, one arrives at a set of Pareto optimal options. Various quantitative tools are used to evaluate the impact of options and trade-offs among multiple objectives.

Phase VII: Safeguards Against Missing Critical Items

One must remember that if management options are implemented, the system will be altered. Phase VII addresses the potential problems associated with the change of state in the system associated with the implementation of management options by reviewing inter/intra-dependencies of success scenarios and failures, evaluating the risk policies against the previously filtered out sources of risk, and revising the risk management options developed in Phase VI. Phase VII analysis provides insight into a number of alternative management options that might have otherwise been overlooked. Phase VII reviews the entire process and assesses if risks were overlooked.

Phase VIII: Operational Feedback

Phase VIII forces the analyst to assess the methodology in terms of the changing and dynamic nature of risk assessment and management. One must be aware that the methodology should be tailored to fit the individual assessment and that evolving sources of risk will develop during the analysis. Two points to make are that the HHM is never finished and there will always be new sources of risk as the project develops, and that one should be cognizant to all benefits, costs, revenues, and risks to human health and the environment. Essentially, one should be prepared to incorporate alternate and extra means of analysis into the methodology to maintain a complete model.

Figure 5 summarizes the discussion in a flowchart, mapping in each phase example inputs and tools that could be used. This could serve as a roadmap for implementing the methodology.

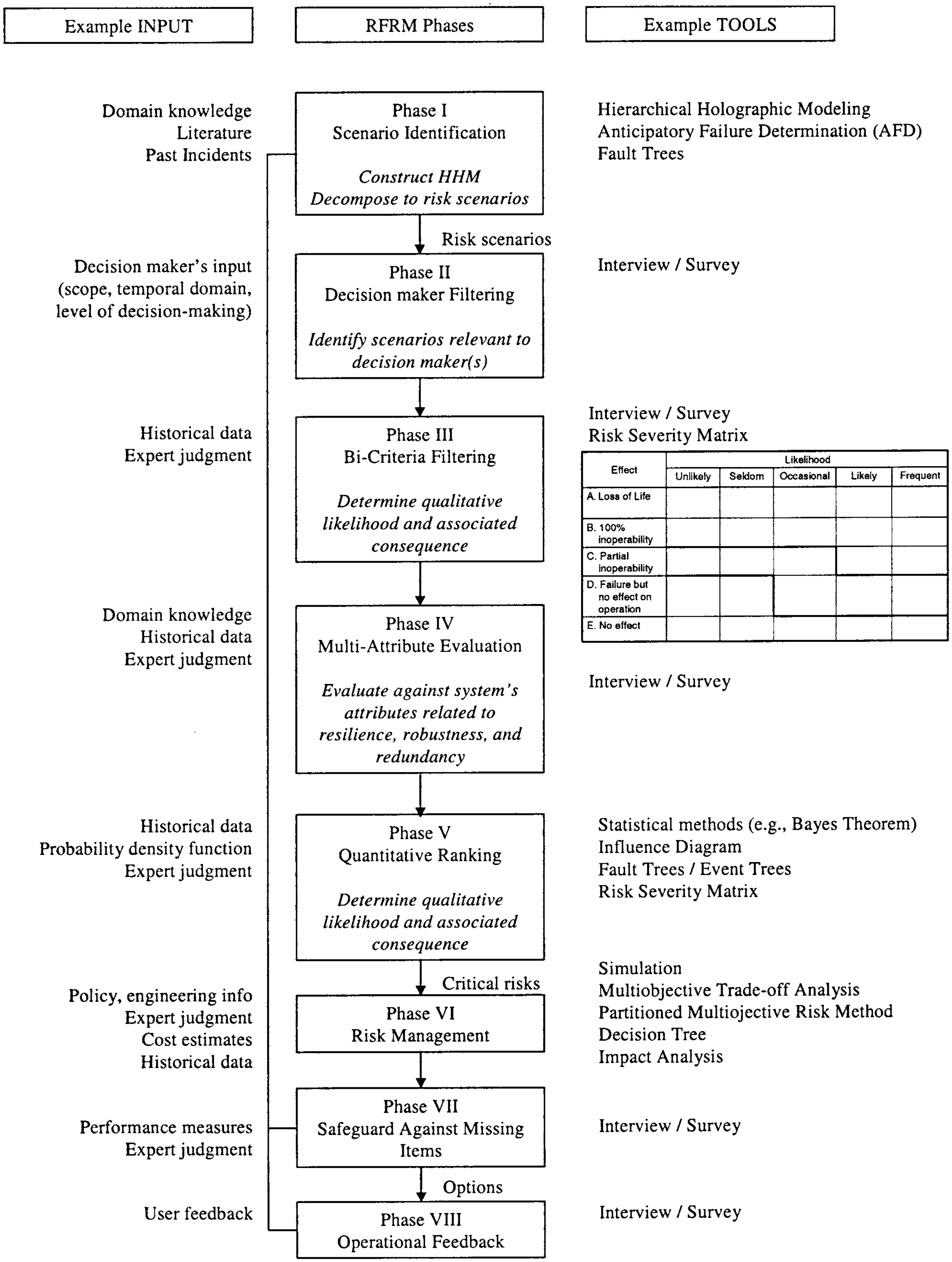
Example Application of Risk Filtering, Ranking and Management (RFRM) Method to Risk Assessment of Transportation Infrastructure

To avoid discussing sensitive information related to risks to these sites, a general discussion is presented, illustrating an example of the methodology implementation to a transportation infrastructure.

Phase I: Scenario Identification

The initial challenge in risk analysis is risk identification. The HHM answers the question, "What can go wrong?" To differentiate willful hazard from natural, this question is asked from two different aspects: "How can the system fail?" and "How can one make the system fail?" The latter question points to scenarios involving willful threats to the system such as terrorism. An HHM for the surface transportation system was developed and it includes eight main perspectives (called *risk headtopics*):

1. Willful - This covers intentional man-made threats to the system, primarily, acts of terrorism targeting cyber assets, physical assets, and system users.
2. Natural - This pertains to natural hazard. It is categorized as seasonal and extreme event. Since seasonal hazards are expected, these hazards allow for more readiness than do extreme events such as a 500-year flood or severe ice storms.
3. Structural - This pertains to hazards that threaten the structural aspect of the asset, including untested new technology (e.g., new materials or construction technology), deterioration (wear and tear), and flawed design.
4. Environmental - This covers hazards that could have significant impact on the environment such as accidents involving hazardous materials, pollution levels, and environmental alterations due to construction.
5. Supervisory Control and Data Acquisition (SCADA) - This pertains to hazards to SCADA systems which include failure of hardware, software, remote control, modeling, feedback systems, and signals.
6. Interdependencies - This pertains to hazards to systems that are dependent on transportation (people, businesses, other agencies), and systems that transportation depends upon in order to function (power, communications, supplies).
7. Organizational - This pertains to hazards to the different aspects of the VDOT organization that threaten its services and effectiveness. These include failure of leadership, management, communication, employees, and policies/regulation.
8. Usage – This pertains to hazards related to use of an asset. These include problem in system capacity, flow design, and regulations.



Effect	Likelihood				
	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of Life					
B. 100% inoperability					
C. Partial inoperability					
D. Failure but no effect on operation					
E. No effect					

Figure 5. Flowchart of RFRM phases with example inputs and tools

These headtopics constitute some of the major perspectives of the risks ro surface transportation system. Although not complete, they provide an adequate starting point for identifying a wide array of possible, significant risk scenarios. The HHM is shown in Figure 6.

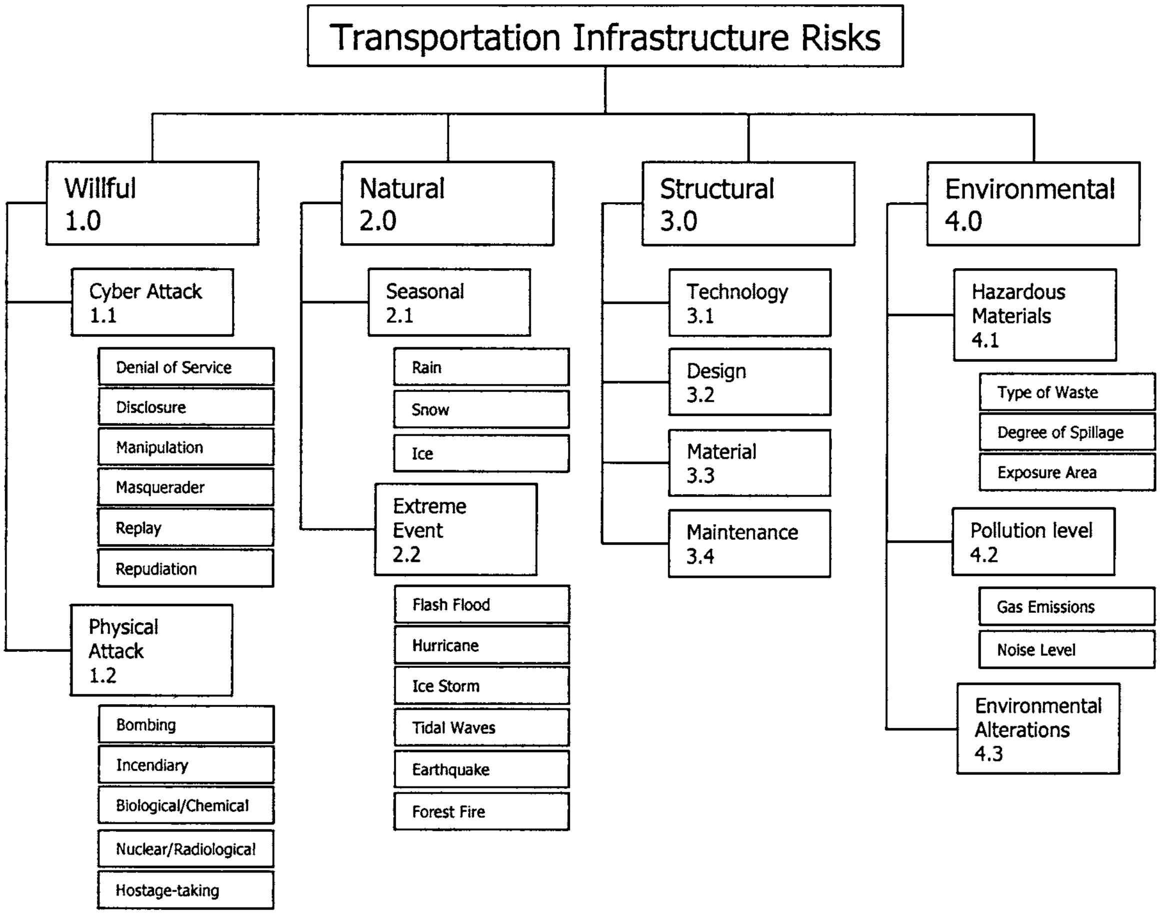
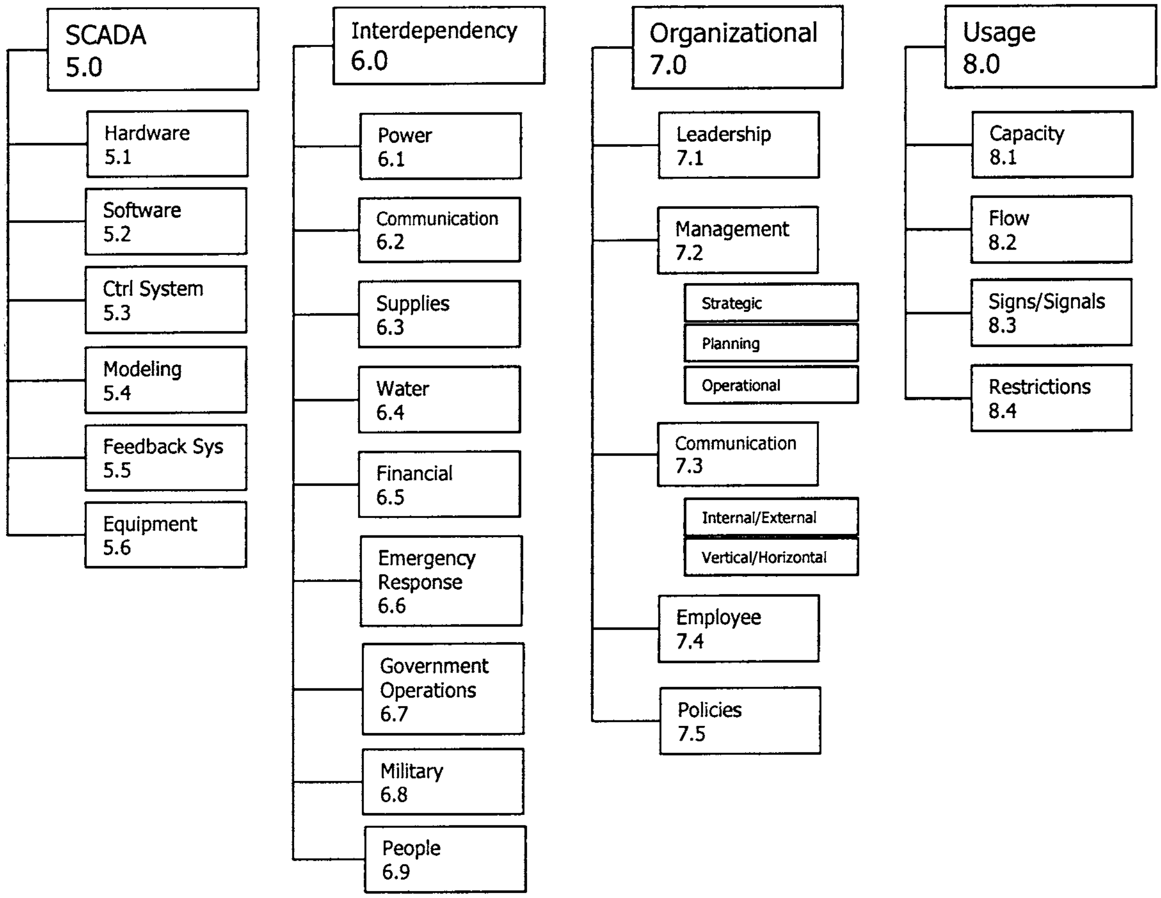


Figure 6. Partial hierarchical holographic model for transportation infrastructure

(a) HHM Risk headtopics including Willful, Natural, Structural, Environmental



(b) HHM Risk headtopics including SCADA, Interdependency, Organizational, and Usage

Risk scenarios are generated through decomposition of the HHM as illustrated in Figure 7. A risk scenario defines a specific failure event in the system. At this level, one can easily specify the associated likelihood and consequences to that event, thereby facilitating succeeding phases of analysis. Table 6 outlines the damage and duration of effect of four of these scenarios, namely (1) major bombing of road structure, (2) major bombing on the road, (3) major bombing of roadside facility, and (4) minor bombing of small roadside structure.

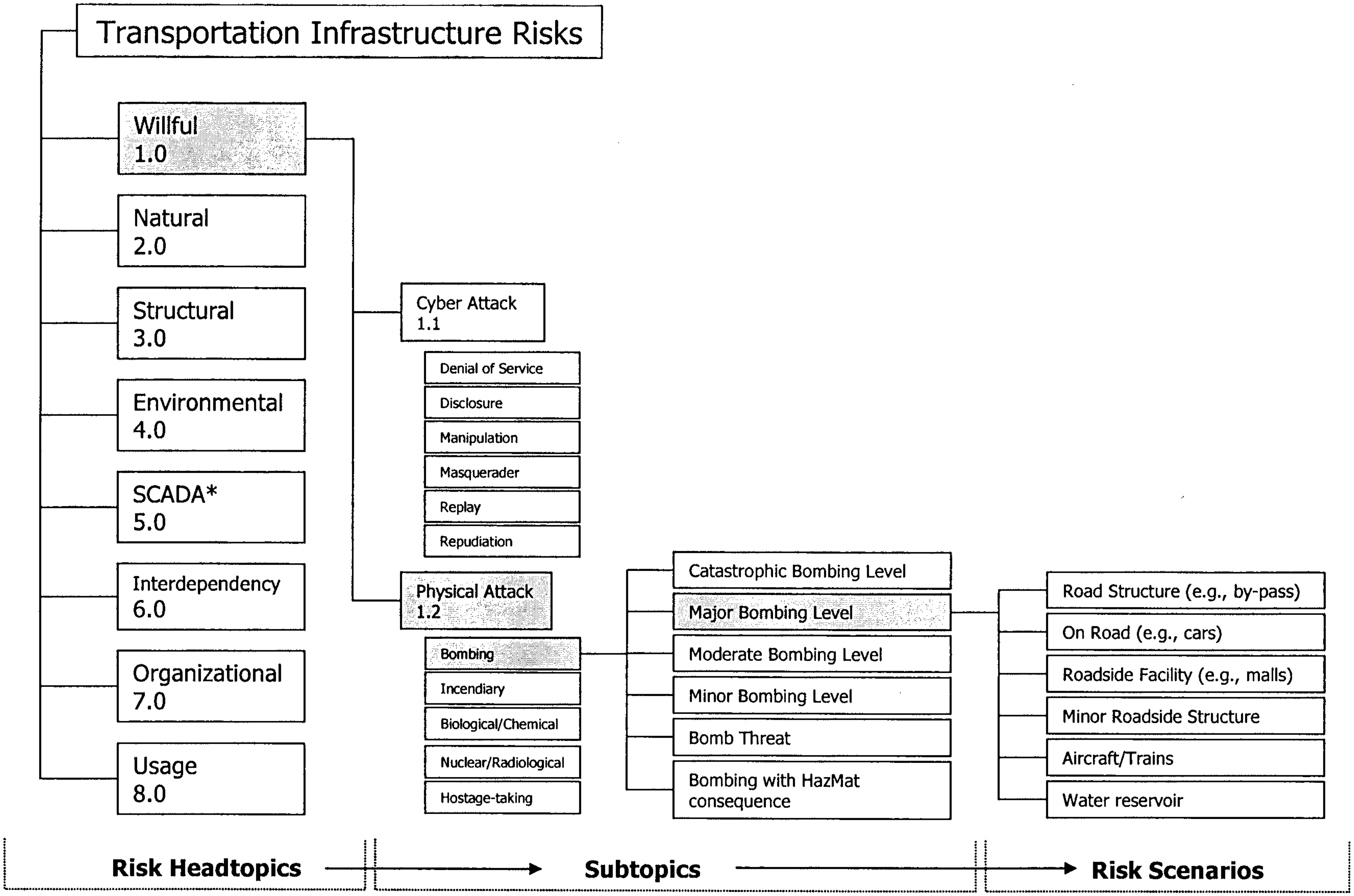


Figure 7. Example decomposition of HHM headtopics to generate risk scenarios

Table 6. Sample of risk scenarios of physical attack (HHM subtopic 1.2) by bombing:

Scenario	Target	Consequence (primary, secondary)	Duration
(1) Major bombing of road structure	by-pass structure	deaths & injuries, severe damage to structure, road closure, public panic	medium to long
(2) Major bombing on road	cars, road	deaths & injuries, damage to structure, road closure, secondary blasts, loss of power and communication, public panic	medium to long
(3) Major bombing of roadside facilities	buildings	deaths & injuries, collapse of structure, partial to complete road closure	Short - medium
(4) Minor bombing of small roadside structure	road signs, light	deaths & injuries, severe damage to roadside structure, partial road closure or traffic build-up	Short

Noting the two extreme cases in Table 6, namely (1) major bombing of road structure and (4) minor bombing of small roadside structure:

- A bombing that destroys a significant part of an interchange would likely cause100% (complete) inoperability of that interchange immediately, and massive casualties. There is no intermediate damage stage; i.e., the system functionality degrades immediately to inoperable, making response time critical. Moreover, the duration of damage would be medium to long term due to the long cleanup, recovery, and reconstruction operations involved after such an attack. There could also be unpredictable secondary effects such as blasts from adjacent gas or electrical utilities, which in turn could cause loss of power and communication services to others.
- A minor bombing that targets small structures along the roadway, such as signposts or public phone booths, would have a different impact on the system. It could cause partial closure of lanes for a short period of time, causing heavier traffic than usual. However, it would not entail 100% inoperability or any long-term consequence to the use of the route.

Specifying risk scenarios creates several distinctive events from a single risk subtopic in terms of impact and likelihood. However, the process commonly leads to the identification of a significant number of risk scenarios, and it is impractical to address each one. Consequently, there is a need to prioritize, and a systematic, principle-based filtering of the scenarios should be conducted.

Phase II: Filtering Based on Decision maker's Scope, Temporal Domain, Level of Decisionmaking

Not all risk scenarios generated in Phase I are relevant and significant to all decision makers. For instance, a high-level official will not be concerned with daily maintenance scheduling problem or "fender bender" accidents.

The scenarios are filtered based on three criteria: (1) decision making scope, (2) temporal domain, and (3) level of decision making. The intention is to generate risk scenarios that are of concern to specific decision maker(s) for whom the assessment is being conducted. For example, assuming risk scenarios that will be of concern at a strategic level of decision making are characterized by:

1. consequences with high social impact (economic and safety),
2. consequences with high damage costs to VDOT and other agencies (asset damage costs, emergency response and recovery costs), and
3. a need for multi-discipline, multi-agency collaboration in response and recovery operations.

The risk scenarios are reduced using these three characteristics. Applying these three characteristics, except for those scenarios relating to leadership, management and long-term maintenance, most of these scenarios associated with VDOT's organizational aspects is filtered out.

Phase III: Bi-Criteria Filtering Using Ordinal Severity Matrix

The remaining subset of risk scenarios is filtered further using a risk threshold criterion based on severity of risk. The severity of the risk scenarios is determined by the joint effect of consequence and likelihood. Severity level is measured in terms of *low*, *moderate*, *high,* and *extremely high.* Risk scenarios with *low* and *moderate* severities can be set aside for later consideration while giving attention to those with *high* and *extremely high* risk severity.

Each risk scenario is characterized in terms of qualitative severity-scales of consequence and likelihood and is mapped in the severity matrix. To illustrate the use of the severity matrix, consider six risk scenarios (see Table 7 and Figure 8):

Table 7. Example risk scenarios used in RFRM Phase III filtering

Headtopic	Risk Scenario	Likelihood	Impact
Willful	(a) Major car bombing	Unlikely	Loss of life
Natural	(b) Excessive rain causing road accidents	Occasional	Loss of life
Environmental	(c) Minor accident involving HazMat vehicle, no spill	Seldom	Partial inoperability
Environmental	(d) Major rail accident near interstate	Unlikely	Loss of life
Interdependencies	(e) Bombing of power facility causing failure of traffic signals	Unlikely	Partial failure

The analyst sets a filtering threshold. In this case, the filter eliminates *moderate-* and *low-risk* severity scenarios. Thus the analysis continues with only *extremely high-risk* and *high-risk* severity scenarios. The heavy black line cutting across the matrix defines the filtering threshold, filtering out scenarios (c) minor accident involving hazardous material vehicle (no spill), and (e) bombing of power facility causing failure of traffic signals.

Effect	Likelihood				
	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of life	**EH** (a) bombing (d) rail accident	**EH**	**EH** (b) excessive rain	**EH**	**EH**
B. 100% inoperability	**H**	**H**	**H**	**H**	**EH**
C. Partial inoperability	**M**	**M** (c) minor hazmat accident	**M**	**H**	**H**
D. Partial failure but no effect on operation	**L** (e) bombing of power facility	**L**	**M**	**M**	**M**
E. No effect	**L**	**L**	**L**	**L**	**L**

EH: Extremely high risk, **H**: High risk, **M**: Moderate risk, **L**: Low risk

Figure 8. Mapping of risk scenarios in risk severity matrix in RFRM Phase III filtering

Phase IV: Multi-Criteria Evaluation

The next phase evaluates scenarios based on their ability to overcome the defensive properties of the system. The seriousness of the risk scenarios is evaluated based on a set of criteria. Table 8 shows an example of a bombing risk scenario evaluated against the following 11 criteria: (1) undetectability, (2) uncontrollability, (3) multiple paths to failure, (4) irreversibility, (5) duration of effects, (6) cascading effects, (7) operating environment, (8) wear and tear, (9) hardware, software, human, and organizational (HW/SW/HU/OR) interfaces, (10) complexity/emergent behaviors, and (11) design immaturity.

The evaluation helps in the subsequent phases. First, it highlights risk scenarios that need to be prioritized. It does so by searching for risk scenarios that are evaluated *high* in most of the criteria. Second, in developing risk management options for these risk scenarios, the effort is directed to focus on those criteria where the system's defenses are the weakest.

Table 8. Example of RFRM Phase IV evaluation of risk scenarios to criteria of system's defenses

Criteria	Risk Scenarios (see Table 7)		
	(a) Major Bombing	(b) Excessive rain	(d) Rail Accident
Undetectability	High	Low	High
Uncontrollability	High	High	Medium
Multiple paths to failure	High	Low	High
Irreversibility	Medium	Low	Medium
Duration of effects	High	Medium	High
Cascading effects	High	Low	Medium
Operating environment	High	High	High
Wear and tear	n/a	Medium	Low
Hardware/Software/Human/Organizational	High	n/a	High
Complexity and emergent behaviors	High	Low	High
Design immaturity	Medium	Low	Low

(a) Major Bombing:

Criteria	Evaluation	Brief Explanation
Undetectability	High	System is very "open", bomb device could be easily planted and hid.
Uncontrollability	High	If bomb is found, it is still difficult to prevent it from exploding.
Multiple paths to failure	High	There could be various secondary effects of bombing incident including HazMat consequences, damage to power, etc.
Irreversibility	Medium	Property damage could be rebuilt (not considering loss of lives).
Duration of effects	High	Long-term period needed for restructuring.
Cascading effects	High	Traffic flow in other routes will be affected; business establishment in the area could also be affected.
Operating environment	High	Threat increases depending on terrorism activities and peace /safety condition
Wear and tear	n/a	Not applicable. For major bombing, structure's condition is of no consequence to the extent of damage.
Hardware/Software/ Human/Organizational	High	Recovery depends on a network of response groups
Complexity and emergent behaviors	High	Bomb device, technology and secondary effects are not completely known to response crew.
Design immaturity	Medium	The adverse condition could be made more serious by incorrect response to the threat.

Phase V: Bi-Criteria Filtering Using the Cardinal Severity Matrix

Given the reduced number of scenarios, quantitative evaluation can now be performed. The quantitative assessment uses the same risk matrix used in Phase III (Figures 2 and 8), except that the likelihood is now expressed quantitatively, in terms of probabilities.

In addition, since the filtering threshold in Phase III filtered all scenarios with consequences (D) and (E), these rows could be eliminated in this phase. The remaining categories of the consequences could be expanded to further differentiate severity of risk scenarios. Figure 9 shows the revised risk matrix used in Phase V filtering. If priority attention will be given to risk scenarios with catastrophic consequences involving moderate to significant number of deaths, risk scenario (c) could be set aside for later consideration.

Effect	Likelihood				
	0 < P < .01	.01 ≤ Pr <.02	.02 ≤ Pr < .10	.10 ≤ Pr <.50	.50 ≤ Pr < 1
A1. Significant number of deaths	**EH** (a) bombing (d) rail accident	**EH**	**EH**	**EH**	**EH**
A2. Moderate number of deaths	**EH**	**EH**	**EH**	**EH**	**EH**
A3. Small number of deaths	**EH**	**EH** (b) excessive rain	**EH**	**EH**	**EH**
B1. 100% inoperability – long term	**H**	**H**	**H**	**H**	**EH**
C. Partial Inoperability	**M**	**M**	**M**	**H**	**H**
D. Partial failure but no effect on operation	**L**	**L**	**M**	**M**	**M**
E. No effect	**L**	**L**	**L**	**L**	**L**

EH: Extremely high risk, **H**: High risk, **M**: Moderate risk, **L**: Low risk

Figure 9. Risk severity matrix with cardinal likelihood scale used in RFRM Phase V filtering

Phase VI: Risk Management

Given the set of most critical risks, the risk management phase develops and evaluates risk management options to address these risks. This discussion proceeds with addressing willful hazard.

A terrorist attack can take several forms, depending on the technological means available to the terrorist, the nature of the political issue motivating the attack, and the target's points of weakness. Terrorist incidents can generally be classified into three groups (FTA 2001b): (1) physical attacks to tangible properties; (2) chemical, biological, radiological or nuclear attacks to people, and (3) electronic, radio frequency, or computer-based cyber attacks on information and communication components.

The various risk management options for countering terrorism include:

- Preventive measures, including deterrence (strong legal consequences), preemption (intelligence, monitoring, detection), and public awareness
- Hardening and adding surety, which concern the infrastructure's redundancy, robustness, and resiliency
- Preparedness, response mechanisms, and recovery, which address training, resources, and coordination
- Institutional measures, which include political will and the development of standards and policies.

Using risk trade-off analysis and extreme-event risk analysis, the options are evaluated based on cost, impacts on public safety, and the functionality of the infrastructure. To illustrate, consider the following four options for managing a bombing threat (note that these alternatives are not mutually exclusive):

1. *Establishing nonstructural programs.* Nonstructural programs may involve emergency response training, increased monitoring and surveillance activities, and public awareness campaigns.
2. *Extending the Smart Travel Program* to include monitoring of critical infrastructures. The Smart Travel Program is aimed primarily at delivering user services such as traffic information. However, in addition to these functions, it could potentially be designed to provide dual-use for security and traffic services for critical infrastructures.
3. *Hardening the structure.* Strengthening roads and bridges would protect them from minor to moderate bombing, lessening the potential damage.
4. *Constructing protective structures to isolate effects of bomb blasts.* Constructing protective walls along the interstate would not prevent damage to the highway infrastructure, but it would protect nearby facilities and residences from bomb blasts.

To evaluate the options, two objectives are considered: (1) minimize cost of investment, and (2) minimize cost of damage.

Generating Damage and Cost Estimates

To evaluate the four risk management options presented above, the associated damage and cost must be specified. Given limited data, expert judgment was employed in generating quantitative estimates for damage and cost. The damage probability distributions were generated using the fractile method (Haimes 1998). The method uses experts' estimates of worst-, best-, and median-case scenarios to develop distributions based on fractile probabilities. Also, cost estimation was facilitated by using normalized cost instead of actual costs. Examples of estimates of damage and cost for each option are shown in Table 9. This information is employed in generating the probability density functions for damage as shown in Figure 10 (a)-(d) (see Appendix B for example computation).

Table 9. Estimated damage and cost for the different risk management options

Options	Damage Estimates (millions $)					Normalized Cost
	Best 0%	25%	Median 50%	75%	Worst 100%	
Do Nothing	5	60	80	100	200	0
A. Nonstructural Programs	5	40	50	80	200	20
B. Smart system	5	15	30	45	150	60
C. Hardening	2	5	20	40	130	100
D. Wall	5	45	60	90	170	40

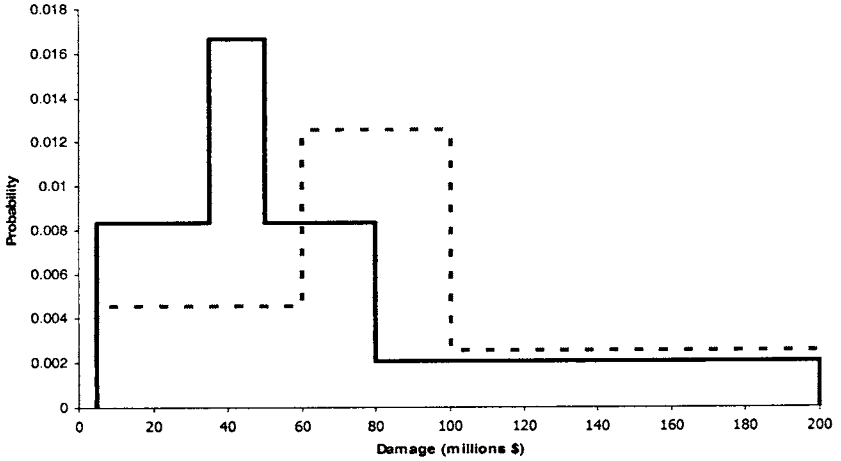
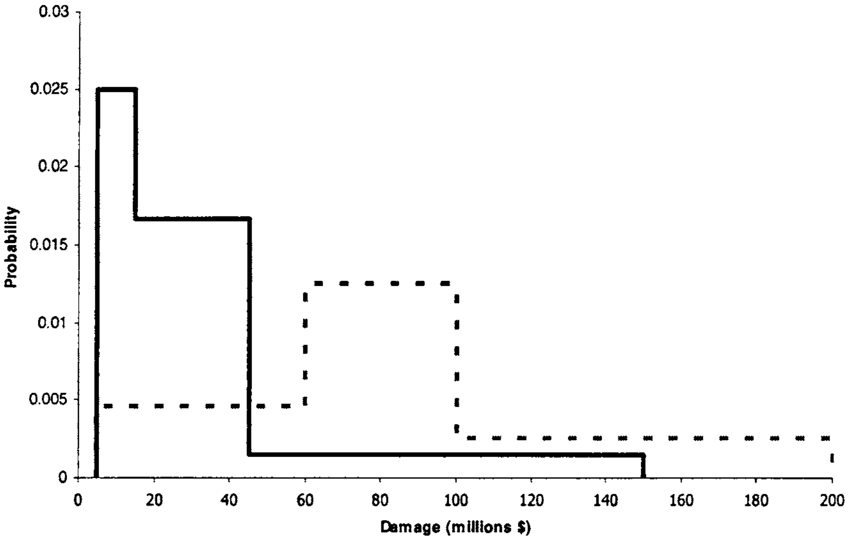
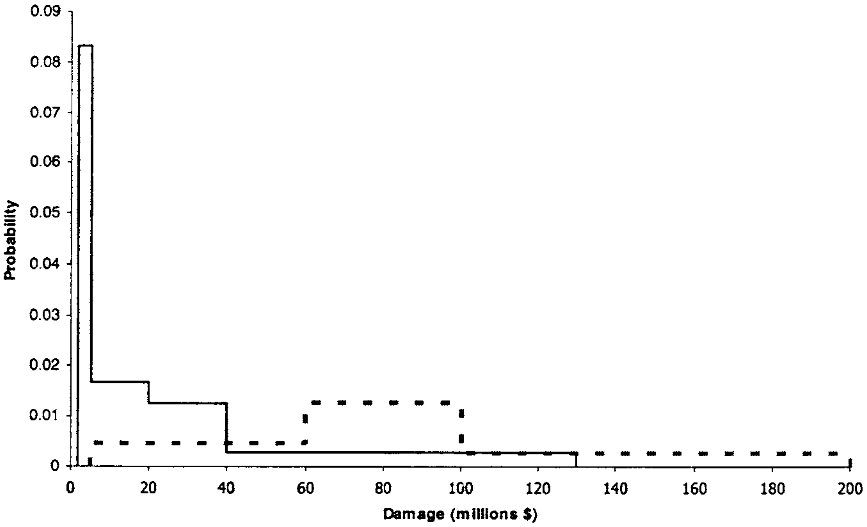


Figure 10. Probability density functions of damage for different risk management options.

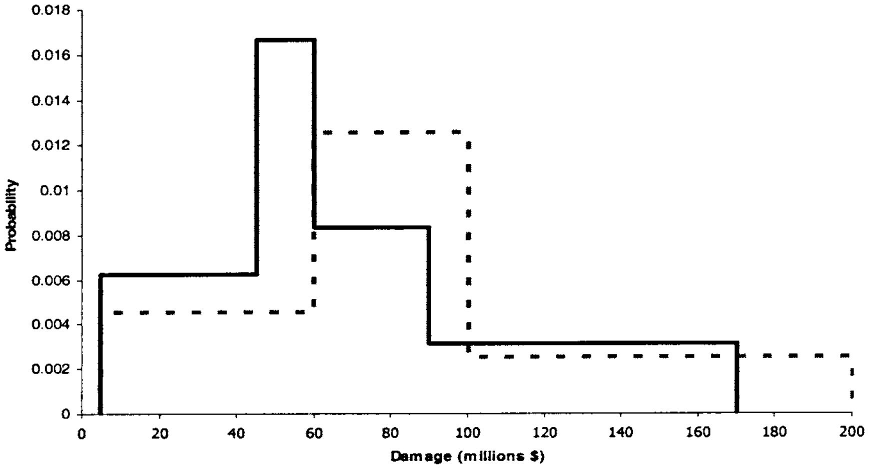
(a) Fractile probability distribution function for Option A (solid line) vs. Do Nothing option (dashed line)



(b) Fractile probability distribution function for Option B (solid line) vs. Do Nothing option (dashed line)



(c) Fractile probability distribution function for Option C (solid line) vs. Do Nothing option (dashed line)

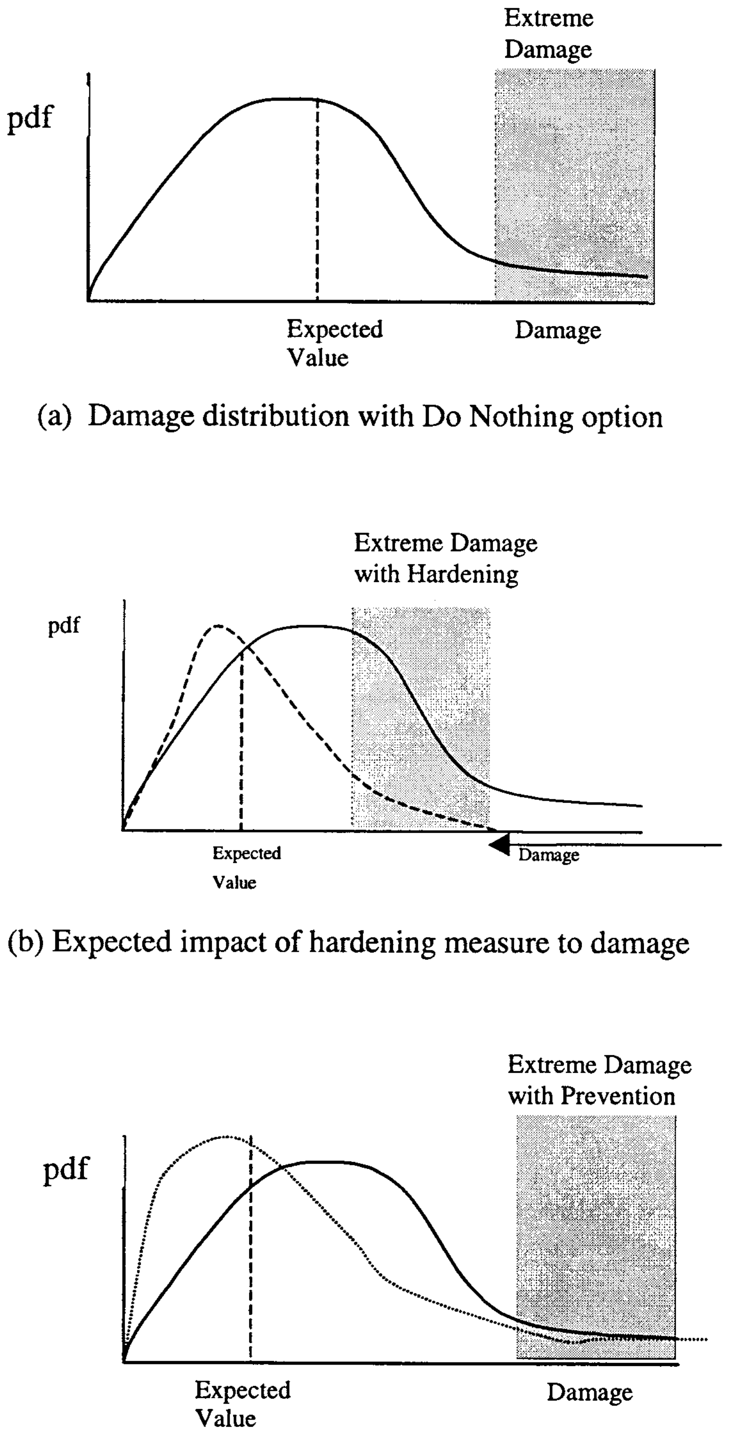


(d) Fractile probability distribution function for Option D (solid line) vs. Do Nothing option (dashed line)

The plots show the different estimated spread of damage given an implementation of an option. In this illustration, Option C showed the most impact in terms of lessening the potential damage of bombing to the system. The spread of potential damage is right-skewed, primarily due to the high-consequence scenario (represented by the long tail to the right of the distribution). Notice that although all options manage to shift the mean of the damage distribution, only Option B (Smart systems), Option C (hardening), and Option D (protective structure) are seen to impact the worse-case value (tail of the distribution). Figure 11 (a)-(c) shows the expected impact of hardening and preventive measures to damage distribution.

Addressing Extreme and Catastrophic Events

In addressing cases with extremely catastrophic events, the expected value is not sufficient. The Partitioned Multiobjective Risk Method (PMRM) is used to supplement the expected value by using conditional expected values (Asbeck and Haimes 1984). A conditional expectation is defined as the expected value of a random variable given that its value lies within some pre-specified probability range. The values of conditional expectations are dependent on where the probability axis is partitioned. Haimes (1998) suggests partitioning of risk according to: $f_2(\cdot)$, of high likelihood and low consequence, $f_3(\cdot)$, of medium likelihood and moderate consequence, and $f_4(\cdot)$, of low likelihood and high consequence.



(a) Damage distribution with Do Nothing option

(b) Expected impact of hardening measure to damage

(c) Expected impact of preventive measure to damage

Figure 11. Expected impact of hardening and preventive measures to minimizing damage

Since the option should be able to protect the system against major bombing attacks, the partitioning should represent the high-consequence/low-probability range. In this case, the partition is made at 10% exceedance probability. This implies that the probability of exceeding the corresponding damage β amount is 10%. Two measures of risk are computed from the distribution: (a) expected values at the damage level (f_5), and (b) conditional expected values at extreme damage levels (f_4). The computed expected values and conditional expected values of damage for the options are given in Table 10. The computation is shown in Appendix C.

Table 10. Example computation of expected and conditional expected values

	Options	Partitioning damage, β (mil $)	Expected Value of Damage, f_5*	Conditional Expected Value of Damage, f_4*	Cost
	Do Nothing	160	86	180	0
A	Nonstructural Programs	152	70	176	20
B	Smart System	108	42	129	60
C	Hardening	94	33	112	100
D	Protective Structure	138	70	154	40

* f_5 and f_4 are the expected and conditional expected value respectively, computed as

$$f_5(\bullet)=\frac{\int_{-\infty}^{\infty} xp(x)dx}{\int_{-\infty}^{\infty} p(x)dx}=\int_{-\infty}^{\infty} xp(x)dx \text{ and } f_4(\bullet)=E[X|\beta > X]=\frac{\int_{\beta}^{\infty} xp(x)dx}{\int_{\beta}^{\infty} p(x)dx}$$

Trade-off Analysis

Figure 12 shows the trade-off between the two objectives. Selection of options is limited to those on the Pareto optimal frontier. Each option on the Pareto optimal frontier offers an improvement in one objective at the expense of another. For instance, hardening the structure (Option C) results in least expected and extreme damage levels; however, it has the highest investment cost. Other options, such as implementing nonstructural programs (Option A), have lower cost but higher damage. Both are optimal solutions along with other options (including the Do nothing option) on the Pareto frontier. The selection depends on the level of damage that is acceptable to the decision maker(s) and possible constraints on the available resource for investment.

Note that it is not necessary to have the same units for the different objectives (pre-commensurating). Given another objective in terms of minimizing system inoperability, the trade-off analysis shows evaluation of three non-commensurate (different units) and conflicting objectives (see Figure 13): (1) cost, in millions $, (2) property damage, in millions $, and (3) inoperability, in percentage.

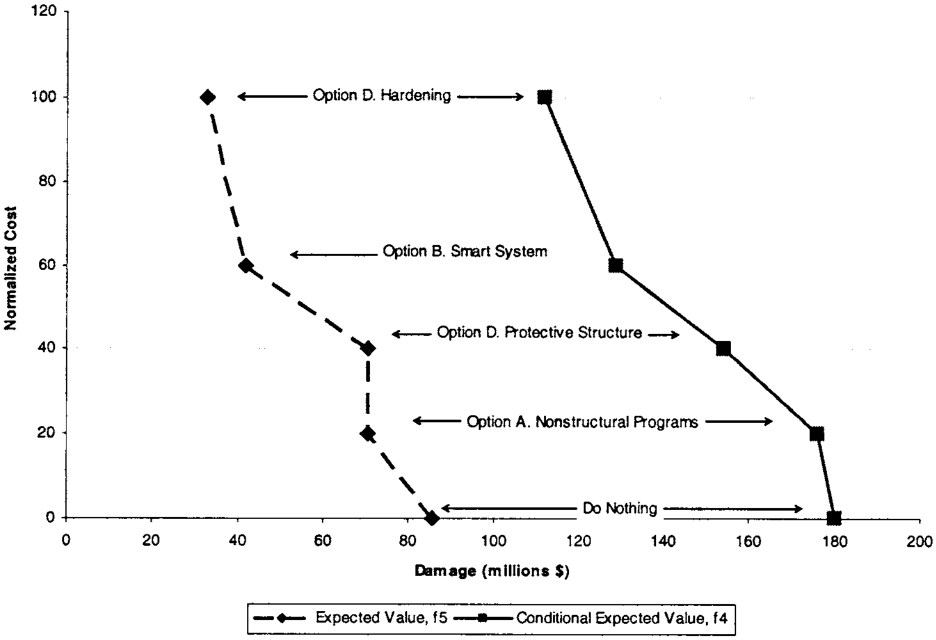
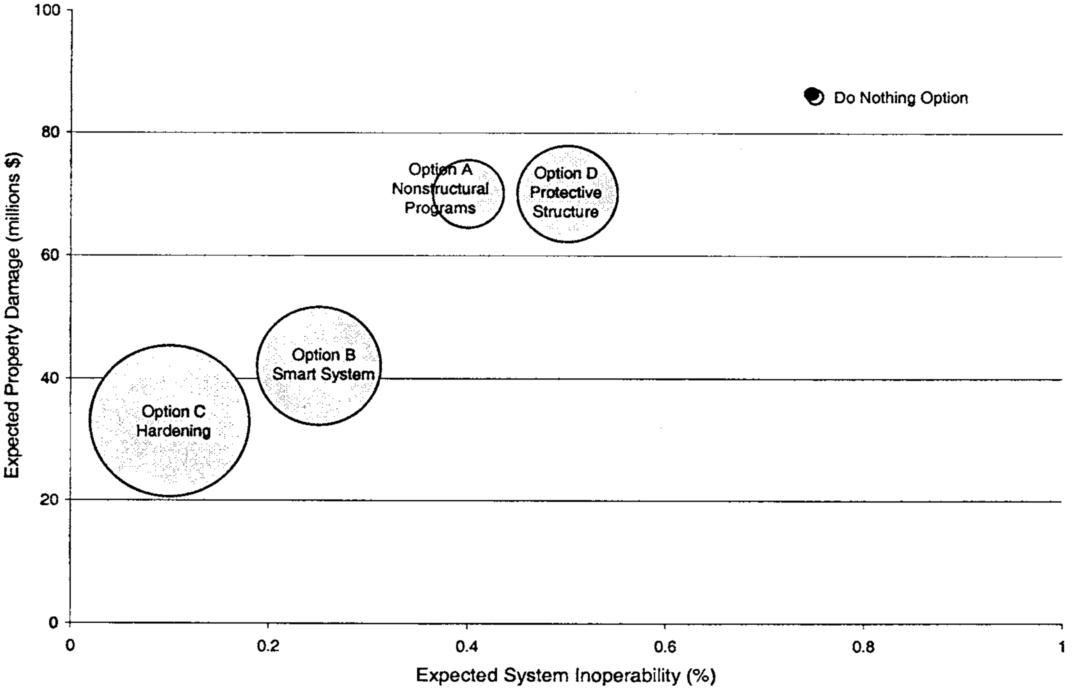


Figure 12. Cost vs. expected value and conditional expected value of damage of the Pareto optimal options



Note: Size of bubble corresponds to cost.

Figure 13. Example of trade-offs among non-commensurate objectives (cost, damage and inoperability)

Note that with from the bubble chart, all options are Pareto optimal options, except for Option D. Notice that Option D has higher cost and higher inoperability and about the same expected damage level as Option A.

Phase VII: Safeguarding Against Critical Items and Phase VIII: Operational Feedback

These phases are essentially feedback loops to allow for various improvements in the analysis and the methodology.

RESULTS

Five case studies were conducted to test the use of the methodological framework described in the previous section. Table 11 gives a brief description of each of these case studies. A sample of critical risks scenarios generated through the use of the RFRM method for each of the case study site is presented. Aside from this, there is no detailed discussion of case studies offered to avoid discussion of any sensitive information.

Table 12 summarizes a sample of the most critical risks scenarios identified in the case studies. Some of the key observations include:

- All of the assets investigated are susceptible to catastrophic events (high consequence, low probability scenarios) generated by *willful threats* (terrorism) and *natural hazards.*

- For road infrastructure (e.g., highways, bridges, and tunnels), cyber attack is not perceived to have as catastrophic impact compared to a physical attack. As can be noted in Tale 12, only the case study on the traffic management system listed cyber threats as critical. This however does not discount the threat of cyber attack. Its impact is expected to change dramatically in the near future with the increasing regional/national integration and growth of other ITS applications.

- Physical attack scenarios are not limited to those generated by bombing using conventional materials. Possible sources of weapons for terrorists include:
  - HazMat vehicles (includes trucks or rail) can be hijacked or intentionally rammed by terrorists using it chemical or radiological weapon in tunnels.
  - HazMat vehicles can be used to set-off explosion underneath a bridge structure.
  - Use of rail, aircraft, boats to crash into structures such as bridges.
  - Pipelines underneath the road structure can be used to set-off an explosion.
  - Fuel storage facilities, nuclear power plants, biological research centers can be rammed by trucks.

Table 11. Brief description of the five transportation CIP case studies

Case Study	Description
1. Traffic management center	The traffic management system (TMS) monitors the regional traffic through an extensive network of computer-controlled, fiber-optic based communication and control network. The case study investigated a TMS center, evaluating its hardware, software, facilities, organization, and personnel aspects. Among its many major risk concerns include cyber attack and maintenance of field and station equipment.
2. Major bridge	This case study investigated a major bridge that carries an arterial highway. Many critical facilities are supported by passage over or under the bridge, such as military bases, a power station, and an airport. In addition, its moving components pose certain concerns relating to control and maintenance.
3. Major bridge-tunnels	In this case study, the risk analysis framework is applied to two interconnected structures, providing two of the major water crossings in the state of Virginia. Facility security and maintenance are among the major considerations.
4. Major interchange between interstates	This case study analyzed a busy interchange between two major interstates. It supports travel to key facilities in the area, including the area's business centers. Its proximity to many military installations make it vulnerable to willful hazard.
5. Major interchange between an interstate and vital urban road	This case study investigated a major interchange between an interstate and an urban road. In close proximity to it are other critical infrastructures such as airport, water reservoir, railroad tracks, and military bases. The asset is also part of the hurricane evacuation route.

Table 12. Critical risks identified in case studies

Case Study Site	Critical Risks
1. Traffic management system	**Cyber attack** • Cyber attack from an insider introduces virus into the system causing total system failure. • Cyber attack from municipality entry point disables or changes control devices causing loss of life. • Internal employee allows for hacker to alter system, causing loss of life. **Terrorism.** Terrorist explosion causes control device to be destroyed resulting in loss of life. **Natural hazard.** Water floods the control wiring causing functions of central system to be fully lost. **Funding.** Shortage in funding for updating of system resulting to system vulnerability to new virus attacks.

Table 12 *(cont'd).* Critical risks identified in case studies

Case Study Site	Critical Risks
2. Major bridge	**Terrorism**. Terrorist to tamper or bomb the bridge's circuitry. **Natural hazard** • Adverse weather condition, such as rain, snow and ice, leads to serious accidents. • Strong waves and wind during category V hurricane (bridge is designed to withstand category I to IV hurricane). • Lightning damages or destroys the electronic systems of the bridge's control.
3. Major bridge/tunnels (***Structure 1 and 2***)	**Terrorism** • Large bomb explosion in ***Structure 1 or 2***, on or above the tunnel roadway surface, causes both tunnels to be shut down. • Terrorist enters the facility and proceeds to the lower levels of Structure 1 or 2, sabotaging underside/topside of the tunnel roadway, pumping system, or ventilation system, resulting to shut down. **Natural hazard** • Extensive wind and water erosion during hurricane damages the structure. • Terrorist enters the facility and proceeds to the lower levels of Structure 1 or 2, sabotaging underside/topside of the tunnel roadway, pumping system, or ventilation system, resulting to shut down. **Equipment Maintenance** • Equipment used for ventilation, pumping, and control system breaks down, forcing partial closure of tunnels. • Shortage or delay of available fund purchase rare replacement parts for fans, generators, ventilation equipment.
4. Major interchange between interstates	**Terrorism** • Terrorist bombing destroys all or part of the interchange. • Terrorist uses biological, chemical, or nuclear weapon in the area that renders the interchange unusable for a long period. **Natural hazard** • Snow and ice accumulation causes structural failings. • Earthquake destroys all or part of the interchange. **Hazmat spill**. Transport vehicle for hazardous materials crashes causing a major spill.

- *Conduct workshops/forum for cooperative information sharing.* Assessing the potential threat to transportation facilities and the implementation of effective measures requires the participation of public and private sectors. A shared responsibility for protection, mitigation, and protection is the strategy envisioned by President's Commission on Critical Infrastructure Protection (PCCIP) – a cooperative "information sharing" and knowledge management that facilitates the conduct of the risk assessment process and secures critical assets against threats and their cascading effects. In addition, knowledge management must become a fundamental paradigm for effective communication and trust between the diverse state and federal organizations in order to ensure timely risk management. The New Mexico Critical Infrastructure Assurance Council (NMCIAC) may serve as a model by which VDOT evaluate its CIP protection policies.

- *Coordinate the efforts of federal, state, and local government agencies, as well as nongovernmental entities involved in CIP.* Effective CIP must recognize these important players and encourage all stakeholders to recognize the importance of CIP in order to ensure a protected infrastructure. Many field officials perceive that national, state and local programs are "patchwork," often resulting in overlapping assessments and redundant training programs. Coordination will exchange innovations and ideas in CIP and allow different agencies to adopt best practices and security technology to strengthen their systems.

- *Plan and implement robust structural and non-structural management options.* This involves the following:

    - *Ensure that proper security measures are currently being implemented.* Most of surface security measures such as those of bridge's control and equipment facilities are not designed to withstand forceful entry. Providing access security and ensuring that security procedures are being done properly are low-cost preventive measures that VDOT can implement immediately for both its physical and cyber assets.

    - *Define threat conditions.* To help in proper dissemination of information, a set of threat levels and corresponding actions could be defined by VDOT. This would be enhanced if the initiative would be implemented for the entire Commonwealth. The U.S. Department of Defense (DoD) has defined a five-level threat conditions (THREATCON) to describe the progressive level of a terrorist threat to all US military facilities and personnel under DOD Directive O-2000.12 (DoD 1998).

    - *Assess the capabilities of emergency response and recovery teams.* Not all incidents can be prevented, and in catastrophic scenarios such as a major bombing, further consequences can be prevented by effective response and recovery operations. In such a statewide recovery and response assessment, particular attention ought to be paid to emergency response to terrorist attacks. Normal emergency procedures may not be adequate and can be extremely costly, particularly if the terrorist act is a hoax. Issues to investigate include adequacy of organization, operational guidelines, communication, inter-agency coordination, skills and equipment, and distribution of manpower and other resources.

  - *Identify key security technology and R&D strategy.* Research should cover strengthening of the infrastructure through design and construction (e.g., improved materials), rapid bridge repair techniques, and security technology.

- *Assess VDOT's critical assets statewide.* Assessment of risk and vulnerabilities must be sustained and expanded to include systemic risks beyond the local damage to an individual facility, as was the case in this study. The proposed direction of future study is to conduct systemwide risk assessment and management of various VDOT systems, focusing on statewide systems such as communication, roads and highway network, and maintenance. Among the key aspects that would be addressed are priority-setting, knowledge mapping, and interdependencies.

  - *Measuring criticality and setting priorities.* VDOT needs to be able to identify its most critical infrastructures. VDOT has traditionally prioritized infrastructures according to transportation performance metrics, such as those pertaining to usage and safety measures. Defining critical assets within the context of PDD 63 goes beyond these metrics to include impact to governance, economy, and national security. As yet, there are no standards with which to measure the criticality of an asset.

    Criticality relates to elements that make an asset more susceptible to risk, thus making the risks more severe. Therefore, criticality is a function of threat, impact, and vulnerability corresponding to risk, consequence, and likelihood. The key tasks are to identify the different properties that are relevant to the criticality of an infrastructure and develop a methodology to measure and integrate these properties in order to assess the criticality of transportation infrastructure systems.

  - *Knowledge mapping.* Is the information for assessing risks to critical infrastructure available? The extent to which VDOT is exploiting and benefiting from information technology must be evaluated. Mapping of current information requirement vs. current available resources for risk assessment and management of willful hazards is needed. Information infrastructure must be built among various agencies to facilitate sharing and at the same time secure sensitive information.

  - *Understanding interdependencies.* Many components of the transportation infrastructure are highly interdependent. Moreover, the expanded use of information technology has increased these interdependencies and introduced new interdependent relationships that have not yet been fully understood.

  - *Multiple simultaneous failures.* The current case studies focus on only one risk scenario for each case study site. Interesting results may be gained by examining the situation where multiple failures occur simultaneously against a particular site. Such a study would examine unique risks associated with the occurrence of multiple failures and their cascading effects, such as the increased demand on emergency and recovery response teams as well as the impact on structural failures and security.

REFERENCES

Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. December 2000. *Part II. Toward a National Strategy for Combating Terrorism.* Second Annual Report to the President and the Congress. Washington, D.C.

Asbeck, E. L., and Haimes, Y.Y. 1984. The partitioned multiobjective risk method (PMRM). *Large Scale Systems*, 6(1), 13-38.

Boyd, A., and Sullivan, J.P. 1997. *Emergency Preparedness for Transit Terrorism.* TCRP Synthesis of Transit Practice 27, Transportation Research Board, National Research Council. National Academy Press, Washington DC.

Critical Infrastructure Assurance Office. 2000. *Practices for Securing Information Assets.* Washington, DC.

Federal Transit Administration. Fall 1999. *State Safety Oversight (SSO) Newsletter*, Issue 6, 10-11. Retrieved online on July 1, 2001, from http://transit-safety.volpe.dot.gov/safety/sso/newsletters/issue6.

Federal Transit Administration. 2001a. *Crime Prevention and Anti-Terrorism.* Retrieved online on July 1, 2001, from http://www.fta.dot.gov/research/safe/crimeprev.

Federal Transit Administration. 2001b. *Surface Transportation Security: Vulnerabilities and Developing Solutions.* Retrieved online on July 1, 2001, from http://www.fta.dot.gov/research/safe/pubs/sursec/sursec.html.

Freedberg, S.J. Jr. March 15, 2001. *Feds Prepare State, Local Governments for Terrorist Attacks.* Retrieved online on July 17, 2001, from http://www.govexec.com/dailyfed/0301.

Haimes, Y.Y. 1981. Hierarchical holographic modeling. *IEEE Transactions on Systems, Man, and Cybernetics* 11(9), 606-617.

Haimes, Y.Y. 1991. Total risk management. *Risk Analysis* 11(2) 169-171.

Haimes, Y.Y. 1998. *Risk Modeling, Assessment, and Management.* John Wiley and Sons, New York.

Haimes, Y.Y., Kaplan, S., and Lambert, J.H. 2002. Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis* 22(2) 381-395.

Kaplan, S. 1992. "Expert information" versus "expert opinions." Another approach to the problem of eliciting/combining/using expert opinion in PRA. *Journal of Reliability Engineering and System Safety*, 35, 61-72.

Kaplan, S., and Garrick, B.J. 1981. On the quantitative definition of risk. *Risk Analysis* 1(1), 11-27.

Meyer, M.A., and Booker, J.M. 1991. Eliciting and Analyzing Expert Judgment: A Practical Guide. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC.

National Research Council. 1999. *Improving Surface Transportation Security: A Research and Development Strategy*, A report by the Committee on R&D Strategies to Improve Surface Transportation Security. National Academy Press, Washington, DC.

National Security Telecommunications Advisory Committee. May 2000. *Information Sharing/Critical Infrastructure Protection Task Force Report.* Washington, DC.

National Science and Technology Council. May 1999. *National Transportation Science and Transportation Strategy.* A report by the Committee on Technology, Subcommittee on Transportation Research and Development. Washington, DC.

O'Neill D.J. 2000. Statewide critical infrastructure protection: New Mexico's Model. *TR News*, November-December 2000, 211, 25-27.

President's Commission on Critical Infrastructure Protection. October 1997. *Critical Foundations: Protecting America's Infrastructures.* Washington, DC.

Roland, H.E., and Moriarty, B. 1990. *System Safety Engineering and Management*, 2nd ed. John Wiley and Sons, New York.

U.S. Department of Energy. 1998. *BY-1998 Guidance Manual.* Retrieved online September 12, 1999, from http://tis.eh.doe.gov/bps/eshplan/rpm.htm.

U.S. Department of Defense. March 1998. Joint Tactics, Techniques, and Procedures for Antiterrorism (Joint Pub 3-07.2).

U.S. Department of Transportation. 1999. *Worldwide Terrorist and Violent Criminal Attacks Against Transportation-1998.* Office of Intelligence and Security, In-house report.

U.S. Department of Transportation. March 1999a. *Guide to establishing an information system protection program (DOT H 1350.250).* Washington, DC.

U.S.. Department of Transportation. October 1999b. *National Security Flagships.* Retrieved online July 5, 2001, from http://www.dot.gov/onedot/newsetl.htm.

US Department of Transportation. September 2000a. *ONEDOT 2000-2005 Strategic Plan.* Retrieved online on July 5, 2001, from http://stratplan.dot.gov/.

U.S. Department of Transportation. October 2001. *Surface Transportation Vulnerability Assessment (General Distribution version).* Research and Special Programs Administration and Office of Intelligence and Security, Washington, DC.

U.S. General Accounting Office. 1988. *Domestic Antiterrorism Efforts at Selected Sites,* GAO/PEMD-88-22. Washington, D.C.

Virginia Department of Transportation. October 17, 2000. *Organization Guide.* Richmond.

APPENDIX A. CONTACT PERSONS

Case Study	Contact Persons
1. Traffic management center (TMC)	Dwayne Cook James Mock Erika Ricks Frederic Harris (SMART Traffic Center)
2. Major bridge	Vince J. Roney (VDOT - Hampton Roads District)
3. Major bridge-tunnels	Bruce Wilkerson (VDOT – Hampton Roads District)
4. Major interchange between interstates	Marcie Parker Wayne Williams
5. Major interchange between an interstate and vital urban road	Quinton D. Elliott (VDOT-Williamburg Residency) Charles A. McIver (VDOT-Central Office, Hydrology) Karen R. Rusak (VDOT-Traffic Management System) Hurley F. Minish (VDOT-Location and Design Division) Jose P. Gomez (VTRC)

APPENDIX B. GUIDE IN CONSTRUCTING DAMAGE DISTRIBUTION USING FRACTILE METHOD

Probability distributions arise from uncertain outcomes. Examples of such uncertain outcomes are the damage consequences and the costs of investment. The nature of the problem dictates which probability distributions may be appropriate for modeling the resulting random outcomes.

Probability distribution are constructed using historical data, simulations, or in cases where data is unavailable, from expert judgment. Such is the case for estimating parameters for willful attack since there are few historical cases available. The fractile method [Haimes 1998] constructs the probability distributions based on expert judgment. The following illustrates the steps involved in using the fractile method.

(1) The fractile method divides the probability axis [0,1] into sections, termed fractiles, as follows:

- 0.00 fractile associated with the best scenario (0 percentile)
- 1.00 fractile associated with the worst scenario (100th percentile)
- 0.50 fractile associated with the median scenario (50th percentile)
- 0.25 fractile (25th percentile), and
- 0.75 fractile (75th percentile)

(2) Expert judgment is solicited from one or more experts to estimate the above scenarios. The estimate for the extent of property damage resulting from a major bombing is given in below (taken from **Error! Reference source not found.** of main report)

Options	Damage Estimates (millions $)				
	Best 0.00	0.25	Median 0.50	0.75	Worst 1.00
Do Nothing	5	60	80	100	200
A. Nonstructural Programs	5	40	50	80	200
B. Smart system	5	15	30	45	150
C. Hardening	2	5	20	40	130
D. Wall	5	45	60	90	170

(3) Compute for *p(x)*

Recall that a continuous random variable X of damages has cumulative density function P(x) and a probability density function p(x) defined by:

$P(x) = prob[X \leq x]$ - cumulative density function (cdf)

$p(x) = dP(x)/dx$ - probability density function (pdf)

with *p(x)* satisfying the following properties:

$p(x) \geq 0$ for all x and $\int_{-\infty}^{\infty} p(x)dx = 1$

We can determine the probability of finding the damage somewhere in the finite interval $[a, b]$:

$$prob(a \leq x \leq b) = \int_{a}^{b} p(x)dx$$

From step (1), we see that the damage has been divided into 4 segments, and each segment has an associated 25th percentile each. This corresponds to the probability of occurrence between a pair of succeeding fractiles. This implies that the probability of finding damage between worst scenario and 0.25 fractile scenario is 0.25. This is true for all pairs of succeeding fractiles.

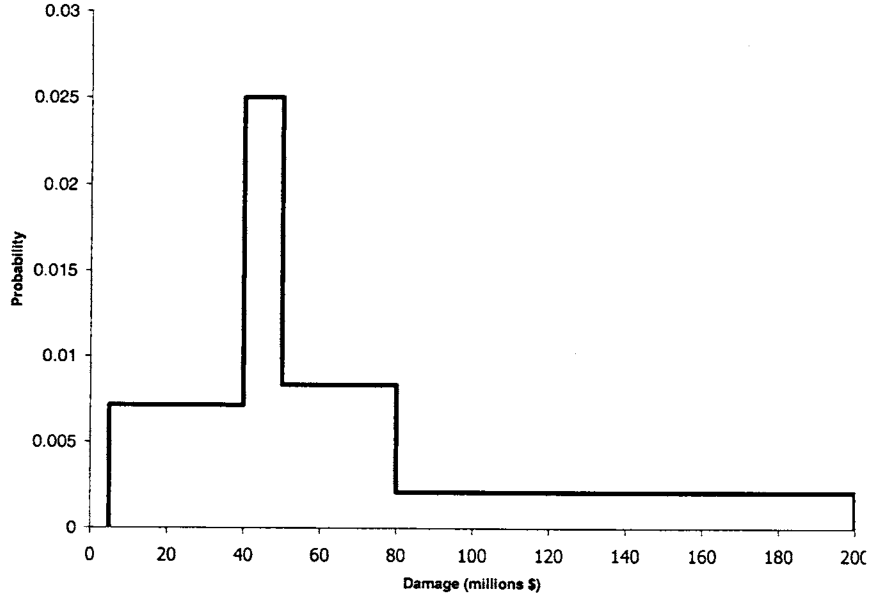
$$prob(a \leq x \leq b) = \int_{a}^{b} p(x)dx = 0.25$$

Computing for *p(x)*, *p(x)* = 0.25/(*b*-*a*) with the following result for Option A (see table of damage estimates in step 2):

Pair of Fractiles	Estimated Damage [*b*–*a*]	*p(x)* = 0.25/(*b*-*a*)
[0.00 and 0.25]	[40 – 5]	0.007
[0.25 and 0.50]	[50 – 40]	0.025
[0.50 and 0.75]	[80 – 50]	0.008
[0.75 and 1.00]	[200 – 80]	0.0021

(4) Plot the damage and corresponding *p(x)*.

Probability distribution function for Option A.



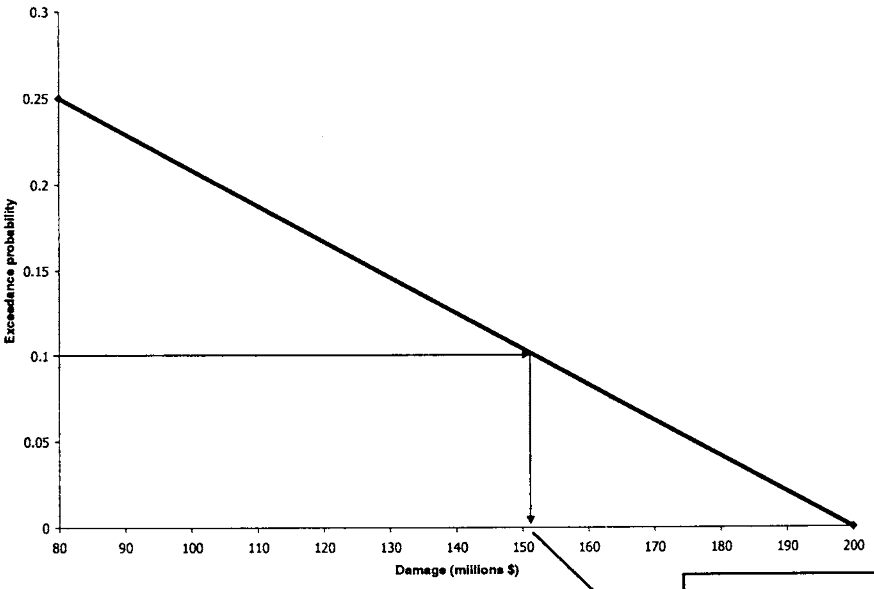
APPENDIX C. COMPUTING THE CONDITIONAL EXPECTED VALUE OF DAMAGE (f_4)

In addressing cases with extremely catastrophic events, the expected value is not sufficient. The Partitioned Multiobjective Risk Method (PMRM) is used to supplement the expected value by using conditional expected values [Asbeck and Haimes 1984]. A conditional expectation is defined as the expected value of a random variable given that its value lies within some pre-specified probability range.

The values of conditional expectations are dependent on where the probability axis is partitioned. Haimes [1998] suggests partitioning of risk according to: $f_2(\cdot)$, of high likelihood and low consequence, $f_3(\cdot)$, of medium likelihood and moderate consequence, and $f_4(\cdot)$, of low likelihood and high consequence. Since the option should be able to protect the system against major bombing attacks, the partitioning should represent the high-consequence/low-probability range.

(1) Defining the partitioning representing high-consequence/low-probability range

In this case, the partition is made at 10% exceedance probability. This implies that the probability of exceeding the corresponding damage β amount is 10%. To compute for β, we look for the damage value associated with the exceedance probability (i.e. p(X > β) equal to 0.10. We know this β will lie within the interval of the last fractile pair [0.75 and 1.00] with corresponding damage interval of [80 – 200] for Option A. Constructing the exceedance probability (1-cdf),



Corresponds to β partition

From the graph, we can use simple geometry to calculate for β,

$$\frac{\beta-80}{200-80}=\frac{0.25-0.10}{0.25} \text{ giving } \beta=152$$

(2) Calculating the conditional expected value f_4 defined by

$$f_4(\bullet)=E[X|\beta>X]=\frac{\int_{\beta}^{\infty} xp(x)dx}{\int_{\beta}^{\infty} p(x)dx}$$

Still using the above example on Option A (note that p(x) for the whole interval [152 - 200] is uniform = 0.0021 (see Appendix B step (3)):

$$f_4(\bullet)=E[X|152>X]=\frac{\int_{152}^{200} x0.0021dx}{\int_{152}^{200} 0.0021dx}=\frac{\left.\frac{x^2}{2}\right|_{152}^{200}}{\left.x\right|_{152}^{200}}=\frac{\frac{(200^2-152^2)}{2}}{(200-152)}=176$$

This conditional expected value ($176 million) is always greater than the expected value ($70 million). In this case, there is a significant difference between the two values. The conditional expected value given by f_4 represents the extreme event. It supplements the expected value measure to highlight the risk resulting from catastrophic scenarios.