FHWA/IN/JTRP-2007/19

Final Report

**SYNTHESIS OF BEST PRACTICES FOR
TRANSPORTATION SECURITY**

Volume I: Vulnerability Assessment

**Haritha Reddy Venna
Jon D. Fricker**

January 2009

INDOT Research

TECHNICAL *Summary*

Technology Transfer and Project Implementation Information

TRB Subject Code: 12-3 State and Regional Studies
Publication No.: FHWA/IN/JTRP-2007/19, SPR-2872

January 2009
Final Report

Synthesis of Best Practices for Transportation Security

Introduction

Disruptions to transportation systems have far-reaching consequences in terms of safety and security. There is an urgent need to reduce vulnerability of critical transportation infrastructure and minimize the economic impacts of such disruptions. Because critical assets and the perceptions of criticality differ from state to state, based on various factors such as nature of the assets and the location and environment of the assets, it is necessary for Indiana Department of Transportation (INDOT) to review and evaluate its assets. The American Association of State Highway and Transportation Officials (AASHTO) suggested preliminary guidelines for vulnerability assessment of transportation assets.

In response to the new terrorist threat, state transportation agencies have been forced to revise

and update their emergency response capabilities. A review of Federal Homeland Security measures in emergency management was undertaken to provide a basis for such integration, including the National Incident Management System and the National Response Plan released by the DHS. An analysis of existing Indiana emergency management practices was performed, and issues in INDOT's current emergency response procedures were identified. A review of best practices in emergency response was developed that will serve as a guide for the future implementation of security measures by INDOT.

Findings

The results of the research include:

1. A list of top 25 critical assets in each district and a general methodology to combine different assets from districts to obtain a comprehensive statewide list.
2. Recommendations to state DOTs for identifying and assessing critical assets with respect to Vulnerability and Criticality.
3. Suggested countermeasures to reduce the vulnerability of a given asset based on its relevant characteristics.
4. Reminder that INDOT needs to make sure that its current emergency response practices are integrated with the practices in place by emergency agencies at all levels. This includes an Emergency Operations Plan that establishes the procedures INDOT personnel at all levels need to follow when responding to an emergency. The procedures included should consider following an all-hazards approach, ensure proper integration and interoperability, and redundancy and Continuity of Operations. The EOP should also ensure INDOT personnel safety during the response efforts.
5. INDOT should adopt the Incident Command System as its organizational structure for emergency response operations.

Implementation

Maintain an active Counter-Terrorism and Security Task Council within INDOT to coordinate elements within INDOT and coordinate with agencies outside INDOT. Adopt

the structures and procedures described in the report, such as the Incident Command System and an all-hazards Emergency Operations Plan, which are becoming standard across the country.

Contacts

For more information:

Prof. Jon D. Fricker

Principal Investigator
School of Civil Engineering
Purdue University
West Lafayette, IN 47907-2051
Phone: (765) 494-2205
Fax: (765) 496-7996
E-mail: fricker@ecn.purdue.edu

Indiana Department of Transportation

Division of Research
1205 Montgomery Street
P.O. Box 2279
West Lafayette, IN 47906
Phone: (765) 463-1521
Fax: (765) 497-1665

Purdue University

Joint Transportation Research Program
School of Civil Engineering
West Lafayette, IN 47907-1284
Phone: (765) 494-9310
Fax: (765) 496-7996
E-mail: jtrp@ecn.purdue.edu
<http://www.purdue.edu/jtrp>

Final Report

FHWA/IN/JTRP-2007/19

SYNTHESIS OF BEST PRACTICES IN TRANSPORTATION SECURITY

Volume I: Vulnerability Assessment

by

Haritha Reddy Venna
Graduate Research Assistant

and

Jon D. Fricker
Professor
School of Civil Engineering
Purdue University

Joint Transportation Research Program
Project No. C-36-67VVV
File No. 9-10-73
SPR-2872

Conducted in Cooperation with the
Indiana Department of Transportation
and the
U.S. Department of Transportation
Federal Highway Administration

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 Indiana Department of Transportation or the Federal Highway Administration at the time of publication. The report does not constitute a standard, specification, or regulation.

Purdue University
West Lafayette, IN 47906
January 2009

1. Report No. FHWA/IN/JTRP-2007/19	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Synthesis of Best Practices in Transportation Security (Two-Volume Report)		5. Report Date January 2009	
		6. Performing Organization Code	
7. Author(s) Hariitha Reddy Venna, Rodrigo Vargas, Jon D. Fricker		8. Performing Organization Report No. FHWA/IN/JTRP-2007/19	
		10. Work Unit No.	
9. Performing Organization Name and Address Joint Transportation Research Program 1284 Civil Engineering Building Purdue University West Lafayette, IN 47907-1284		11. Contract or Grant No. SPR-2872	
		13. Type of Report and Period Covered Final Report	
12. Sponsoring Agency Name and Address Indiana Department of Transportation State Office Building 100 North Senate Avenue Indianapolis, IN 46204		14. Sponsoring Agency Code	
15. Supplementary Notes Prepared in cooperation with the Indiana Department of Transportation and Federal Highway Administration.			
16. Abstract <p>Part I of the research focused on developing a methodology to identify and evaluate the most critical and vulnerable INDOT assets. This method aims at obtaining an index that reflects the vulnerability and criticality of an asset on the basis of multiple performance criteria. This methodology was tested on the seven INDOT districts. Because not all the factors that influence the vulnerability do have same weight, the analytical hierarchical process is used to obtain the weights for the criteria. Countermeasures are suggested as a part of the research to reduce the vulnerability of a given asset based on its relevant characteristics. The results included a list of top 25 critical assets in each district and a general methodology to combine different assets from districts to obtain a comprehensive statewide list. The research also includes recommendations to DOTs for identifying and assessing critical assets with respect to Vulnerability and Criticality.</p> <p>Part II of the research focused on developing a blueprint for an INDOT Emergency Operations Plan that will effectively integrate its emergency response practices with the larger national and statewide emergency management framework. The Incident Command System was confirmed to be a good standard practice among state DOTs, which can be applied to enhance INDOT's emergency response procedures. Other practices reviewed included communications, the application of Intelligent Transportation Systems to emergency response, and the use of Decision Support Systems to support emergency operations. A version of the Incident Command System for adoption by INDOT Districts and Central Office was developed. Finally, a structure was proposed for the development of an INDOT EOP.</p>			
17. Key Words transportation security, vulnerability assessment, criticality, emergency response, asset protection, recovery, communications, continuity of operations		18. Distribution Statement No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages I-104 II-172	22. Price

TABLE OF CONTENTS

	Page
LIST OF TABLES.....	iv
LIST OF FIGURES	v
 CHAPTER1. INTRODUCTION	 1
1.1. Background.....	1
1.2. Problem Statement.....	3
1.3. Research Objectives and Scope	5
1.4. Organization of the Report	6
CHAPTER 2. LITERATURE REVIEW	7
2.1. Overview of Transportation Security and Vulnerability Assessment	7
2.2. Transportation and Security.....	8
2.3. Components of Vulnerability Assessment	9
2.4. Vulnerability Assessment Methodologies	10
2.4.1. AASHTO Methodology	10
2.4.2. Federal Transit Agency Method	14
2.4.3. TMC Risk Assessment Methodology	22
2.4.4. TMC Risk Assessment Method	25
2.4.5. Comparison of Vulnerability Assessment Methodologies	26
2.5. Other VA Methodologies used by States and Agencies.....	27
2.5.1. Iowa Plans for Critical Asset Protection.....	27
2.5.2. Transportation Security Activities in Texas.....	28
2.5.3. TMSARM Vulnerability Self Assessment Tool	29
2.5.4. Blue Ribbon Panel Approach for Bridge VA	30

	Page
2.5.5. Sandia National Lab Community Vulnerability Assessment Methodology (VAM).....	33
2.6. Multi Criteria Decision Methods	33
2.6.1. The WSM Method	35
2.6.2. The WPM Method	36
2.6.3. The AHP Method.....	37
2.6.4. The ELECTRE Method	38
2.6.5. Resolving Conflicts.....	39
2.7. Fuzzy Logic	40
2.8. Neural Networks.....	41
2.9. Need for this Study	42
CHAPTER 3. RESEARCH METHODOLOGY	44
3.1. Research Framework	44
3.2. Vulnerability Assessment	46
3.2.1. Vulnerability and Criticality Index	47
3.2.2. Vulnerability and Criticality Index Formulation	48
3.3. Data Collection	49
3.3.1. Identification of Assets -- Preliminary Survey	49
3.4. Development of District Survey	50
3.4.1. Determination of Vulnerability and criticality Definitions.....	53
3.4.2. District Survey Data Collection	55
3.5. Obtaining the Weights Using AHP	56
3.5.1. Decomposition of the problem into hierarchy	57
3.5.2. Comparative Judgment of Elements	61
3.5.3. Synthesis of Priorities	62
3.5.4. Justification for AHP	67
CHAPTER 4. ANALYSIS AND DISCUSSION OF RESULTS.....	68
4.1. Analysis of District Survey Results.....	68
4.2. Discussion of Results.....	73
4.3. Combining Vulnerability and Criticality Indices	74

4.4. Comparing Results from Different Districts.....	76
4.5. Comprehensive Vulnerability Assessment using AHP	79
4.5.1. Determination of Criteria Weights Using AHP	82
4.6. Iterative Vulnerability Assessment and Neural Networks.....	84
CHAPTER 5. RECOMMENDATIONS FOR INDOT TO CONDUCT VA.....	85
5.1 Introduction.....	81
5.2 Multidisciplinary Team Composition.....	81
5.3 Resources and Data Needs.....	87
5.4 Critical Asset Identification	88
5.5 Threat Assessment	90
5.6 Identification of Assets for Improvement.....	91
5.7 Recommended Countermeasures.....	91
5.7.1. Choosing an Appropriate Countermeasure for an Asset.....	94
5.7.2. Response and Recovery Measures.....	95
CHAPTER 6. CONCLUSIONS	96
6.1 Research Contributions.....	97
6.2 Lessons Learned and Limitations	98
6.3 Recommendations for Further Research	99
LIST OF REFERENCES.....	101

LIST OF TABLES

Table	Page
Table 1. Analysis of Criticality of Bus Assets.....	17
Table 2. Relevant Bus Scenarios	21
Table 3 Fundamental Scale for Pairwise Comparisons	61
Table 4. Pairwise Comparison of Criteria.....	63
Table 5. Pairwise comparison of assets with respect to Importance.....	65
Table 6. Local Priorities for Alternatives	66
Table 7 Prioritization of Assets Using Vulnerability and Criticality Index.....	75
Table 8 Comprehensive Vulnerability Survey.....	80
Table 9 Weights of Criteria Obtained from AHP Survey.....	83
Table 10 Critical Asset Factors and Values.....	90

LIST OF FIGURES

Figure	Page
Figure 1. Six steps for conducting vulnerability assessment	13
Figure 2 Risk Assessment Process.....	15
Figure 3. Threat Assessment Process.....	20
Figure 4 Research Framework	46
Figure 5 Introductory User Interface	52
Figure 6 The Definition User Interface.....	52
Figure 7 Expert Information Input User Interface	53
Figure 8 Vulnerability and Criticality Matrix.....	56
Figure 9 The AHP Hierarchical Process.....	58
Figure 10 Illustration of AHP	58
Figure 11 Crawfordsville Vulnerability and Criticality Matrix.....	69
Figure 12 Fort Wayne Vulnerability and Criticality Matrix.....	70
Figure 13 Greenfield Vulnerability and Criticality Matrix.....	71
Figure 14 LaPorte Vulnerability and Criticality Matrix.	72
Figure 15 Vincennes Vulnerability and Criticality Matrix	73
Figure 16 Vulnerability and Criticality Matrix – All District Plot	76
Figure 17 AHP Framework used in the Research.....	83

CHAPTER 1. INTRODUCTION

The events of September 11, 2001 revealed the vulnerability of transportation systems and the massive consequences of attacks on them. Tom Ridge, Secretary for Homeland Security, said “The terrorist only has to be right once; we have to be right all the time.” (DHS, 2003). These words explain the difficulty and the importance of protecting the U.S. infrastructure against terrorist attacks. The first step is identifying what to protect, because of the limited resources for any agency. That makes it necessary to prioritize assets so that the most important asset is protected first. In the case of terrorist threats, prioritizing assets is done based on the assets’ vulnerability and criticality.

This chapter provides an overview of the importance of assessing and prioritizing assets and implementing security measures for transportation assets. The research concentrates on assets maintained and operated by Indiana Department of Transportation (INDOT). The chapter also includes the problem statement, scope, objectives and approach for this research.

1.1. Background

A secure transportation system is critical to overall national security from terrorism. Groups or individuals motivated to terrorize or injure people or the economy often have transportation facilities as a target or a tool. Transportation activities comprise

12 percent of the gross domestic economy, and virtually all of the economy is dependent on a functioning transportation system. Disruption to any critical link in the transportation system may cause serious economic harm. Thus, securing the transportation system is a critical consideration in overall security planning.

Terrorists may be motivated to cause personal injury to concentrations of people or to strike at symbolic targets, many of which are a part of the transportation system. Examples are the Golden Gate Bridge and other high-profile transportation facilities. Terrorists need to deliver the people, munitions, explosives, biological agents, or other destructive elements in their acts of terrorism. Thus, transportation is also an element of the delivery of terror. Collectively, the transportation sector is intimately involved in the security of our society and, in many respects, will be a front-line area of focus in enhancing security.

The future of transportation will be very much influenced by security considerations (Polzin, 2003). Surface transportation in the United States is an extraordinarily large and complex system. It is responsible for the movement of vast numbers of passengers and vast quantities of freight. It includes many thousands of interdependent operators. The system's efficiency and convenience are essential to the strength of our economy, the security of our nation, and the quality of our lives.

Transportation agencies have taken steps to increase the security of their assets. Two important references are AASHTO's "Guidelines for Vulnerability Assessment of Critical Infrastructure (2002)" and "Guidelines for Emergency Response (2002)". These guides are based on the responses from 32 states to a USDOT survey. Based on the

responses and various levels of security measures implemented by DOTs in their states, AASTHO published these reports as preliminary guidelines for use by state DOTs.

Although efforts are being made to deal with emergency situations like natural hazards such as fires and hurricanes, less effort has been focused on preventing terrorist attacks. Prevention begins with identifying what needs to be protected. Thus, there is a need to identify critical assets in order to use resources to strengthen those assets that are most important.

This study presents methods used by different agencies to assess vulnerabilities. Also presented is a method developed specifically to address Indiana's needs and that can serve as a tool to identify critical assets for INDOT in their districts and statewide. Countermeasures are suggested to address the security needs for the assets identified as critical and vulnerable.

1.2. Problem Statement

Emergencies arising from terrorist threats highlight the need for transportation agencies to minimize the vulnerability of people and assets through incident prevention, preparedness, response, and recovery. Agencies are seeking to reduce the chances that transportation vehicles and facilities are targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. The awareness levels in all the spheres of government have heightened and efforts are being made across all areas to strengthen security. The activity involves agencies at federal, state and local levels, as well as academia and private organizations.

Transportation security has two aspects to it:

1. Evaluating the ability of a system or application, including current security procedures and controls, to withstand assault, which is vulnerability assessment, and
2. Developing procedures to ensure efficient response to a terrorist attack, which is emergency response.

Faced with threats to the security of the transportation system, there is an urgent need to develop systematic efforts to protect the physical well-being of users of transportation assets by reducing the vulnerability of critical transportation infrastructure and services. Despite this pressing need, there is limited experience with the qualitative or quantitative methods to identify vulnerabilities or the consequences of such disruptive attacks. (Srinivasan, 2004).

Although AASHTO developed guidelines to conduct vulnerability assessment, critical assets differ from state to state. It is necessary for INDOT to develop its own methods or adapt the AASHTO guidelines to suit its particular needs. The prevention part of transportation security begins with vulnerability assessment. “*Vulnerability describes the non-operability of the network under varying strenuous conditions (i.e., the susceptibility to fail to function)*”. (Husdal, 2004).

Identifying and evaluating how vulnerable and critical the assets are is a major challenge, given the subjective nature of the factors involved. There is a need to develop systematic methods to assess the vulnerability of existing and emerging infrastructure, reduce the occurrence of disruptive attacks and, if possible, prevent the terrorist attacks by strengthening assets. Selecting an asset from a statewide list of assets that have been identified at the local level is another challenging task. In order to help agencies apply their limited resources to secure their assets, this study focuses on identifying and

developing methods to prioritize assets based on their vulnerability and criticality level. This study also suggests several countermeasures appropriate for specific asset types.

1.3. Research Objectives and Scope

The objective of this project is to provide a flexible, transferable method to identify the vulnerability of assets and address transportation issues related to security from the perspective of prevention. The specific objectives of this research include:

- Determine the best practices available for vulnerability assessment of transportation assets.
- Determine whether accepted and usable methods exist for conducting vulnerability assessments on a statewide basis.
- Develop a methodology appropriate for INDOT, or adapt an existing methodology to suit Indiana's needs.
- Test the suggested methodology in INDOT districts.
- Develop a method to combine assets from various districts.
- Develop countermeasures to reduce the vulnerabilities of an asset.
- Develop recommendations for INDOT for conducting vulnerability assessments, based on the results obtained from case studies.

In conducting this study, we surveyed the seven INDOT districts in Indiana. Each district selected 25 critical assets. We developed a method to identify the vulnerabilities of the 175 assets. This phase of vulnerability assessment classifies which of the identified critical assets in each district are vulnerable. A method is developed to compare the asset lists from each district. Once the most critical and vulnerable assets are identified, more

refined vulnerability assessment at an asset level could be conducted using the AASHTO guidelines. Because the factors that affect vulnerability do not all have the same weights, the analytical hierarchical process is used to obtain the weights. General countermeasures are suggested, based on USDOT and Virginia DOT guidelines, which are appropriate for different asset types.

1.4. Organization of the Report

This report consists of five chapters. Chapter 1 discusses the motivation and the background for this research. Presented in Chapter 2 is the literature review, which discusses transportation issues with regards to security. Also, discussed in Chapter 2 are various methodologies available to assess the vulnerability and criticality of transportation assets. Chapter 2 also discusses the various multi-criteria decision methods available. Chapter 3 presents the framework for the development of vulnerability assessment methodology and the prioritization methods for selecting the assets from various districts. Chapter 4 discusses the results obtained from the surveys. Chapter 5 provides a set of recommendations to INDOT for conducting vulnerability assessment. Chapter 6 provides a summary of the results and the vulnerability assessment methodology developed. It also includes limitations of this approach and recommendations for future research.

CHAPTER 2. LITERATURE REVIEW

2.1. Overview of Transportation Security and Vulnerability Assessment

Transportation infrastructures make attractive targets for intentional harmful attacks—they are highly visible, carry large numbers of commuters, and are very accessible. Although research work on natural disasters and accidents is relevant, willful attacks pose some unique issues and challenges—primarily because these acts are intelligent, unpredictable, and deliberate in generating catastrophic consequences. Enhancing the security of our transportation system is one of the highest priorities of transportation agencies in the wake of September 11. Informed decisions regarding vulnerability assessment and emergency response are essential for secure and safe operation of highway assets.

The need to protect critical infrastructures, as well as information, people, equipment, facilities and operations, requires a comprehensive systematic evaluation of Vulnerability and Criticality to improve overall organizational security. This chapter provides a synthesis of transportation security issues. Also, this chapter summarizes the different methods that are available to conduct vulnerability assessments in various degrees of detail and for different assets. Various multi-criteria decisions suitable to the problem are also discussed.

2.2. Transportation and Security

The executive order issued by The White House (Executive Order, 1996) identifies certain national infrastructures so vital that their incapacitation or destruction would have a debilitating impact on the defense or economic security of the United States. Some of these critical infrastructures are telecommunications, electrical power systems, storage and transportation of gas and oil, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and stability and continuity of government. There are two types of threats possible: physical threats to tangible property and cyber threats. Cyber threats are in the nature of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures.

Prior to September 11, 2001, the majority of works published on the subject of transportation security were focused on protecting public surface transportation. A series of transportation security reports by the Mineta Transportation Institute (MTI) became some of the most read literature in the nation. Brian Michael Jenkins (Jenkins, 2001) wrote “Contemporary terrorists have made public transportation a new theatre of operations.” The best source of information, before and after September 11, 2001, dealing with methods and techniques for the protection of infrastructure can be found in the Army Field Manual (2001). Most of the countermeasures suggested in the AASHTO guidelines were based on this manual.

The major focus of the existing literature was found to be aviation security, mass transit security, and port security, which implies these modes are higher-order terrorist targets than highways because of their high visibility and high cost facilities. GAO (2003)

supports the findings of the other literature reviewed and indicates that efforts to strengthen transportation security face several long-term institutional challenges that include (1) developing a comprehensive risk management approach; (2) ensuring funding needs are identified and prioritized and that costs are controlled; (3) establishing effective coordination among the many responsible public and private entities; (4) ensuring adequate workforce competence and staffing levels; and (5) implementing security standards for transportation facilities, workers, and security equipment.

2.3. Components of Vulnerability Assessment

Assets can be defined as the infrastructure, facilities, equipment, information, and personnel that comprise each transportation system. Vulnerabilities in highway transportation generally fall into three categories:

1. Physical facilities.
2. The vehicles (private and commercial motor carriers) operating on the system.
3. The information infrastructure that monitors and manages the flow of goods, vehicles, and people on the highway system. (AASHTO, 2002).

The vulnerability assessment procedure is usually performed in stages that are similar to or a slight variation of the steps described below.

- Identifying critical assets to be assessed.
- Assessing vulnerabilities and criticality
- Assessing consequences
- Identifying countermeasures
- Estimating the cost of countermeasures

As part of this study on “synreport of best practices for transportation security”, a thorough literature review to determine the methodologies developed so far has been conducted. Then a methodology that could be used or tailored for use, by INDOT officials for identifying critical and vulnerable highway infrastructure projects on a statewide basis was developed. It was applied to INDOT’s seven districts.

2.4. Vulnerability Assessment Methodologies

A process is necessary for prioritizing all INDOT transportation assets with respect to their vulnerability in terms of their criticality and the ability to deter, deny, detect, delay, and defend against terrorist attacks. The U.S. Department of Homeland Security Office for Domestic Preparedness identified a need to examine and classify various types of vulnerability assessment methodologies, software, and tools that could be used by state and local governments to assess the vulnerabilities of their assets. Forty four methodologies were considered in the study. (DHS, 2003). In the wake of September 11, 2001, several good publications have been developed. One of the objectives of this research is to synthesize the best practices of transportation security relating to vulnerability assessment (VA). The relevant methodologies for VA are discussed below.

2.4.1. AASHTO Methodology

As a part of the efforts to improve surface transportation security, NCHRP-funded projects were performed for the American Association of State Highway and Transportation Officials (AASHTO) Security Task Force. Two guidelines were

developed and distributed to member states in May 2002. The two guidelines address (1) vulnerability assessment and (2) highway emergency response plans, which will be discussed later in this report. These reports give a general overview of the framework to conduct vulnerability assessment of transportation assets in the states. (AASHTO, 2003). The vulnerability assessment guide is discussed at some length, because these guidelines are the primary basis for this study.

“A Guide to Highway Vulnerability Assessment for Critical Asset Identification and protection” (AASHTO, 2002) was prepared under the direction of the National Cooperative Highway Research Program (NCHRP) for American Association of State Highway and Transportation Officials (AASHTO). The AASHTO guide addresses our nation’s vulnerability assessment needs for highway transportation subsequent to the terrorist attacks of September 11th, 2001. A terrorist attack against the nation’s highway infrastructure could result in many injuries and fatalities, the disruption of vehicular traffic and commerce, and significant regional or national economic losses. The intent of the AASHTO Task Force was to discover what is being done or is under development in selected states and to provide “best practices” in the form of a guide or handbook that state DOTs may use to prepare for and respond to future acts of terrorism.

The AASHTO guide deals with physical highway transportation assets, such as bridges, tunnels, roadways, interchanges, toll houses, and roadside infrastructure (e.g., signs, barriers, sensors).

The AASHTO ‘Guide for Vulnerability Assessment’ was developed as a tool for State Departments of Transportation (DOTs) to:

- Assess the vulnerabilities of their physical assets, such as bridges, tunnels, roadways, and inspection and traffic operation facilities.
- Develop possible countermeasures to deter or detect and delay the consequences of terrorist threats to such assets;
- Estimate the capital and operating costs of such countermeasures; and
- Improve security operational planning for better protection against future acts of terrorism.

The AASHTO vulnerability assessment guide can benefit

- State DOTs, including senior officials involved in the initial planning state of the vulnerability assessment process.
- Mid-level managers charged with developing assessment plans and procedures
- Field personnel who will likely conduct the assessment of critical assets.

The AASHTO vulnerability assessment guide can be used as a basic framework to build and plan the complete vulnerability assessment of state assets. The guide recommends that state DOTs organize and manage a multidisciplinary team whose members must possess a working knowledge of department's mission, its critical assets, and its policies, plans and procedures. The AASHTO vulnerability assessment guide also identifies the activities typically required by the team to conduct vulnerability assessment. The vulnerability assessment process presented in this guide is derived from a careful review of information compiled from state, federal, and international agencies and their personnel. The guide provides six steps for conducting a vulnerability assessment of highway transportation assets. They are shown in Figure 1.

Figure 1. Six steps for conducting vulnerability assessment (AASHTO, 2002)

The six steps represent an integrated and iterative approach to vulnerability assessment. These six steps provide a straightforward method for examining critical assets and identifying cost effective countermeasures to guard against terrorism. For each step, the objective is clearly stated, the practice of that step by the other state and federal agencies is referenced, a detailed approach is described, and illustrative examples are provided in the guide. The criteria used in selecting preferred approaches include availability, accessibility, transparency, replicability, reasonableness, scalability, robustness, cost effectiveness, and modularity.

Given that the information on threats, vulnerabilities and consequences will probably come from sources external to the state DOT, the multidisciplinary team will need to either include or frequently interact with the state or local organizations representing law enforcement, fire services, public safety, public health, and emergency management. To address the issues and to ensure the team is well equipped to proceed with the assessment procedures, training exercises should be held prior to vulnerability assessment.

Phases of vulnerability assessment according to AASHTO guidelines:

In the first phase (pre-assessment), the department assembles the assessment team, conducts team training exercises, makes contact with external organizations, plans and schedules the vulnerability assessment process, and collects the required resources.

In the second phase (assessment), the team conducts the vulnerability assessment by making use of the available data sources, physically examining critical assets, interviewing personnel, assessing the data, and making recommendations on countermeasures.

In the third phase (post-assessment), the department, working with the team, develops a strategy for implementing the recommended countermeasures. Activities in this phase may include cost-benefit analyses, trade-off studies, and procuring equipment and services.

The AASHTO vulnerability assessment guide describes general methods that apply to a wide range of asset types. The vulnerability assessment methods in the guide are applicable to any state DOT once they are modified.

2.4.2. Federal Transit Agency Method

Federal Transit Administration (FTA, 2003) proposed a model that prioritizes system factors, so that transit systems may more effectively ensure the security of its assets. The FTA method aims at identifying the critical assets with respect to transit systems. The process of selecting anti-terrorism measures evaluates potential threats, the consequences of those threats, and the techniques available to mitigate them. This framework is presented in Figure 2 and has five steps:

- asset criticality;
- threat evaluation;
- vulnerability assessment;
- countermeasure investigation; and
- security measure selection.

Figure 2 Risk Assessment Process

Identify asset criticality: The structured management of overall security risks begins with an understanding of the relative criticality and value of the transportation system's assets. In this method, the prioritization approach includes Criticality

Assessments and Critical Factor Evaluations. In deciding which assets or categories of assets have the greatest impact if lost, damaged, or disrupted, two different approaches were considered: critical factor evaluation approach and check-list based assessment.

These approaches vary primarily based on the presence of passengers and employees and the use of the asset by outside responders, such as emergency responders and the US military. These two approaches are also applied based on similarities between and among classes of transportation assets.

For transportation systems, such as public transit, the General Accounting Office (GAO), in its 1988 assessment of the vulnerability of public transportation to acts of terrorism and extreme violence, entitled Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems developed a useful analytical tool to prioritize critical assets. This tool assesses the criticality of each transit asset according to the impact of its disruption on people (either the public or employees) and the ability of the system to function (GAO, 1988)

In the critical factor evaluation approach, each asset, or category of asset, must be identified, and then using a relative or quantitative scale, evaluated for the impacts its loss would have on passengers, employees and system functioning during different times of day (peak and off-peak service). Impacts can be measured in terms of the number of passengers and employees present in a given location within an asset who could be affected, as well as the cost of replacing the lost asset, including all indirect costs, such temporary services required until the asset is rebuilt, liability and workers compensation claims, and changes in insurance coverage. Each transit system must assign its own values for ranking impacts, based on its experience and available information.

The GAO recommends the use of high, medium, and low categorizations. Based on this model, Table 1 below presents the results of analysis performed concerning the criticality of generic bus assets. The results of the analysis shows public transportation systems can identify single assets and categories of assets whose loss would potentially result in high casualties or system disruption.

Table 1. Analysis of Criticality of Bus Assets (FTA, 2003)

Bus Transportation Assets	Criticality (Level of Impact)	
Assets	People	System
Terminal/Station	High ¹	Medium to High ²
<ul style="list-style-type: none"> Entrances and exits 	High ¹	Low ²
<ul style="list-style-type: none"> Escalators/elevators/stairs 	High ¹	Low ²
<ul style="list-style-type: none"> Corridors/pathways 	Medium ¹	Low ²
<ul style="list-style-type: none"> Mezzanines and concourses 	High ¹	Low ²
<ul style="list-style-type: none"> Passenger loading and unloading 	High ¹	Medium ²
<ul style="list-style-type: none"> Vendors 	High ¹	Low ²
<ul style="list-style-type: none"> Restrooms 	Medium	Low ²
<ul style="list-style-type: none"> Support facilities and storage 	Low ¹	Medium to High ²
<ul style="list-style-type: none"> Administrative/employee 	Medium to High ¹	Medium to

• facilities		High ³
Transit Center	High ¹	Low ²
• Entrances and exits	Medium to High ¹	Low ²
• Passenger waiting areas	Medium to High ¹	Low ²
• Restrooms	Medium ¹	Low ²
• Passenger loading and unloading	Medium to High ¹	Low ²
• Vendors	Medium ¹	Low ²
• Support facilities	Low ¹	Low ²
Multi-use/intermodal connection	High ¹	Low to Medium ²
Bus stops and shelters	Medium to High ¹	Low
Vehicles (buses and vans)	Medium to High	Low
Roadways	Low	Low
High Occupancy Vehicle (HOV) lanes	Low	Low to Medium
ITS technology and equipment	Low	Low to Medium
Parking lots	Low to Medium	Low
Bus garages and storage facilities	Low ³	High
Heavy repair facilities	Low ³	Medium to High
Service and inspection facilities	Low ³	Medium to High
Inventory and storage facilities	Low ³	Medium
Alternative fuel facilities	Low ³	High

Operations control center	Low ³	High
Communications system	Low ³	Medium to High
Revenue collection facilities	Low ³	Medium
Administrative facilities	Medium to High ³	Medium to High
Employee parking lots	Low to Medium ³	Low
Transit police facilities	Medium to High ³	Medium to High
¹ Depends on what time of day incident occurs. Greater impact would be experienced during rush hour than non-rush hours. ² Depends on location in the system where an incident occurs. An incident at a major transfer center or station would have greater impact than one at an outlying bus stop. Also depends on the alternatives available, such as redundancies, rerouting capabilities, and other factors. ³ Affects employees only.		

FHWA developed an assessment methodology that uses critical asset factors to prioritize assets (AASHTO, 2002). For example, the factor ‘Ability to provide protection’ has a value of 1. The factors and associated values can be obtained from the AASHTO guide. Each of the factors is given a default value. The assignment of these factor values to assets is binary. If the critical asset factor applies to the asset being evaluated, then the asset receives the full value assigned to that factor. However, if the factor does not apply, the asset is assigned a value of 0 for that factor. For each asset, the applicable critical asset factor value is assigned. The sum of these values represents asset’s total score, which can be used to prioritize assets.

The selected items that form the prioritized critical asset list can then be assessed to determine threats, vulnerabilities, consequences, and ultimately, security measures. The threat assessment process emphasizes five factors used in the collection and analysis of information from all sources bearing on terrorist threats. The factors are: existence, capability, history, intentions and targeting. An example of the threat analysis factors is shown in Figure 3.

Figure 3. Threat Assessment Process

Vulnerabilities largely determine the likelihood that a potential adversary will succeed in damaging, disrupting, or destroying a prioritized critical asset. Two approaches presented in this report are scenario-based assessment and checklist-based assessment.

The scenario-based approach uses threat scenarios based on threat evaluation for prioritized critical assets, and then to attempt to determine how well existing measures identify, mitigate, or support response to each scenario. Table 2 below provides sample scenarios used in bus transportation to support these assessments.

Table 2. Relevant Bus Scenarios (FTA, 2003)

Bus Assets	Threats
Bus stations and/or terminals	<ul style="list-style-type: none"> π High-yield vehicle bomb near station π Lower-yield explosive device in station π Armed hijacking, hostage, or barricade situation in station π Chemical, biological, and nuclear release in station π Secondary explosive device directed at emergency responders
Bus vehicles	<ul style="list-style-type: none"> π Explosives placed on or under bus π Improvised explosive device (pipe or fire bomb) on bus π Chemical, biological, or nuclear release on bus π Armed assault, hostage, or barricade situation on bus π Secondary explosive device directed at emergency responders
Fuel storage facilities	<ul style="list-style-type: none"> π Explosives detonated in or near fuel farm/facilities
Command Control Center	<ul style="list-style-type: none"> π Physical or information attack on bus communications system π Armed assault, hostage, or barricade situation π Explosive device near or in control center

In the checklist-based assessment, vulnerabilities are uncovered by making a systematic survey of the security elements that provide protection to prioritized critical assets from evaluated threats. In this process, security relies on the “defense in depth” concept, where different rings of protection are identified, as appropriate for a specific facility or category of facilities. Survey questions direct a detailed walk-through and evaluation of each prioritized critical asset. The survey questions are based on agency experience and previously developed checklists prepared by the US military, the Federal Aviation Administration, the Department of Justice, other transportation systems, and consultants. Countermeasures considered applicable to protecting transportation assets are often identified in terms of their capabilities to deter, detect, and delay threats.

2.4.3. TMC Risk Assessment Methodology

The TMC Risk Assessment Methodology (SAIC, 2005) is based on best practices of several proven risk assessment methodologies. The approach used is drawn from the Systematic Assessment of Facility Risk (SAFR) and a methodology developed by the Department of Homeland Security (DHS) Office of Domestic Preparedness toolkit along with ideas from AASHTO’s *Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. The TMC Risk Assessment Methodology (TMC RAM) components include: asset identification; threat assessment; consequence assessment; vulnerability assessment; and countermeasure development.

The components of the TMC RAM process are:

- Asset identification
- Threat Assessment

- Consequence assessment
- Vulnerability assessment
- Countermeasure development.

The TMC RAM evaluates relative risk to multiple assets. Relative Risk (“RR”) is a function of the overall threat to the asset or facility (Threat, or “T”), the attractiveness of a particular target to a given adversary (Target Attractiveness, or “TA”), the potential consequences of a successful attack on a target (Consequences, or “C”), the ability to deter an adversary from attempting an attack (Deterrence, or “LD,” expressed in terms of the inability to deter, or “1-LD”), and the effectiveness of the system to prevent an attack should one be attempted (System Effectiveness, or “LS,” expressed in terms of system ineffectiveness, or “1-LS”).

The formula is expressed as:

$$RR = TA \times T \times C \times (1-LD) \times (1-LS) \quad (2.1)$$

Calculating the relative risk to one asset has limited value; it only indicates the risk to that asset relative to the highest and lowest possible RR.

In order to limit the asset list to only those critical to the mission, it is recommended that assets be identified based on an examination of the overall mission of the TMC, the functions that support that mission, and the assets critical to continuation of those functions.

A number of factors go into a terrorist’s decision to attack a target, or increase the magnitude of potential adversaries interested in striking at a particular target.

-Knowledge that target exists.

-Availability of information about the site and security

- *Symbolic importance*
- *Publicity generated by attack attempt or success*
- *Mass casualty potential*
- *Perceived criticality of systems*
- *Potential economic disruption*
- *Public confidence*
- *Level of effort*

The vulnerability assessment begins with development and documentation of a scenario to facilitate the discussion of system effectiveness. The consequences associated with an aggressor act can be described in a myriad of ways. In some cases the dollar value of resources lost, stolen, damaged or destroyed as well as the cost of repair, replacement, or substitution have provided analysts with a method for assessing consequences. The variables that are used to assess consequences in this manual are consistent with the results of a successful aggressor act, and include:

- Fatalities/Casualties – Dead and injured as a result of the event.
- Mission Downtime/Degradation – Time the facility is unable to continue operation at full capacity or at all.
- Economic Impact – Direct economic impact on the facility to repair or replace (not including lawsuits, etc.).
- Downstream Effects – The extent of the downstream impact on the transportation system.

2.4.4. TMC Risk Assessment Method

Xia et al. (2004) in their study proposed a framework that uses continuous traffic monitoring data in addition to the static infrastructure characteristics. A set of indices are developed to indicate the risk level of each component.

1. Index A reflects the static characteristics of highway components against a terrorist attack. The characteristics include structural stability, number of alternatives, and response resources of highway components.

2. Index B incorporates the dynamic characteristics of a highway's network components that could affect its risk. They include dynamic traffic flow information such as volume, speed, occupancy, vehicle classification, and queue length. Furthermore, weather information and work zone activities can be included.

3. Index C represents the potential of a terrorism attempt. It is the possibility of an attack occurrence, which is estimated in terms of both functional significance and symbolic importance of a highway component.

Thus, the risk score of a highway component can be defined as a linear combination of the three indices.

$$R = (\alpha A + \beta B) * C / 100 \quad (2.2)$$

In which,

R: risk score of highway network component

A: static characteristic index

B: dynamic characteristic index

C: attack potential index

α : weight of static characteristic index

β : weight of dynamic characteristic index

The values for parameters α and β can be determined through a structured decision-making process. All indices in this study are assumed to be independent. Also, all attributes in each index, to be discussed below, are assumed to be independent.

The score of index A can be calculated using the following equation.

$$A = W_{A1} * a + W_{A2} * b + W_{A3} * c + W_{A4} * d \quad (2.3)$$

The score of index B can be calculated using the following equation.

$$B = W_{B1} * e + W_{B2} * f + W_{B3} * g + W_{B4} * h + W_{B5} * i \quad (2.4)$$

where W's are the weights predetermined with the help of the experts.

The probability of a terrorism attempt mainly can be measured by symbolic importance and functional classes. Let j and k represent the attributes of functional types and symbolic importance, respectively.

The score of index C can be calculated as follows.

$$C = W_{c1} * j + W_{c2} * k \quad (2.5)$$

2.4.5. Comparison of Vulnerability Assessment Methodologies

The above three approaches aim at achieving similar objectives of identifying critical assets and evaluating their vulnerabilities. These assets help in prioritizing assets when the assessment is conducted at an asset level, where each asset is evaluated for each of the mentioned criteria. None of the approaches deal with a system-level statewide network nor provide an easy way to pick those assets that need immediate attention. This

aspect is crucial because of the limited nature of the funds available to any agency. The TMC RAM method, although comprehensive, has extensive data needs. It is a good model theoretically but it requires a lot of effort on the part of the experts to quantify the value of subjective criteria like the value of the lives lost. Because the values for these subjective criteria are predictions based on one's knowledge and expertise, there could be inconsistency and variance.

The AASHTO methodology, on the other hand, is more subjective and uses surveys to obtain data. In addition, the approaches differ in terms of the identification and evaluation criteria used to assess vulnerability and criticality. TMC RAM evaluates vulnerability and criticality in terms of relative risk and target attractiveness where as AASHTO follows a slightly different approach by using factors such as visibility, accessibility, and economic impacts. Once the final list of critical assets is formulated, any of the above approaches could be used to conduct in-depth vulnerability assessment depending on the nature of the data available.

2.5. Other VA Methodologies used by States and Agencies

2.5.1. Iowa Plans for Critical Asset Protection

The main features of the plan are

- Quantify 12 individual elements of potential critical assets. Eight elements address criticality (static over time) of the asset, while four address vulnerability, which is dynamic and influenced by changing threat levels and implementation of measures.

- Iowa identified about 12,000 assets. Few of the 12,000 assets are critical assets. Out of the critical assets, 93% are not public owned.
- Protective measures for the critical assets are monitored by homeland security monitoring system, so they can be activated at the most appropriate threat level.
- Iowa plans for critical asset protection has a multi-hazard approach. The plans take into account natural hazards like fire, earthquakes, hurricanes, not just terrorism.
- Iowa State DOT is developing an interdependency model. No asset is isolated and independent.

Contact: Larry Brennan (IT Department, Iowa DOT), A J Mumm (Iowa Emergency Management Division)

2.5.2. Transportation Security Activities in Texas

Rummel et al. (2003) uses a two-step process to rank critical bridges across the State of Texas. The first step is an automated ranking of all the bridges listed in the National Bridge Inventory (NBI) for the state. This ranking is accomplished through the use a Microsoft Access program using the Texas Bridge Criticality Formula given below.

TEXAS BRIDGE CRITICALITY FORMULA-The following equation represents Texas' formula for ranking bridge criticality.

$$\begin{aligned} \text{Criticality Index} = & \{((\text{Truck ADT} \times \text{Truck ADT Factor} / \text{Max. Truck ADT}) + (\text{ADT} \times \\ & \text{ADT Factor} / \text{Max. ADT}) + (\text{Detour} \times \text{ADT} \times \text{Detour Factor} / \text{Max. Detour} \times \text{Max.} \\ & \text{ADT}) + (\text{Intersect Rt. ADT} \times \text{Intersect Rt. Factor} / \text{Max. Intersect Rt. ADT}) + \\ & (\text{Interstate Intersection} \times \text{Interstate Intersection Factor}) + (\text{Navigation Importance} \times \end{aligned}$$

$$\text{Navigation Factor}) + (\text{International Importance} \times \text{International Factor}) + (\text{Military Importance} \times \text{Military Factor})) / 8\} \times \text{Replacement Factor} \quad (2.6)$$

The formula accounts for several criteria that are measured using data available from the National Bridge Inspection database that can be downloaded to the Access program. The criteria incorporated into the formula were those items TxDOT considered important, based, in part, upon the responses to an AASHTO/TRB Task Force survey that helped define and prioritize these criteria. The criteria included the economic impact due to disruption of commerce by using the international factor, truck AADT, detour, etc. General passenger transportation needs and risks to public safety were also considered. The quantitative analysis of these factors can be obtained from the paper. This methodology is less subjective. However, it is specific to one type of assets, namely, bridges.

2.5.3. TMSARM Vulnerability Self Assessment Tool

The Transportation Security Agency (TSA) self-assessment tool guides a user through a series of security-related questions in order to develop a comprehensive security baseline of a transportation entity. The user is then prompted to assess the baseline security system effectiveness in response to specific threat scenarios. The effectiveness is then reassessed based upon the addition of countermeasures in response to conditions of heightened threat. This tool has restricted access and is available only to certain companies and agencies. TSA intends to develop TSARM modules specific to transportation modes. TSA currently has deployed a self-assessment module in support of targets such as maritime vessel and facility categories and is planning to extend it to other modes of transportation.

2.5.4. Blue Ribbon Panel Approach for Bridge VA

In order to provide guidance to bridge owners, the Federal Highway Administrator appointed members to the Blue Ribbon Panel (BRP, 2003) on bridge and tunnel security. The panel's objective was to apply its collective experience and knowledge about structural design, structural integrity, and environmental stress and strain to new ways of examining how critical bridges and tunnels can be protected against potential terrorist attacks

The large number of bridges (600,000) and tunnels (500) in the US requires a two-tiered approach: prioritization and risk assessment. The first tier, prioritization, is typically most efficiently done in two steps. The first step is a data-driven approach, such as that used by the Texas Department of Transportation (Rummel et al., 2003), for ranking bridges using common criteria. The National Bridge Inventory (NBI) provides much of the data needed for this step. In the second step of prioritization, additional data comes from owners and operators familiar with specific characteristics of the facilities and the services they provide. In this first tier ranking, prioritization of bridges and tunnels is based on characteristics such as the following:

- Potential for mass casualty based on Average Daily Traffic (ADT) and associated peak occupancies
- Criticality to emergency evacuation and response to emergencies
- Military or defense mobilization
- Alternative routes with adequate available capacity

- Potential for extensive media exposure and public reaction; symbolic value (to what extent does the facility represent ideals and values that are important to the American public, also visual symbolism, e.g., "signature bridges")
- Mixed-use bridges and tunnels where highway and rail are co-located
- Potential for collateral damage (land, marine, rail), including collateral property and utilities
- Maximum single span length as it relates to the time required to replace the facility
- Commercial vehicle vs. passenger vehicle mix and volume as a surrogate for economic impact
- Bridge or tunnel dimensions (as a surrogate for replacement time/cost)
- Significance of revenue streams (e.g., tolls, fares) associated with the facility
- Bridges and tunnels at international border crossings

The second tier is a risk assessment of high priority bridges taken from the first tier (prioritization) to determine vulnerabilities and evaluate countermeasures to deter attack and/or mitigate damages. The risk, R , to the facility is determined following an approach similar to that developed for seismic retrofit and can be expressed as follows:

$$R = O \times V \times I \quad (2.7)$$

where,

O = Occurrence: This factor is hazard oriented and will change with the nature of the hazard. In the context of the report, the occurrence factor approximates the *likelihood* that terrorists will attack the asset. It includes target attractiveness (from the perspective of the threat), level of security, access to the site, publicity if attacked, and the number of prior threats. Input into this factor typically comes from the law enforcement and intelligence communities' familiar with threat and operational security measures.

V = Vulnerability: Vulnerability is an indication of how much the facility or population would be *damaged or destroyed* based on the structural response to a particular hazard. In the context of the report, vulnerability is the likely damage resulting from various terrorist threats (weapon type and location). It is a measure of expected damage, outcome of the event, expected casualties, and loss of use, all features of the facility itself. Input for this factor typically comes from engineering analysis and expertise.

I = Importance: Importance is a characteristic of the facility, not the hazard. Importance is an indication of *consequences* to the region or nation in the event the facility is destroyed or unavailable. Is the facility on an evacuation or military mobilization route; is it likely to be used by first responders to emergencies; what is its historic and associated significance; what is its peak occupancy? Input for this factor typically comes from owners, operators, users, and beneficiaries of the facilities, often governmental sources, and will use factors similar to those used in the first tier prioritization.

The formula for R properly expresses the interaction among the three factors. Dominant factors magnify risk; negligible factors diminish it. Other formulas, such as models that add the factors, fail to account for their interactive effects. For example, in the absence of a threat ($O'=\emptyset$), the risk should be zero as this model provides; additive models would have a residual risk. In the multiplicative model, eliminating any one factor to zero (or near zero) reduces the risk to near zero (e.g., low importance leads to low risk regardless of other factors).

2.5.5. Sandia National Lab Community Vulnerability Assessment Methodology (VAM)
This methodology was developed as a prototype for the Chemical Facility Vulnerability Assessment Project and lays the foundation for a computer-based vulnerability assessment tool. Sandia National Laboratories has a Dams Security Assessment Methodology, Water Supply and Treatment VAM, Vulnerability Analyses and Security Design Reviews for Correctional Facilities, as well as the VAM-CF. This methodology is applicable to all mission/sector categories, in addition to Education, Recreation Venues (parks, museums, tourist attractions, etc.), Emergency Facilities, Foreign-represented Governments (Embassies, residences, businesses, etc.), and special categories, such as abortion clinics and religious facilities.

2.6. Multi Criteria Decision Methods

Multi Criteria Decision Analysis (MCDA) is a procedure aimed at supporting decision maker(s) whose problem involves numerous and perhaps conflicting interpretations. (Figueria, 2005). A multi-criteria decision problem generally involves choosing one of a

number of alternatives based on how well those alternatives rate against a chosen set of criteria. The criteria themselves are weighted in terms of importance to the decision maker, and the overall “score” of an alternative is the weighted sum of its rating against each criteria. The ordering of the alternatives by the decision scores is taken as the ranking of the alternatives based on the participant’s input. MCDA aims at highlighting the conflicts in the decision process between people and deriving a way to come to a compromise in a transparent process. When MCDA involves a certain element of subjectivity, the values of the researcher implementing MCDA play a significant part in the validity of the outcome of the MCDA process. The most appropriate MCDA method depends on the problem at hand and may to some extent depend on which model the decision maker is most comfortable with. The intent of MCDM (Multi Criteria Decision Methods) is to improve the quality of the decisions involving multiple criteria by making choices more explicit, rational, and efficient.

MCDM has six functions that support this goal (Hobbs, 2000):

1. To structure the decision process.
2. To show trade-offs among criteria.
3. To help people reflect upon, articulate, and apply vague judgments concerning acceptable trade-offs, resulting in recommendations concerning alternatives (Stewart, 1992).
4. To help people make more consistent and rational evaluations of risk and uncertainty.

5. To facilitate negotiation between the stakeholders. Giving a mathematical structure to a subjective problem will help in corroborating the claim during negotiations.
6. To document how decisions are made.

There are three steps in utilizing any decision-making technique involving numerical analysis of alternatives:

1. Determine relevant criteria and alternatives.
2. Attach numerical measures to the relative importance of the criteria and to the impacts of alternatives on these criteria.
3. Process the numerical values to determine a ranking of each alternative.

The following are some MCDM models for obtaining weights and ranking alternatives:

2.6.1. The WSM Method

The Weighted Sum Model (WSM) is probably the most commonly used approach, especially for single-dimension problems. If there are m alternatives and n criteria, then the best alternative is the one that satisfies (in the maximization case) the following expression.(Fishburn,1967)

$$A^*_{WSM-Score} = \max_i \sum_{j=1}^n a_{ij} w_j, \quad \text{for } i=1, 2, 3, \dots, m \quad (2.8)$$

where $A^*_{WSM-Score}$ is the WSM score of the best alternative, n is the number of decision criteria, a_{ij} is the value of the i -th alternative in terms of the j -th criterion, and w_j is the weight of j -th criterion.

This model is based on the additive utility assumption (Fishburn, 1967), which says that the total value of each alternative is equal to the sum of the product given in the Equation 2.8.

2.6.2. The WPM Method

The Weighted Product Model (WPM) is similar to WSM. The main difference is that, instead of adding the values and the weights as in WSM, the ratios of the values (a_{ij}) are multiplied. Each alternative is compared with the others by multiplying a number of ratios, one for each criterion. Each ratio is raised to the power equivalent to the relative weight of the respective criterion. (Miller, 1969) In order to compare two alternatives, A_k and A_l , the following product has to be calculated:

$$R(A_k / A_l) = \prod_{j=1}^n (a_{kj} / a_{lj})^{w_j} \quad (2.9)$$

where n is the number of criteria, a_{ij} is the value of the i -th alternative in terms of the j -th criterion, and w_j is the weight of the importance of the j -th criterion.

If the term $R(A_k / A_l)$ is greater than or equal to one, then it indicates that alternative A_k is more desirable than alternative A_l . The best alternative is the one that is better than or at least equal to all alternatives. The advantage of this method is it can be applied

independently of the units of measure, because the method uses ratios instead of actual values.

2.6.3. The AHP Method

The Analytic Hierarchy Process (AHP) decomposes a complex MCDM problem into a system of hierarchies. AHP is used to estimate the weights for the different factors effecting vulnerability and criticality in this research. (Saaty, 2000). The application of the AHP approach explicitly recognizes and incorporates the knowledge and expertise of the participants in the priority setting process by making use of their subjective judgments. The importance of AHP, its variants, and the use of pairwise comparisons in decision making is best illustrated in Saaty (2000). The use of AHP is discussed in Chapter 3. The final step in the AHP deals with the structure of an $m \times n$ matrix, where m is the number of alternatives and n is the number of criteria. The matrix is constructed by using the relative importances of alternatives in terms of each criterion. The vector $(a_{i1}, a_{i2}, a_{i3}, \dots, a_{in})$ for each i is the principal eigenvector of an $n \times n$ reciprocal matrix that is determined by pairwise comparisons of the impact of m alternatives on the i -th criterion. The process is shown in Chapter 3. Once the a_{ij} 's for each alternative with respect to each criteria are obtained in the $m \times n$ matrix, the best alternative is indicated by Equation 2.10.

$$A^*_{AHP-Score} = \max_i \sum_{j=1}^n a_{ij} w_j, \text{ for } i = 1, 2, 3, \dots, m \quad (2.10)$$

This step of AHP is similar to the WSM method (Section 2.6.1), the difference being AHP uses relative values instead of absolute ones. AHP can be used in a single- or multi-dimensional decision making processes.

2.6.4. The ELECTRE Method

The ELECTRE method (for Elimination and Choice Translating Reality) (Triantaphyllou, 2000) deals with “outranking relations” by using pairwise comparisons among alternatives under each one of the criteria separately. The outranking relationship of two alternatives A_i and A_j , denoted as $A_i \rightarrow A_j$, describes that even when the i -th alternative does not dominate the j -th alternative quantitatively, then the decision maker may still take the risk of regarding A_i as almost surely better than A_j . The ELECTRE method has had limited acceptance by the scientific and practitioner communities. Alternatives are said to be dominated if another alternative is better than they are in terms of one or more criteria and equal in the remaining criteria.

Two important concepts underscore the ELECTRE approach: thresholds and outranking. (Triantaphyllou, 2000) Assume that there exist defined criteria, $g(j)$, $j=1,2,\dots,r$ and a set of alternatives, A . Traditional preference modeling assumes the following three relations hold for two alternatives $(a, b) \in A$:

aPb (a is preferred to b), $g(a) > g(b)$

aIb (a is indifferent to b), $g(a) = g(b)$

aJb (a cannot be compared to b)

If, for example, you have two cups of tea - one has 10 mg of sugar and the other has 11 mg of sugar - could you tell the difference? Traditional preference modeling says that,

because the amount of sugar is not equal, then one will be preferred over the other. In contrast to the traditional approach, ELECTRE introduces the concept of indifference threshold, q , and the preference relationships are redefined as follows:

aPb (a is preferred to b) $g(a) > g(b) + q$

aIb (a is indifferent to b) $|g(a) - g(b)| \leq q$, and

aJb (a cannot be compared to b) remains.

The ELECTRE method begins with pairwise comparisons of alternatives under each criterion. The indifference threshold varies with the decision maker and cannot be clearly specified. There is a point at which the decision maker changes from indifference to strict preference, although this point may not always be clearly defined. The set of binary or pairwise relations of alternatives are called outranking relations. Through the consecutive assessments of outranking relations of the alternatives, the ELECTRE method elicits the concordance index, defined as the amount of evidence to support the conclusion that one alternative outranks or dominates another alternative. The discordance index is the counterpart of the concordance index. This method is convenient when a large number of alternatives are involved and a few criteria.

2.6.5. Resolving Conflicts

Few of the MCDM methods yield completely consistent results. If more than one MCDA method is used for an application, different methods generally lead to diverse results. (Hobbs, 2000) Different participants arrive at different results. Also, a participant applying the method at different times may come up with dissimilar results. One of the ways to resolve this issue is to expose members of the group to each other's views. Often,

a search for consensus will establish at least some common ground. Areas of agreement and disagreement need to be identified by comparing rank orders chosen by different people. (Hobbs, 2000) Are there any options that are ranked in the top three by every person? Are there alternatives that are not ranked first, second, or third by any person? If there is little consensus, then the problem can be broken down to two or more perspectives and dealt with separately. The successive elimination method could be used to delete options that are not found best under any set of weights between those alternatives selected by the participants. Hamalainen et al. (1999) suggest that cluster analysis or factor analysis could be used to define a few distinct set of weights or rank orders of options that summarize the positions of various experts. For MCDM methods to be useful, the group must have sufficient time and clear, consistent perspectives about the problem to provide thoughtful responses.

2.7. Fuzzy Logic

Zadeh (1965) proposed fuzzy set theory as the means for quantifying the inherent fuzziness that is present in ill-posed problems, which are a majority of real-life problems. Fuzziness is found in many of our decisions, in the way we process information, and, particularly in our thinking. Fuzziness stems from different perceptions or interpretations we give to such phases as “later” and “high temperature”. Fuzzy logic is used when either the data or the background knowledge of the data is riddled with vague concepts and judgmental rules. (Triantaphyllou, 2000) The most critical step in the application of fuzzy set theory is to effectively estimate the pertinent data or the membership function. If x is the number of vehicles in a queue, “small” may be considered as a particular value

of the fuzzy variable “queue”, and each x is assigned a number in the range from zero to infinity, $\mu_{\text{small}}(x) \in (0, \alpha)$, that indicates the extent to which that x is considered to be small; $\mu_{\text{small}}(x) \in (0, \alpha)$ is called a membership function. In fuzzy logic, the values are not crisp and the fuzziness of the values exhibits a distribution described by the membership function. Consider min-max fuzzy logic. If we consider union or OR, the outcome is equal to the input variable with the greatest value, $\max(x_1, x_2, x_3, \dots, x_n)$. If $A = 0.5$, $B = 0.7$ and $C = A \text{ OR } B$, then $C = \max(0.5, 0.7) = 0.7$. In most fuzzy problems, the rules are generated based on past experience. Because every step in the VA process involves uncertainty, fuzzy logic could be used to incorporate the uncertainty and subjectivity into the VA process.

2.8. Neural Networks

Neural networks, inspired by models of the human brain, have significant potential for solving complex real-life problems. An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information. It is composed of a large number of highly interconnected processing elements (neurones) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process. (Stergiou, 1999) Neural networks, with their remarkable ability to derive meaning from complicated or imprecise data, can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques. A trained neural network can be thought of as an "expert" in the category of information it has been

given to analyse. This expert can then be used to provide projections, given new situations of interest, and answer "what if" questions.

One of first projects of risk assessment that used neural networks is in the area of internal audit called auditMASTERPLAN. (Burger, M. S., 1998) The purpose of the risk assessment was to determine a hierarchical risk ranking for a population made up of 600 auditable units. The original risk model included nineteen risk variables, such as asset liquidity, degree of computerization, and existence of internal control systems. Based on audit experience, variables were assigned an attribute from 1 to 10 to represent the institutional impact of the risk related to each variable. The first step in building a neural network application to replicate the risk assessment results was to develop a data set for the neural network to use in training itself. A database containing the nineteen attribute values based on the relative ranking of the variable's characteristics and the results from auditMASTERPLAN was built using a spreadsheet format. During the training process, a large number of such examples are learned by the neural network model, which then enables it to perform quite well on previously unseen problems. Three different commercial neural network products were selected to test the feasibility of using neural network tools for this purpose. Because VA is an iterative process, neural networks could be used to train the system to make decisions about the vulnerability and criticality of the assets. The system could be trained initially using the input from the experts.

2.9. Need for this Study

Many organizations and agencies have conducted risk, threat, and vulnerability assessments to keep their systems safe and secure. Although there are numerous commercial and government methodologies in use today, currently no single method has

become standard for the vulnerability assessment at the statewide level. Most of these methodologies are based on AASHTO guidelines, which capture the issues concerning vulnerability, but have serious limitations in the nature of extensive data requirements. Few of the well-developed quantitative methods are highly specific to a particular asset type, in most cases, bridges. Because we are interested in the statewide system-level assessment and the methodologies available so far pertain to the particular asset, there is a need to develop a method to suit Indiana's immediate needs. Our study tries to develop a methodology that addresses the vulnerability issues while reducing the need to answer cumbersome surveys for a particular asset. Once the top high priority assets in terms of vulnerability and criticality are determined, AASHTO guidelines could be used to conduct comprehensive vulnerability assessment of a particular asset.

CHAPTER 3. RESEARCH METHODOLOGY

This chapter presents the framework and method used for identifying critical assets that are under the control of the Indiana Department of Transportation. For the purpose of the study, a methodology based on AASHTO guidelines (AASHTO, 2003) was developed to identify the critical assets. The primary purpose of this chapter is to establish a methodology based on the state-of-the-art in order to address the issues specific to Indiana.

3.1. Research Framework

As in the case of most methodologies developed so far for vulnerability assessment, this research framework is done in five stages. The main objective is to develop a decision making tool for INDOT to identify and evaluate the level of vulnerability of assets susceptible to terrorist attacks. The five steps are:

1. Identify assets from the thousands of assets that are under INDOT's control. To reduce the numbers to manageable size, a filter needs to be applied to select those assets that are critical. Each of INDOT's seven districts selected their 25 most critical assets. The resulting 175 assets were prioritized at the statewide level in stage 4 of the assessment process, based on their vulnerability .
2. Establish vulnerability and criticality factors to identify and evaluate those assets selected in step 1. This step is important, because the selection depends on the criteria specified. Also, there is no standardization available for the set of criteria

that will help in evaluating the vulnerability and criticality of an asset. No literature, so far in this field has defined a set of criteria that can be used universally for evaluating vulnerability of assets. All methods have their own definitions for vulnerability and criticality and assess assets based on those definitions.

3. Develop a survey that will enable the experts to evaluate the assets electronically.
4. Assess the vulnerability and criticality of the assets, based on the criteria identified in stage 2 of the process. Using the graphs and the vulnerability-criticality index, prioritize the list of assets.
5. Suggest a method to conduct in-depth vulnerability assessment, if necessary, of the assets identified in stage 4 and suggest countermeasures suitable to these assets. In this stage, the methodology suggested by AASHTO (AASHTO, 2002) is used.

This research focused on these first five steps. The methodology can be written as a logic diagram shown in Figure 4.

Figure 4 Research Framework

Fuzzy logic could be used in each of the steps to deal with the subjective nature of the input. Because vulnerability assessment is a continuous process, it needs to be redone after every countermeasure implementation. This is represented by the loop in Figure 4. Neural networks could be used to train the system to identify critical assets and assess the vulnerabilities. Also, repeated vulnerability assessments can be conducted by implementing neural networks.

3.2. Vulnerability Assessment

There is no standard definition for vulnerability assessment. Recently, efforts have been made by the National Infrastructure Advisory Council (NIAC) to promote a common understanding of vulnerabilities. Because the NIAC definition is not yet universally

accepted, given below are some of the more common definitions used for vulnerability assessment.

- Systematic examination of critical infrastructure, the interconnected systems on which it relies, its information, or product, to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation. (CIAO, 2004)
- Systematic examination of an asset or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Primode, 2004)
- Vulnerability is defined as a set of conditions that may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system. (NIAC, 2004)

3.2.1. Vulnerability and Criticality Index

In order to assess and evaluate assets, there needs to be common criterion for evaluating relative vulnerability and criticality of assets. The assets considered in this research are of varied nature, such as bridges, routes, equipment and personnel. In order to compare them, it is necessary to identify a common measurable factor. Because none of the characteristics of these assets are universal to all assets, we devised an index that transforms the specific characteristics and the capability of an asset to respond to terrorist attack into a quantifiable form. This index called the Vulnerability and Criticality Index, is based on a set of criteria that are portable to evaluate different asset types. Some of the

factors considered are importance of an asset to the community and the economy, number of lives lost or affected and recoverability time. The criteria values are subjective in nature. For purposes of implementation, the factors mentioned in the AASHTO guidelines and the ones mentioned in this section that influence vulnerability and criticality are captured in the definitions mentioned in Section 3.4.1. Because of the subjective nature of the problem, the evaluation of assets is based on professional judgment and previous experience.

The Vulnerability and Criticality Index reflects both how critical and how vulnerable an asset is. Because each of the criteria considered does not influence vulnerability and criticality to the same extent, they have different weights. The weights are obtained using the Analytical Hierarchical Process (AHP), which will be explained later in this chapter. Experts provide the input for these weights, relying on their prior experience and knowledge.

3.2.2. Vulnerability and Criticality Index Formulation

The assets in each district will be named as $A_1, A_2, A_3, \dots, A_m$ where m is the maximum number of assets in each district. In our case study, $m = 25$. The notation for 175 assets from 7 districts is as follows. The asset names start with the first letter of the district. For example, Greenfield assets are denoted from G1 to G25.

There are six criteria to evaluate the criticality and vulnerability of an asset, such as importance and susceptibility to a threat, denoted as $D_1, D_2, D_3, \dots, D_6$.

The vulnerability and criticality values for each asset j in District i are denoted as V_{ij} and C_{ij} , where $j = 1, 2, 3, \dots, 25$, $i \in \{G, V, S, T, L, C, F\}$, and

G = Greenfield, V = Vincennes, S = Seymour, T = Toll Road, L = LaPorte , C = Crawfordsville and F = Fort Wayne.

3.3. Data Collection

In order to put together a list of critical and vulnerable assets and to assess their vulnerabilities, data were collected at various stages of the project.

3.3.1. Identification of Assets -- Preliminary Survey

Because the total number of assets that could be protected is overwhelming, a method needs to be devised to narrow down the set of assets to the most critical and vulnerable ones. The purpose is to consider all assets and identify those that are critical by considering how critical each transportation asset is to the function and mission of the activities it supports. For the purpose of identifying the assets, a preliminary survey was conducted. Representatives from each of INDOT's seven districts (6 geographic districts and the Indiana Toll Road) were asked to identify the 25 assets that they consider to be most critical within their jurisdiction. The idea was that the people local to the assets would have the best knowledge about the assets. This method was selected also because the criteria that affect criticality were mostly subjective and not measurable. The survey was intentionally kept open ended so as not to influence the expert's judgment as to the nature and the type of the critical assets. The people in the district would know best what assets are critical. Responses to this survey were varied. Because of the open-endedness, there were differences in the type of assets identified. Some districts considered certain highway corridors important and some highlighted bridges.

Other districts considered their equipment, facilities, or personnel to be their most important assets. This indicates that an assessment vulnerability and criticality of assets is highly subjective and is dependent on the perspective of the experts queried.

Problems arise at this stage because an expert must assume the nature of the threat while choosing a critical asset. The vulnerability or criticality of an asset might vary depending on the characteristics of the asset and its response to a particular type of threat. For example, a bridge is not the likely target of a biological attack. Experts should be instructed to consider the most likely type of an attack against an asset when assigning the vulnerability and criticality of that asset. Identifying assets according to the asset types such as bridges, routes and facilities and assessing the assets for criticality and vulnerability within these asset types is recommended. Evaluating the assets within asset types makes it easier to compare assets.

3.4. Development of District Survey

The results from the preliminary survey were collected and analyzed. The results included a wide variety of assets -- bridges, corridors, US and state routes, unit sites, Traffic Management Center, headquarters, personnel, etc. Because of the highly varied nature of the top 25 assets in each district, designing a set of common quantifiable criteria to assess vulnerability was not feasible. Two strategies were considered.

1. Develop a method that uses different measurable attributes based on the characteristics of the asset and use them as factors indicating vulnerability and criticality. There are two important limitations to this method. (A) The attributes are not consistent among all the asset categories. This limitation makes the comparison of various assets difficult because of a lack of common factor for evaluation. (B) The second limitation is, apart from

bridges and routes, other kinds of assets do not have clear measurable attributes that reflect their vulnerability.

2. Use a subjective approach. Because of the limitations of the first methodology, we decided to take a more subjective approach and use expert knowledge in assessing the vulnerability of the critical assets (AASHTO, 2003). This approach is widely used in situations where statewide analysis needs to be conducted considering various asset categories. The idea was to develop a method that is concise and requires minimum input from experts while fully incorporating the factors that define vulnerability. The trade-off was consider a few assets and conduct an extensive assessment based on AASHTO guidelines or consider a larger set of assets using a moderate depth of analysis. Because this is the preliminary attempt at VA for INDOT, we decided to analyze all 175 assets (25 from each of the 7 districts) before prioritizing them. In the next stage of data collection, surveys were sent to the districts, asking them to evaluate the identified assets based on the definitions of vulnerability and criticality. These definitions were a result of putting together various criteria from different sources and methods mentioned in Chapter 2. Owing to the subjective nature of the survey, providing careful definition of these terms was very critical. Visual Basic and Macros in Excel were used to develop an online survey with graphic interface. The survey sent to the districts looks as shown in Figures 5 to 7. The definition interface gives the user the definitions of Vulnerability and criticality before the expert begins to input values. The expert is asked to enter the values for each of the assets for their specific district, as shown in Figure 7. These values, once saved, can be retrieved from the Excel sheet.

Figure 5 Introductory User Interface

Figure 6 The Definition User Interface

Second_set [X]

Evaluate each asset against these criteria on a scale of 1 to 50. 50 = most vulnerable or most critical.

Evaluation Criteria

LIST OF ASSETS	VULNERABILITY	CRITICALITY
I-865 in Marion County	<input type="text"/>	<input type="text"/>
Indiana Government Center North	<input type="text"/>	<input type="text"/>
Indianapolis Subdistrict complex	<input type="text"/>	<input type="text"/>
Indianapolis Subdistrict Unit Sites	<input type="text"/>	<input type="text"/>
Indianapolis Traffic Management Center	<input type="text"/>	<input type="text"/>
S.R.37 in Marion county	<input type="text"/>	<input type="text"/>
S.R.67 in Marion County	<input type="text"/>	<input type="text"/>
Tipton Subdistrict complex	<input type="text"/>	<input type="text"/>
Tipton Subdistrict Unit sites	<input type="text"/>	<input type="text"/>
U.S 40 in Marion County	<input type="text"/>	<input type="text"/>
U.S.52 in Marion County	<input type="text"/>	<input type="text"/>
US-231 in Marion County	<input type="text"/>	<input type="text"/>

Figure 7 Expert Information Input User Interface

3.4.1. Determination of Vulnerability and criticality Definitions

Because there is no standard definition of vulnerability and criticality, we devised a definition to suit our research needs. According to AASHTO guidelines (AASHTO, 2003), vulnerability and criticality are evaluated based on a survey of about 20 questions. This process is feasible in a case in which the number of assets to be evaluated is few. Because we had 175 assets to evaluate, we had to devise a method that captures the main

factors that affect vulnerability and criticality. The method should also require minimum data input for each asset from the experts because of the constraints on their time. Such a procedure would be especially helpful if a larger number of assets were being considered in a vulnerability assessment. The objective was to devise a set of criteria that provide a common basis to measure the vulnerability and criticality of an asset. The factors that affect vulnerability and criticality were identified and definitions were devised based on these factors. Using the vulnerability and criticality definitions, the assets are evaluated to obtain an index that reflects the assets' vulnerability and criticality based on the criteria defined.

Vulnerability of an asset (V_{ij})

We define the vulnerability of an asset as

1. The ease with which a person can get close enough to the asset to destroy/disable it.
2. An asset's design, implementation, or operation that renders the asset susceptible to destruction or incapacitation by a threat.
3. The existence of materials at the site that expose human life, property, and resources to damage from the results of a terrorist attack.
4. The symbolic importance of the asset to the community.

Criticality of an asset (C_{ij})

We define the criticality of an asset as

1. How essential the physical or cyber-based system is to the minimum operations of the economy and government.
2. How severe an impact on security, public health and safety would the incapacitation or destruction of those systems and assets?

3. The availability of an alternative or substitute/replacement, for example, a detour in the case of a disrupted route.

4. The time needed to restore the facility to its normal function.

By applying these definitions to an asset, the values for vulnerability and criticality are obtained. These values are combined using the weights obtained from an AHP Survey to obtain an index on a scale of 1 to 50. Based on the value of the index, the assets are ranked and the most critical and vulnerable ones are strengthened by implementing suitable countermeasures. Implementing countermeasures may reduce an asset's vulnerability, so that its index drops. Vulnerability assessment is a continuous process. Implementation of countermeasures can reduce the vulnerability of highly vulnerable assets. The strengthening of an asset and increased security will result in the reduction of vulnerability, and the asset may drop down on the list of prioritized assets.

3.4.2. District Survey Data Collection

A survey containing the assets identified in the preliminary survey was sent to the seven districts. Each survey had assets specific to its district. From the responses, the Vulnerability and criticality values for each asset were obtained. The values from this survey were used to obtain Vulnerability and Criticality Indices. Plotting these on a vulnerability and criticality matrix (shown in Figure 8) would help us prioritize those assets that fall in the upper right hand quadrant. A more extensive vulnerability assessment could be conducted for assets that had the highest preliminary rank before suitable countermeasures are suggested and implemented. The survey results from this assessment can be combined using the AHP weights to obtain an over-all index. This index will help in ranking the assets and in guiding resource deployment. The weights

were obtained from the knowledge of experts using the Analytical Hierarchical Process (AHP). AHP will be described in the following section.

Figure 8 Vulnerability and Criticality Matrix (AASHTO, 2002)

3.5. Obtaining the Weights Using AHP

The Analytic Hierarchy Process (AHP) is a mathematical technique for multicriteria decision making. The pertinent data are derived by using a set of pairwise comparisons. These comparisons are used to obtain the weights that represent the importance of the decision criteria, and the relative performance measures of the alternatives in terms of each individual decision criterion. The analytic hierarchy process (AHP) is a comprehensive, logical and structural framework that allows improving the

understanding of complex decisions by decomposing the problem into a hierarchical structure. (Saaty, 1980). The incorporation of all relevant decision criteria, and their pairwise comparison allows the decision maker to determine the trade-offs among objectives. It enables people to make decisions involving many kinds of concerns, including planning, setting priorities, selecting the best among a number of alternatives, and allocating resources. The application of the AHP approach explicitly recognizes and incorporates the knowledge and expertise of the participants in the priority setting process, by making use of their subjective judgments. This is a particularly important feature for decisions that must be made without precisely measurable information.

The AHP is based on three principles:

1. Decomposition of the decision problem,
2. Comparative judgment of the elements, and
3. Synthesis of the priorities.

3.5.1. Decomposition of the problem into hierarchy

The first step is to structure the decision problem in a hierarchy as depicted in Figure 9. The goal of the decision, such as "Identifying the vulnerability and criticality of assets", is at the top level of the hierarchy. The next level consists of the criteria relevant for this goal. At the bottom level are the alternatives (in our case, various assets or asset categories) to be evaluated. The asset categories considered are routes, equipment, personnel, etc. Individual assets could also be considered as alternatives. For example, route 1, route 2, etc. The purpose of the AHP is to compare the alternative at the third

level of Figure 9 using the criteria at second level. Because the number of assets in our case is large (175), it was not practical to use AHP to evaluate alternatives at stage 3. Stage 3 would have required experts to create a matrix of order 175 for each of the 5 criteria. Because of its tedious nature, we used AHP only until step 2, where relative importance of criteria is evaluated. The weights for different criteria are obtained by pairwise comparison of the criteria at step 2. These weights help in the extensive vulnerability assessment. The three steps for the example are shown in Figure 10.

Figure 9 The AHP Hierarchical Process

Figure 10 Illustration of AHP

The criteria considered for INDOT assets are

1. Importance:

- How important is this asset to the normal functions of society?
- Would the loss of this asset cause severe economic impacts?
- Would an attack on this asset cause substantial psychological fear among people?

2. Recoverability

- Existence of alternative assets to maintain customary operations
- Time to return the asset to regular condition

3. Number of people using the facility and personnel (Personnel Safety)

- Number of INDOT personnel normally present at the site
- Number of other people normally at the facility
- Does the asset or site attract crowds for special events or on a regular basis?

4. Accessibility

- Is there a fence around the asset?
- Is access to the asset regulated by pass or guard personnel?
- How close to the asset can unauthorized vehicles get?

5. Visibility

- How visible is the asset as a potential target?
- How aware are people of the target's existence?

6. Susceptibility to threat: Consider explosive, chemical, biological, radiological weapons, as well as hazardous materials or other dangerous items.

- How vulnerable is the asset to such threats?

- Is there a system to control access to such weapons and materials at the site?
- Can any products stored or used on your site be used as, or in the manufacture of, a mass casualty weapon, or cause extensive environmental damage?

AHP can be used to evaluate the vulnerability of assets, if the assets are considered as alternatives in step 3 of the hierarchy. The alternatives could be

1. Asset categories such as bridges, routes, equipment and personnel
2. Assets within the same category such as bridge 1, bridge 2, ...
3. Individual assets from different categories such as bridge 1, route 2, equipment 3, ...

For the sake of illustration, we chose asset types as our alternatives. In the research, AHP was used only until stage 2 where criteria are compared. The following are the asset categories considered for the purpose of assessing their vulnerabilities based on the criteria mentioned above. The categories are the result of grouping the “top 25” responses received from seven districts to our survey.

The asset categories considered are

1. Route sections with bridges
2. Route sections without bridges
3. Traffic Management Center
4. Central and district offices
5. Communication systems
6. Equipment
7. Personnel

3.5.2. Comparative Judgment of Elements

The second step in the AHP process is the comparison of the alternatives and the criteria. The asset categories are compared in pairs with respect to each element of the next higher level. For example, all the assets (alternatives) are pairwise compared with respect to criterion ‘importance’ as shown in Table 5. For this comparison, the fundamental scale of Table 3 can be used. It allows the analyst to express the comparisons in verbal terms, which are then translated to the corresponding numbers.

Table 3 Fundamental Scale for Pairwise Comparisons

Comparative Importance	Definition	Explanation
1	Equally important	Two decision elements (e.g., indicators) equally influence the parent decision element.*
3	Moderately more important	One decision element is moderately more influential than the other.
5	Strongly more important	One decision element has stronger influence than the other.
7	Very strongly more important	One decision element has significantly more influence over the other.
9	Extremely more important	The difference between influences of the two decision elements is extremely significant.
2, 4, 6, 8	Intermediate judgment values	Judgment values between equally, moderately, strongly, very strongly, and extremely.
Reciprocals		If v is the judgment value when i is compared to j , then $1/v$ is the judgment value when j is compared to i .

* Parent decision element is the goal or the main objective in the hierarchy process. It is the element at the top of the structure in Figure 9.

3.5.3. Synthesis of Priorities

In step 3, the criteria are evaluated against each other by pairwise comparison. This process helps identify the importance of criteria relative to each other. This is particularly useful when the criteria that influence the criticality or vulnerability of an asset do not have the same weights. For example, to determine the vulnerability of an asset, the criterion ‘recoverability’ could have more weight than the criterion ‘visibility’ in influencing vulnerability. In such a case, we need to identify how much each of the factors contributes to the vulnerability of an asset. AHP process helps us determine those weights. Sum of the weights for each of these criteria add up to 1.

To illustrate the AHP process, an example of pairwise comparisons is given below.

Table 4. Pairwise Comparison of Criteria

	Importance	Recoverability	No of ppl & prsnl	Accessibiity	Visibiliy	Susceptibility-Threat	impacts-economic	Sum	Weights
Importance	1	0.5	0.5	3	4	0.333	2	11.33	0.155
Recoverability	2	1	0.5	2	3	1	3	12.50	0.171
No of ppl & personnel	2	2	1	4	3	1	4	17.00	0.233
Accessibiity	0.33	0.5	0.25	1	2	0.25	0.5	4.83	0.066
Visibiliy	0.25	0.33	0.33	0.5	1	0.25	0.33	2.99	0.041
Susceptibility-Threat	3	1	1	4	4	1	3	17.00	0.233
Impacts	0.5	0.33	0.25	2	3	0.33	1	7.41	0.101
								73.06	

Consider the shaded region in Table 4. The number in the first row, second column is obtained as follows. The importance criteria are weighed against recoverability and, in the analyst's opinion, importance is not as significant as recoverability. It is halfway between "equally important" and "moderately less" important. Hence, the value assigned is $1/2$. The upper triangular half of the matrix is filled in a similar way. The diagonal elements are 1 because the criteria are evaluated against themselves. The lower triangular matrix is obtained by inverting the entries in the upper triangular matrix. Mathematically, they can be represented as $a_{ij} = 1/a_{ji}$. Once all the cells in the shaded area are filled, the elements in each column for a row are added to obtain 'sum'. The weights are obtained for each criterion by normalizing the values under 'sum' so that the sum of the values for 'weights' adds up to one.

The next step in the AHP process is the comparative judgment of elements (alternatives), which is pairwise comparison of assets with respect to each criterion. This step is performed only if the entire vulnerability assessment is performed using AHP. In such a case, the assets (alternatives) are evaluated by pairwise comparison. This is feasible if the number of alternatives is not large. In the example, asset categories are considered as alternatives. The asset categories are compared in the manner explained above, but with respect to one criterion, in this case, Importance. Number 3 in the first row third column is obtained when the "routes sections with bridges" asset category is weighed against TMC with respect to importance. The matrix is filled similar to Table 5 by pairwise comparing each asset against the other with the criterion 'importance' in mind. Because

there are six alternatives, six matrices will be generated, one with respect to each criterion. These tables give the weights of each of the asset categories against each criterion.

Table 5. Pairwise comparison of assets with respect to Importance

	RS w Bridges	RS w/o Bridges	TMC	C and D offices	communication Systems	Equipment	Sum	Weights
Route Sections w bridges	1	2	3	3	2	4	15	0.334
Route sections w/o bridges	0.5	1	0.5	2	1	2	7	0.156
TMC	0.33	2	1	2	1	2	8.33	0.185
Central and District offices	0.33	0.5	0.5	1	1	2	5.33	0.119
Communicatio n Systems	0.5	1	1	0.5	1	2	6	0.134
Equipment	0.25	0.5	0.5	0.5	0.5	1	3.25	0.072
							44.91	

In the synthesis step of the AHP process, we synthesize the comparisons to get the priorities of the alternatives with respect to each criterion and the weights of each criterion with respect to the goal. The elements in Table 6 are the outputs (local priorities with respect to each criterion) of tables similar to Table 5. Relative weights for the criteria are obtained from Table 4. The local priorities are then multiplied by the weights of the respective criteria obtained in Table 4. The results are summed up to get the global priority for each alternative.

Table 6. Local Priorities for Alternatives

	Importance	Recoverability	No of ppl	Susceptibility- threat	<u>Global Priority</u>	<u>Normalized Global Priority</u>	Ranking
Weights	0.16	0.17	0.23	0.23			
Route Sections w Bridges	0.33	0.32	0.17	0.29	0.21	0.27	1
Route Sections w/o Bridges	0.16	0.20	0.17	0.15	0.13	0.17	4
TMC	0.19	0.15	0.29	0.22	0.17	0.22	2
Central and District Offices	0.12	0.17	0.22	0.19	0.14	0.18	3
Communication Systems	0.13	0.10	0.10	0.10	0.08	0.11	5
Equipment	0.07	0.07	0.06	0.06	0.05	0.06	6
					0.79	1.00	

The number in the first row under Global Priority is obtained by multiplying the row 1 (route sections with bridges) values by the corresponding numbers in the row weights (the weights for each criteria obtained from Table 4.

Sample Calculation:

Global Priority for Route Sections with Bridges =

$$(0.33 * 0.16) + (0.32 * 0.17) + (0.17 * 0.23) + (0.29 * 0.23) = 0.21. \quad (3.1)$$

The values for Global Priority are normalized so that they sum up to one, as shown in the column under Normalized Global Priority. Using these values, the asset categories are ranked.

3.5.4. Justification for AHP

The principle assumption of AHP is that the weights of the criteria do not depend on the alternatives under consideration. In cases where weights are not independent, AHP can be combined with utility theory. Utility theory deals with the subjective probabilities. When the preference of a particular alternative depends not just on the choice of the decision maker but also on the state and nature of the alternatives that are beyond the control of the decision maker, utility theory is used. AHP is simple to apply and is the most widely used MCDM method when the criteria are subjective. (Triantaphyllou, 2000) AHP is less biased when care is taken by the decision-makers to choose meaningful weights. Among the MCDM methods, hierarchical rating is preferred, because experts find it easier and more logical than direct weighting methods such as WSM (Hobbs, 2000).

CHAPTER 4. ANALYSIS AND DISCUSSION OF RESULTS

This chapter presents the results obtained from the district survey and the analytical hierarchical process of vulnerability assessment. The results from the district survey can further be investigated for vulnerabilities using the AASHTO method. The values from this method can be combined using the weights obtained through AHP. The purpose of the model is to provide a tool for the agencies in Indiana to evaluate the vulnerability and criticality of assets. This method can assist transportation agencies to prioritize any asset. The important aspect of this method is the transferability and the simplicity of the methodology. This is especially helpful when a large number of assets need to be filtered to obtain a subset of assets that are critical and vulnerable. Also, the results are interpreted and the limitations of the method are identified in this chapter.

4.1. Analysis of District Survey Results

Five districts out of seven responded to the district survey. Each of the 25 assets in each district was evaluated for its vulnerability and criticality. This evaluation resulted in two indices criticality index and a vulnerability index. The values for these indices were obtained based on the criteria defining vulnerability and criticality. These indices transform the subjective nature of the criteria into a numerical value. The results obtained from the districts are plotted on the vulnerability and criticality matrix (Figure 8) suggested by AASHTO (2002). In this method, the values for vulnerability (V_{ij}) and

criticality (C_{ij}) are plotted against each other for each asset. The AASHTO method uses a scale of 0 to 100. We used a scale of 0 to 50 to reduce the dispersion. We noticed that there is a tendency for experts to assign values in multiples of 5 or 10, whether the scale was 0 to 50 or 0 to 100. The assets that fall in Quadrant I are classified as highly critical and vulnerable. An assumption that all assets that have both vulnerability and criticality index greater than 25 (50% of 50) fall in Quadrant I was made. AASHTO (2002) suggests that any asset that has 50% of the maximum value or greater can be classified as a priority asset. The following figures (Figures 11 to 15) show the results and the plotted matrices for the districts that responded.

Figure 11 Crawfordsville Vulnerability and Criticality Matrix

There are fewer than 25 points in the matrices, because of the overlap of the points. Some of the assets had identical vulnerability and criticality values. The points are not identified by ID's or names because of the sensitive nature of the information. Similarly in other cases too, there is an overlap of points. For example, in the case of Fort Wayne, as shown in Figure 12, 14 assets had the same criticality value of 45 and vulnerability value of 50.

Figure 12 Fort Wayne Vulnerability and Criticality Matrix

Figure 13 Greenfield Vulnerability and Criticality Matrix

Figure 14 LaPorte Vulnerability and Criticality Matrix.

Figure 15 Vincennes Vulnerability and Criticality Matrix

4.2. Discussion of Results

The plots for the districts tended to follow two patterns. For some districts, most of the assets were clustered in Quadrant I; for other districts, the assets were distributed in all quadrants. Assets that fall in Quadrant I of Figures 11 to 15 can be classified as critical and vulnerable. If all assets in a district were being considered, one would expect only a few assets to fall in the top right quadrant. In such a case, the assets that fall in Quadrant I could be classified as most critical and immediate improvements could be considered.

Because the 25 assets being considered by each district had already been listed as the most critical and vulnerable, it is reasonable to expect that most of the assets would fall in

Quadrant I. In such a case, it is more difficult to distinguish the most critical and vulnerable assets from the others.

The pattern observed in the Greenfield district appears to be the result of taking the 25 assets as the universe, and trying to distinguish among those 25 without considering the other assets in the district that were not a part of the top 25.

This method may work better when all assets in the district are considered. In such a case, there would be a clearer segregation between the assets that are critical and vulnerable and the rest of the district assets. The results we obtained from the districts could be also different due to the varied interpretations of the definitions of Vulnerability and Criticality. An attempt to distinguish between the top 25 assets in an INDOT district will probably lead to a much different plot based on a rating of all assets in the district. However, this assessment of each district's top 25 assets will help as preparation for the statewide vulnerability assessment.

The discrepancies in the results from various districts could be reduced if the experts are trained to think with the same perspective. Once the top 25 assets are identified, the experts can be asked to rate these top 25 assets relative to each other without considering the rest of the assets in the district.

4.3. Combining Vulnerability and Criticality Indices

Because the plotting of the indices did not give clear results, we attempted to combine the values for the vulnerability and criticality indices to give vulnerability and criticality index. Using this one number, we prioritized the assets which gave better results. In this case, we assumed, vulnerability and criticality have the same weight. Table 7 shows an example of this prioritization method. Some of the assets had the same value for the

combined Vulnerability and Criticality Index. In such a case, the assets were given equal priority. When choosing an asset for countermeasure implementation among equally important assets, a more extensive vulnerability assessment as discussed in Section 4.5 can be used.

Table 7 Prioritization of Assets Using Vulnerability and Criticality Index

Assets	Criticality Index (CGj)	Vulnerability Index (VGj)	Vulnerability and Criticality Index	Priority
Asset 24	50	50	100	1
Asset 25	50	50	100	1
Asset 23	45	50	95	3
Asset 22	40	50	90	4
Asset 13	35	45	80	5
Asset 14	35	45	80	5
Asset 15	35	45	80	5
Asset 16	35	45	80	5
Asset 17	35	45	80	5
Asset 18	35	45	80	5
Asset 19	40	40	80	5
Asset 20	40	40	80	5
Asset 21	40	40	80	5
Asset 10	30	45	75	14
Asset 11	30	45	75	14
Asset 12	30	45	75	14
Asset 6	30	40	70	17
Asset 7	30	40	70	17
Asset 8	30	40	70	17
Asset 9	30	40	70	17
Asset 2	20	45	65	21
Asset 3	25	40	65	21
Asset 4	25	40	65	21
Asset 5	25	40	65	21
Asset 1	20	40	60	25

4.4. Comparing Results from Different Districts

The results obtained from different districts need to be combined to get a statewide list of priority assets. This is not straightforward, because the assets in each district are not equally critical or vulnerable. For example, all the assets identified in the list from District 1 could be more critical than the top asset in District 2. In such a case, the assets in District 1 would need to be protected first before attending to District 2 assets. Figure 16 shows the Vulnerability and Criticality Matrix where the assets from all five districts are plotted. The assets in each district are not spread out equally in all the quadrants. The assets from District V are scattered in all quadrants while the assets in District C are concentrated in Quadrant I.

Figure 16 Vulnerability and Criticality Matrix – All District Plot

The variation in the pattern is probably because of a difference in the perception of the experts while evaluating the assets. Some of them considered the top 25 assets as a

separate group, and others considered all the assets in the district while assessing their top 25. We devised a few methods that might help in converting the various district lists into a statewide list of critical and vulnerable assets.

1. Have a committee of experts consider the top 5 assets in each district and rank them from 1 to 25. Using the ranks for the assets from each district, obtain a weight for each district. This could be done by adding the ranks for the assets in each of the districts and obtaining a sum. The inverse values of these sums can be used as the weight for each district. The criticality and vulnerability index of each of the assets can be multiplied by the respective district weight to obtain the ranking for the entire set of assets. The limitation of this procedure is that if a district has only one prominent asset and the rest are not so important, the weight of the prominent assets carries over to the rest of the assets in the district.
2. Obtain a weight for each district using the judgment of a group of experts. Each district weight would then be applied to all the 25 assets in the respective district. For example district G might be given a weight of 1.2 and district V is given a weight of 1.08. Then the assets G1 to G25 are multiplied by 1.2. To obtain G'1 to G'25. Similarly, assets V'1 to V'25 are obtained by multiplying V1 to V25 by 1.08. Ranking a statewide list of assets is obtained by sorting the asset values such as G'1,..., G'25 and V'1 to V'25. This procedure has the limitation of being biased. Every asset in district G is not more important or less important than any asset in district V to the same extent. The criticality and vulnerability of an asset is not dependent only on which district the asset belongs to. There are other

factors such as the environment, the existence of an alternative and usage that affect the critical and vulnerable nature of an asset.

3. Obtain weights for each asset type using expert judgment. For example, say “bridges” are 1.2 times more important than “facilities”. As an example, bridge 1 in a district = 1.2 X subdistrict building 1 in that district. Rank assets within asset categories and use these weights to combine the all assets across the state. This method has the limitation that all assets belonging to one asset type are not equally more important or less important than other asset types. Also, an asset’s criticality and vulnerability depends on many factors, such as location and usage, not just the type of asset.
4. Assuming the assets are evaluated at the state level, a counter-terrorism committee of individuals who have adequate knowledge about threats and are familiar with assessment studies is convened. This committee will consider the top assets in all districts and choose the most critical and vulnerable asset among them. The chosen asset is selected for countermeasures and reassessed for its subsequent vulnerability and criticality. Examples of countermeasures are discussed in Chapter 5. Because of the asset’s reduced vulnerability, it may drop down on the list of assets in that district. If the countermeasure selected does not reduce the vulnerability level, choose a different countermeasure based on the feasibility and the budget. The process of choosing an asset for countermeasure implementation is performed again among the seven assets from seven districts. This list will be similar to the earlier one with a possible change that the second most important asset will be the top priority asset in that particular district where

an asset was chosen in iteration 1 of this process. Depending on the available resources and budget, agencies can pick one among seven assets in a similar manner as described above for countermeasure implementation.

Experts at INDOT suggest that the best way to identify assets is by asset types, such as bridges, routes and facilities. This classification by asset type is used in budgeting and allocating resources. Once the assets are classified by type, the assets within each district can be ranked. A group of experts at the central office along with the experts from each district can be convened together to help decide on the overall ranking at the state level for the assets identified at the district level within each asset category.

4.5. Comprehensive Vulnerability Assessment using AHP

Once the high priority assets are identified through two filters, an extensive vulnerability assessment can be conducted. The comprehensive vulnerability assessment could also be used if there are fewer assets to evaluate. The two filters help to identify the critical assets first and then identify vulnerable assets among the selected critical assets. Table 8 shows a survey based on AASHTO guidelines (AASHTO 2002). There are six criteria affecting vulnerability and criticality.

1. Importance
2. Accessibility.
3. Recoverability
4. Susceptibility to threat
5. Visibility
6. Number of people affected.

Each of the six criteria has various factors affecting it, as shown in Figure 10 and Table 8. A default value is given for each factor. Each factor is applied to the asset under consideration and, if applicable, gets its default value. Otherwise, the assigned value is zero. Once all the values are determined, they are summed up for each of the criteria and there would be six values, D1 through D6. The values D1 to D6 are normalized on a scale of 1 to 10, so that values for all the criteria are on a same scale. The Vulnerability and Criticality Index is obtained by calculating the weighted sum of the normalized values D1 through D6. The weights used (d1 to d6) are obtained using AHP. The Vulnerability and Criticality Index =

$$(D1*d1) + (D2*d2) + (D3*d3) + (D4*d4) + (D5*d5) + (D6*d6). \quad (4.1)$$

The order of criteria in Table 8 is according to the weight of each criterion obtained using AHP shown in Table 9. The criterion that has the highest weight (d1) is included first in Table 8.

Table 8 Comprehensive Vulnerability Survey

Criteria	Factor	Default value	Description
Recoverability (D1)	Replacement cost	3	Will significant replacement cost be incurred if the asset is attacked?
	Down time	3	Will an attack on the asset cause significant replacement/down time?
	Emergency Response Function	5	Does the asset serve an emergency response function and will the action or activity of emergency response be affected?
	Availability of an alternative	4	Is this the only asset that can perform its primary function?
Susceptibility to threat (D2)	Ability to Provide Protection	1	Does the asset lack a system of measures for protection? (i.e., Physical or response force)

	Relative Vulnerability to attack	2	Is the asset relatively vulnerable to an attack? (i.e., Due to location, prominence, or other factors)
	Receptor Impacts	1-5	1 - No environmental or human receptor effects 2- Acute or chronic toxic effects to environmental receptor(s) 3- Acute and chronic effects to environmental receptor(s) 4-Acute or chronic effects to human receptor(s) 5- Acute and chronic effects to environmental and human receptor(s)
Accessibility (D3)	Access Proximity	1-5	1 Asset with no vehicle traffic and no parking within 50 feet 2 Asset with no unauthorized vehicle traffic and no parking within 50 feet 3 Asset with vehicle traffic but no vehicle parking within 50 feet 4 Asset with vehicle traffic but no unauthorized vehicle parking within 50 feet 5 Asset with open access for vehicle traffic and parking within 50
	Security Level	1-5	1 Controlled and protected security access with a response force available 2 Controlled and protected security access without a response force 3 Controlled security access but not protected 4 Protected but not controlled security access 5 Unprotected and uncontrolled security access
Importance (D4)	Government Continuity	5	Is the asset necessary to maintain government continuity?
	Military Importance	5	Is the asset important to military functions?
	Economic Impact	5	Will damage to the asset have an effect on the means of living, or the resources and wealth of a region or state?
	Functional Importance	2	Is there an overall value of the asset performing or staying operational?
	Symbolic Importance	1	Does the asset have symbolic importance?

Number of people affected (D5)	Casualty Risk	5	Is there a possibility of serious injury or loss of life resulting from an attack on the asset?
	Attendants/Users	1-5	1 Less than 10 2 10 to 100 (Major Incident per FEMA) 3 100 to 1000 4 1000 to 3000 5 Greater than 3000 (Catastrophic Incident per FEMA)
Visibility (D6)	Level of recognition	1-5	1 Largely invisible in the community 2 Visible by the community 3 Visible Statewide 4 Visible Nationwide 5 Visible Worldwide

4.5.1. Determination of Criteria Weights Using AHP

The survey was sent to the members of the Study Advisory Committee and the Prevention Subcommittee of INDOT-CTASC (Counter Terrorism and Security Task Council). The experts used their knowledge to provide the input. The weights were calculated for each of the six criteria. The values of the weights (d1 to d6) obtained from the surveys are given in Table 9. In this research, AHP was used only until stage two to compare the criteria and get weights, as shown in Figure 17. Stage 3 of AHP requires the alternatives to be compared pairwise against each other. This is feasible only when there are few alternatives, on the order of 2 to 9. Our study assessed 175 assets, each asset being an alternative. Pairwise comparison of 175 assets would be tedious. The weights in Table 9 indicate that the experts considered ‘recoverability’ and ‘susceptibility to threat’ as the most important criteria. This shows that the experts consider the functionality of the asset above other criteria in evaluating vulnerability and criticality of an asset.

Table 9 Weights of Criteria Obtained from AHP Survey

Criteria	Notation	Weights
Recoverability	d1	0.308
Susceptibility to Threat	d2	0.215
Accessibility	d3	0.159
Importance	d4	0.143
No of people affected	d5	0.111
Visibility	d6	0.065

Figure 17 AHP Framework used in the Research

Vulnerability and Criticality Index =

$$(0.308 * D1) + (0.215 * D2) + (0.159 * D3) + (0.143 * D4) + (0.111 * D5) + (0.065 * D6) \quad (4.2)$$

Using this index, the list of assets can be prioritized. This survey was not used in the study. It is included here as a recommendation for INDOT for conducting future vulnerability assessments. The reason for not using this survey in the study is because of its extensive data needs. Each asset needs to be assessed for each of the six factors and sub factors of the six criteria. Because one person at each district would be providing the information regarding all the assets, we decided to use a simpler version of the survey. The simpler version combines these factors into vulnerability and criticality. By

incorporating the factors into the definitions of vulnerability and criticality, we were able to assess the vulnerabilities of the assets. This procedure was described in Chapter 3.

4.6. Iterative Vulnerability Assessment and Neural Networks

Vulnerability assessment is a continuous process. Once the assets are identified, evaluated, ranked and appropriate countermeasures are implemented, the security level of that asset may go up and its vulnerability is reduced. This would cause the asset to drop down on the list. Also, with time, the circumstances and the threat levels change, which influence vulnerability and criticality. To incorporate such changes, vulnerability assessment needs to be conducted on a regular basis. This is shown as a loop in Figure 4 in Chapter 3.

CHAPTER 5. RECOMMENDATIONS FOR INDOT TO CONDUCT VA

5.1 Introduction

This chapter presents the framework and recommendations for conducting Vulnerability Assessment (VA) for the Department of Transportation in Indiana on a statewide as well as at an asset level. The framework involves a set of guidelines and procedures that best fit INDOT and will help it conduct VA. The framework includes forming a multidisciplinary team, identifying assets on a statewide level, narrowing down the list to a few important assets based on their vulnerability and criticality, conducting extensive VA, identifying countermeasures, implementing them and redoing the vulnerability assessment.

5.2 Multidisciplinary Team Composition

The success of vulnerability assessment depends greatly on the expertise and the varied composition of the team members conducting the assessment. The formation of a multidisciplinary team is essential in order to address various critical and vulnerable components of an asset, knowledge about which is not usually available with one individual. This approach suggests the formation of a dedicated, multidisciplinary team with access to required resources, ranging from databases to personnel. In addition to the formation of a team, commitment from senior State DOT officials to examine critical assets carefully and identify cost-effective countermeasures is crucial. AASHTO (2002)

suggests that the State DOT organize a multidisciplinary team whose members possess a good knowledge of the department's mission, critical assets, and policies, plans and procedures. It is advised that the team members should represent departmental functions such as:

- Budget
- Communications
- Environmental management
- Maintenance
- Purchasing
- Construction
- Facilities management
- Materials testing
- Safety
- Design of structures
- Human resources
- Planning
- Traffic operations

In addition to the internal members, the team will require the services of members from external sources such as law enforcement, fire services, public safety and emergency management services. External members are essential, because a DOT does not have personnel specifically trained to deal with terrorism issues.

5.3 Resources and Data Needs

To address the issues and to ensure the team is well equipped to proceed with the assessment procedures, training exercises should be held prior to vulnerability assessment. USDOT and AASTO conduct Vulnerability Assessment and Emergency response workshops from time to time. The following list identifies the types of resources that can be tapped into by the team to conduct a highway vulnerability assessment.

- Asset data could be obtained from
 - National Bridge Inventory System
 - Hazardous Materials Information System
- Threat data such as “Is the threat credible?” Or “How grave is the threat?”
 - Law Enforcement
 - State’s Emergency Management Agency
 - Homeland Security Office
- Vulnerability data is obtained by conducting surveys of experts regarding factors such as the ease of access and probability of attack.
- Consequence data identifies the assets which, if attacked, produce the greatest risks for undesirable outcomes. Consequences can impact human life or economic activity.
- Countermeasures data estimate delay to aggressors who seek to gain access by using tools in a forced entry or protection of the asset from the effects of tools, weapons, and explosives. For example, installing security systems with video capability at all DOT facilities.
- Cost data

- Policies, plans, and procedures
- Personnel (interviews)
- Geographic Information Systems (maps, drawings)

5.4 Critical Asset Identification

A process is necessary for prioritizing all assets with respect to their vulnerability in terms of their criticality of the ability to deter, detect, delay, and defend against terrorist attacks. The large number and varied nature of assets in the state lends itself to a two-tiered approach: prioritization and vulnerability assessment. The first tier, prioritization, is typically the first step where a few assets among many are identified. This study suggested a prioritization methodology called the Vulnerability and Criticality Index method that can be used efficiently to identify the first set of assets. This prioritization methodology was discussed in Chapter 3 and Chapter 4, along with a case study. We recommend giving clear instructions as to the nature and the type of the assets. The experts need to be trained to think of the most likely attack on the asset before assessing the criticality of an asset. Also, clear instructions should be given to consider only the top 25 assets identified in the first stage to obtain consistency in the perception and evaluation of assets. If some assets, after this assessment stage, are assigned a similar vulnerability and criticality index, a more comprehensive vulnerability assessment procedure, as suggested in Section 4.5, may be conducted.

From our study and the information gathered from other states, we recommend the following set of assets be included in the preliminary assessment.

- Infrastructure such as bridges, interstate highways, US and state routes, corridors and tunnels.
- Facilities for storage, maintenance, headquarters, testing labs, ports of entry, traffic operation centers, unit complexes, district offices, rest areas, weigh stations, etc.
- Equipment such as vehicles carrying hazardous materials and roadway monitoring variable message signs.
- Personnel including vendors and contractors.

Once the set of assets is identified, the next step is to evaluate the assets for their vulnerability and criticality. This preliminary assessment can be done using the procedure described in Chapter 3. Each asset is assessed for vulnerability and criticality separately, based on the factors mentioned in the previous chapter. Those assets that are highly critical and vulnerable are selected and an extensive VA assessment can be conducted using AASHTO guidelines. This is comprehensive; it requires extensive knowledge of the asset characteristics and is time consuming. It requires answering a set of questions for critical asset factors and vulnerability assessment factors and noting if the factor is relevant to the particular asset as shown in Table 10. In case a factor is applicable, it takes a binary value of 1; otherwise zero. The total score for criticality is the sum of all the applicable critical factor values for that asset. Similar analysis is done for Vulnerability and a score is obtained.

Table 10 Critical Asset Factors and Values

CRITICAL ASSET FACTOR	VALUE	DESCRIPTION
<i>Deter/Defend Factors</i>		
A) Ability to Provide Protection	1	Does the asset lack a system of measures for protection? (i.e., Physical or response force)
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (i.e., Due to location, prominence, or other factors)
<i>Loss and Damage Consequences</i>		
C) Casualty Risk	5	Is there a possibility of serious injury or loss of life resulting from an attack on the asset?
D) Environmental Impact	1	Will an attack on the asset have an ecological impact of altering the environment?
E) Replacement Cost	3	Will significant replacement cost (the current cost of replacing the asset with a new one of equal effectiveness) be incurred if the asset is attacked?
F) Replacement/Down Time	3	Will an attack on the asset cause significant replacement/down time?
<i>Consequences to Public Services</i>		
G) Emergency Response Function	5	Does the asset serve an emergency response function and will the action or activity of emergency response be affected?
H) Government Continuity	5	Is the asset necessary to maintain government continuity?
I) Military Importance	5	Is the asset important to military functions?
<i>Consequences to the General Public</i>		
J) Available Alternate	4	Is this the only asset that can perform its primary function? (i.e., There are no alternate facilities that will substitute adequately if this asset is damaged or destroyed)
K) Communication Dependency	1	Is communication dependent upon the asset?
L) Economic Impact	5	Will damage to the asset have an effect on the means of living, or the resources and wealth of a region or state?
M) Functional Importance	2	Is there an overall value of the asset performing or staying operational?
N) Symbolic Importance	1	Does the asset have symbolic importance?

5.5 Threat Assessment

Assessing the threats to the assets is one of the components of vulnerability assessment. This factor needs special consideration, because threats are dynamic and have uncertainty associated with them. Furthermore, the information regarding the threats comes from a source outside of INDOT. AASHTO (2002) states that The U.S. Department of Justice (USDOJ) developed an approach for threat analysis as part of its “State Domestic Preparedness Equipment Program.” Few states have adopted the threat analysis approach

suggested by USDOT (AASHTO, 2002). Threat information could also be obtained from the Homeland Security Advisory System, which provides a framework for assessing and communicating the nature and degree of threats. It assesses whether the threat is imminent and credible. The effective method is to consider factors such as existence, history, intent and nature of target while conducting threat analysis.

5.6 Identification of Assets for Improvement

Once the vulnerability and criticality scores are obtained, they are plotted against each other as shown in Figure 8. If this procedure does not give clear results as to the most important assets, an alternate method is to use weights for vulnerability and criticality. The weights are obtained using AHP and a Vulnerability and Criticality Index is calculated (Refer to Section 4.5). Using the Vulnerability and Criticality Index, the assets are sorted and ranked. This method was explained in Chapters 3 and 4. The top ranked assets are chosen for immediate improvements. Suitable countermeasures are suggested and implemented. This may reduce the vulnerability of the asset.

5.7 Recommended Countermeasures

Countermeasures are the protection measures that reduce the level of vulnerability to threats. Existing safeguards that protect the asset against threats must be assessed. After identifying the top priority assets with respect to vulnerability and criticality, the next step is to implement countermeasures and reduce vulnerability below the acceptable level. In case the existing measures are unlikely to be sufficient, either new countermeasures need to be implemented or the existing ones strengthened. There are three types of countermeasures. (Physical Security Risk Analysis, 2004)

- Preventive - This type countermeasure is designed to prevent damage or impact from an action or event from occurring. Example: A fence around a bridge can prevent attack to some extent.
- Detective - These countermeasures provide some type of notification that something has gone wrong. Example: Surveillance cameras.
- Corrective or Responsive - Some countermeasures have the ability to correct identified problems and respond to the emergency. Example: Training personnel to respond to an attack.

An effective partnership between engineers, administrative officials and security agents is essential to develop cost-effective countermeasures. Countermeasures are typically developed specific to an asset type, based on the characteristics of an asset. They commonly are in the form of work around the asset, strengthening the asset itself, increasing detection capabilities, and developing plans and procedures to increase security. Most of the countermeasures recommended for a physical asset are classified based on their functionality, such as deterrence, detection and defense. The Army Field Manual (2001) defines these terms as follows:

Deterrence – A potential aggressor who perceives a risk of being caught may be deterred from attacking an asset. The effectiveness of deterrence varies with the aggressor's sophistication, the asset's attractiveness, and the aggressor's objective.

Detection – Detection senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force. A detection system must provide all three of these capabilities to be effective.

Defense – Defensive measures protect an asset from aggression by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from weapons and explosives. Defensive measures (1) delay aggressors from gaining access by using tools in a forced entry, (2) prevent an aggressor's movement toward an asset, and (3) protect the asset from the effects of tools, weapons, and explosives.

Below are a list of potential countermeasures that can be adopted based on the nature and the characteristic of the asset. There are based on the recommendations from AASHTO and blue ribbon panel on bridges.

1. Increase inspection efforts to identify potential explosive devices as well as increased or suspicious potential criminal activity.
2. Give personnel training to be more alert and aware of suspicious activities and potentially dangerous packages, boxes, people, etc.
3. Institute full-time surveillance at the most critical assets.
4. Eliminate parking under critical assets, such as key bridges. This could be done by using concrete barriers.
5. Install security systems at DOT facilities with video capabilities, if feasible.
6. Install Mylar sheeting on inside of windows to protect employees from flying glass in the case of an explosion in high employee incident areas.
7. Employ a full-time security officer to control access, at least to major buildings such as headquarters.
8. Lock all access gates and install remote controlled gates where necessary.

9. Limit access to all critical buildings through the issuance of a security badge with specific types and levels of access identified and controlled through the card.
10. Add motion sensors to fences if it is cost effective.
11. Stricter enforcement of HAZMAT requirements.
12. Impose restrictions on flying zones around critical assets. This regulation would reduce the accessibility to the asset and hence reduces vulnerability of the asset.
13. Protect suspension cable in case of suspension and cable stayed bridges.
14. Increased patrol by law enforcement and coast guard and port authorities
15. Immediate removal of abandoned and unclaimed vehicles near assets.
16. Removal of vegetation to provide clear lines of sight.
17. Apprise local law enforcement officials of critical assets.
18. Install advance warning systems in case of important assets. An example is when the entry of every vehicle into a facility is detected and relayed to a monitoring system when the vehicle is still in the driveway.
19. Introduce redundancies in the system, especially in the case of an emergency route.

5.7.1. Choosing an Appropriate Countermeasure for an Asset

All the countermeasures listed above will not be equally effective for all assets. A countermeasure needs to be customized based on the characteristic of the asset. A countermeasure that will work for bridges may not be as effective in the case of buildings. Given specific threats, the effectiveness of countermeasures is measured subjectively by assessing how well its application reduces the potential for and

consequences of attacks. As the risk increases, more and stronger measures should be taken. Managers need to balance between demands for security and the resources needed to enact and finance the measures. After identifying possible countermeasures for an asset, the one that is most cost effective can be chosen for implementation. This can be done by using the cost benefit analysis method. (Laboy-Rodriguez, 2005). The approach should help establish a basis for evaluating and justifying investments, policies and procedural changes. The analysis should include implementation, installation and operating cost of the countermeasure. The benefits can be quantified based on how much less vulnerable the asset is after countermeasure implementation. A countermeasure for which benefits exceed the costs should be chosen. The effectiveness of the measure to reduce vulnerability should also be considered before implementation.

5.7.2. Response and Recovery Measures

The preceding section talks about the countermeasures that either deter or detect the attack. There are countermeasures that help in recovering and restoring the asset. Response is a countermeasure in the sense that effective response and recovery will reduce the number of lives lost. The number of people affected is one of the factors affecting vulnerability. Reducing the number of casualties will reduce vulnerability too. In the case of response as a countermeasure, a disaster may require state and federal agency involvement, activation of special plans and procedures, and extensive coordination of personnel from multiple agencies. Emergency response plans will be discussed in Volume II of this report.

CHAPTER 6. CONCLUSIONS

A secure transportation system is critical to overall national security from terrorism. The events of September 11th 2001 revealed the vulnerability of transportation systems. Surface transportation is important because of its high visibility and public usage. The need to strengthen security measures and to protect the transportation assets has caused the transportation agencies to increase their efforts towards security. The results of such efforts by the federal agencies are the reports published by AASHTO and NCHRP for Vulnerability Assessment and Emergency Response. These reports guide state DOTs in conducting Vulnerability Assessment. Because critical assets differ from state to state, it is necessary for Indiana to assess its own assets and strengthen them against any possible terrorist attacks. In order to strengthen an asset, it is essential to identify ‘which assets to assess?’

To assist agencies in identifying the critical and vulnerable asset and evaluating them for the security levels, this study focused on developing a prioritization method for vulnerability assessment. Once the assets that are highly vulnerable and critical are selected, suitable countermeasures are suggested for implementation. In order to compare assets, there needs to be common measurable criteria. Because assets of different type are considered in this research, identifying common criteria to measure the attributes of these assets that reflect vulnerability is a challenging task. Because of the lack of such a criterion, the study came up with definitions to measure vulnerability and criticality.

Applying these definitions to assets resulted in indices that could be used to identify critical and vulnerable assets.

6.1 Research Contributions

Terrorist attacks can cause massive damage to people, government, assets and economy and such attacks are sudden and unexpected. The most effective strategy is to plan and in advance to prevent such attacks. In order to prevent attacks and minimize disruption and losses, the primary step is to identify what to protect. Because no agency has infinite funds, it is critical to prioritize the assets so important assets can be protected first. Because there are no common measurable characteristics for all asset types, identifying a criteria for comparison is a challenging task.

The study developed a method that can be used to identify critical and vulnerable assets among any asset types. The study identified common criteria based on subjective surveys and expert knowledge to compare assets. Using these criteria, vulnerability and criticality indices are obtained for each asset that can be used to prioritize assets. Once the assets are prioritized in terms of their need for protective measures, appropriate countermeasures can be implemented depending on the agencies available resources. While conducting surveys, clear instructions need to be given to the experts as to the type to the assets to be chosen, and the nature of the threat to consider. The experts need to be trained to consider the most likely threat to the asset that would cause maximum disruption. It is recommended that the assessment process be done as a group to reduce the differences in the perception of the definitions of vulnerability and criticality and their evaluation scales. Clear and consistent understanding of the definitions of vulnerability and criticality will help in reduction in the variation in the results.

6.2 Lessons Learned and Limitations

The study was mainly limited by the subjective nature of the responses and the difficulty in obtaining data. Responses to the survey varied significantly because of the subjective nature of the surveys. The difference in the perception and the interpretation of the factors and the criteria and expert's background and experience could be causes of the variation. Also, because the assets were evaluated at the local level, the statewide perspective is not incorporated into the evaluation process. The larger perspective may be missing in the responses from the districts.

With different types of assets to compare and assess, there needs to be a common basis for ranking. Because such measurable criteria do not exist for a wide variety of statewide assets, this is not the most efficient way to identify the top priority assets. The solution would be to split the assets into their respective categories, such as bridges, routes, equipment and buildings. Assessment can be done within the asset groups using some of the quantifiable or measurable criteria specific to those asset groups. For example, for bridges, measures like span length, AADT and truck volume can be used to build a model. And determine vulnerability and criticality values. Comparison using the vulnerability and criticality indices among similar category assets would lead to more reliable results. Once assets in the each of the categories are prioritized, you could gather a group of experts in a common place and decide which assets to consider, based on the funding availability and the needs and the mission of the agency.

6.3 Recommendations for Further Research

The research here is a preliminary effort in the field of transportation security. Further research in this topic is crucial to better understand the assessment of vulnerabilities of assets and securing them. The following are some of the areas, where further research will enhance the usability of the existing research.

1. Based on the vulnerability assessment conducted in this project, better and consistent results could be obtained if the assessment was conducted as a workshop instead of mail-in surveys. This could possibly reduce the variation in the perception and understanding of various factors that influence vulnerability.
2. The shortcomings in the transportation security area are the absence of significant methodological tools to prevent and manage terrorist attacks. Future studies could concentrate on developing more quantitative tools and methods to evaluate vulnerabilities of assets.
3. The quantitative methods would have large data needs regarding the characteristics of assets. Studies should develop methods to obtain data to identify the likelihood and the consequences of various disruptive events on transportation systems.
4. Future research could also focus on developing models to assess and compare the influences of various factors on component and system level vulnerability.

The data and the models will help decision-makers make informed decisions.

5. There is also a need to clearly define the performance metrics to be used in risk and vulnerability assessment analysis and standardize them. This would help in comparing assets of different types for their vulnerability.
6. Further research could also concentrate on developing workshops to train personnel in assessing vulnerabilities at the local, state and federal level.
7. To incorporate the subjectivity and the uncertainty in the input by the experts, Fuzzy AHP could be used to obtain the criteria weights.

LIST OF REFERENCES

AASHTO Report, 2002. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification*, http://security.transportation.org/doc/guide-VA_FinalReport.pdf as viewed on 25 November, 2004.

Army Field Manual, *Physical Security*, 2001. Army Field Manual FM 3-19.30.

BRP, Blue Ribbon Panel, 2003. "Recommendations for Bridge and Tunnel Security", <http://www.fhwa.dot.gov/bridge/security/brp01.htm> as viewed on 14 June 2004.

Burger, M.S., 1998, "Applying Neural Networks to Risk Assessment", <http://www.audits.uillinois.edu/Publications/IAART5.htm> as viewed on May 24, 2005.

CIAO, 2003. <http://www.ojp.usdoj.gov/odp/docs/vamreport.pdf> as viewed on 30 November, 2004.

DHS, 2003. "Vulnerability Assessment Methodologies Report", <http://www.ojp.usdoj.gov/odp/docs/vamreport.pdf> as viewed on 23 August, 2004.

Executive Order, 1996. http://www.epic.org/security/infowar/eo_cip.html as viewed on 02 February, 2005.

Figueria, Jose', Salvatore Greco, and Matthias Ehrgott, 2005. *Multiple Criteria Decision Analysis, State of Art surveys*, Springer Publications, New York, NY.

Fishburn, P. C., (1967). “Additive utilities with incomplete product set: Applications to priorities and Assignments”, Operations Research Society of America, Baltimore, MD

FTA, 2003. http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/Top20/1%20--%20Management%20and%20Accountability/3B%20--%20Security%20Design%20Criteria/Essential/Security_Risk_Assessment_Framework.doc as viewed on 19 December, 2004.

GAO, 1998. *Domestic Terrorism: Prevention Efforts in Selected Federal Courts and Mass Transit Systems*, General Accounting Office (GAO), Washington, DC.

GAO, 2003. *Post-September 11th Initiatives and Long-Term Challenges*, General Accounting Office testimony before Congress, April 1, 2003, Washington, D.C.

Hamalainen, R. P., E. Kettunen, M. Marttunen, and H. Ehtao, 1999. “Towards Decision and Negotiation Support in Multi-Stakeholder development of lake Regulation Policy”, Proceedings of the 32nd Annual Hawaii intl. Conf. on System Sciences, IEEE Press, Piscataway, NJ.

Hobbs, Benjamin and P. Meier, 2000. *Energy Decisions and the Environment*, Kluwer Academic publishers, Boston, MA.

Husdal, Jan, 2004. “Vulnerability of Road Networks in a Cost-Benefit Perspective” , http://www.husdal.com/gis/trb2005_final.pdf as viewed on 01 January, 2005

Jenkins, Brian Michael and Larry N. Gersten, 2001. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research and Best Security Practices*, Mineta Transportation Institute, MTI Report 01-07, San Jose, CA.

Laboy-Rodriguez, Sylvia, 2005. *A cost effective model to evaluate anti-terrorist countermeasures for bridges*, Masters Report, Purdue University.

Miller, D.W., and M.K. Starr, 1969. *Executive Decisions and Operation Research*, Prentice-Hall, mc, Englewood Cliffs, NJ.

NIAC, 2004. *Common vulnerability scoring system*, National Infrastructure Advisory Council.

Polzin, Steven E, *Security considerations in Transportation Planning*, Southeastern Transportation Center. <http://stc.utk.edu/htm/pdf%20files/web/webcomstc.pdf> as viewed on 16 August, 2004

Primode, <http://www.primode.com/glossary.html> as viewed on 12 October, 2004

Physical Security, 2001. Field Manual, No. 3-19.30, Department of the Army, Washington, DC.

Physical security risk analysis, 2004
<http://security.lifesafety.ca/2004articles/2004sec047.htm> as viewed on 08 February, 2005

Rummel, T., Hyzak, M. and Ralls, M.L., 2003. "Transportation Security Activities in Texas", Texas Department of Transportation, Austin.

SAIC, 2005. "Reducing Security Risk for Transportation Management Centers", presented at 84th Annual Transportation Research Board Meeting, 2005.

Saaty, T.L., 1980. *The Analytic Hierarchy Process*, McGraw Hill, New York, NY.

Saaty, T.L., 2000. *Fundamentals of Analytic Hierarchical Process*, RWS Publications, Pittsburgh, PA.

Srinivasan, Karthik., 2004. "Transportation Network Vulnerability Assessment: A quantitative framework", Southeastern Transportation Center.,
<http://stc.utk.edu/htm/pdf%20files/web/webcomstc.pdf> as viewed on 30 January, 2005.

Stergiou, Christos, 1999. "Neural Networks",
http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html#What%20is%20a%20Neural%20Network as viewed on May 25, 2005.

Stewart, T.J., 1992. "A Critical Survey on the Status of multiple Criteria Decision Making Theory and Practice". OMEGA,20(5/6), 569-586.

Triantaphyllow, Evangelos, 2000. *Multi-Criteria Decision making Methods: A Comparative Study*, Kluwer Academic Press, Boston, MA.

Xia, J., Chen, M., Lie, R., 2004. "A Framework for risk assessment of Highway network", presented at the 84th Annual Transportation Research Board Meeting.

Zadeh, L.A., 1965. "Fuzzy Sets", Information and Control, Vol. 8, pp.338-353.