FHWA NJ 2006-011

Simple Bridge Security Inspection

FINAL REPORT
September 2006

Submitted by

Hani Nassif [1]
Associate Professor

Layla Issa[1]
Graduate Student
Joe Davis[1]
Research Associate

Husam Najm[1]
Associate Professor

[1]Dept. of Civil & Environmental Engineering
Rutgers, The State University
Piscataway, NJ 08854-8014

NJDOT Research Project Manager
Mr. Edward S. Kondrath

In cooperation with

New Jersey
Department of Transportation
Bureau of Research
And
U. S. Department of Transportation
Federal Highway Administration

DISCLAIMER STATEMENT

"The contents of this report reflect the views of the author(s) who is (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 New Jersey Department of Transportation or the Federal Highway Administration. This report does not constitute a standard, specification, or regulation."

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

TECHNICAL REPORT
STANDARD TITLE PAGE

1. Report No. FHWA NJ-2006-011	2.Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Simple Bridge Security Inspection		5. Report Date September 2006
		6. Performing Organization Code CAIT/Rutgers
7. Author(s) Hani Nassif, Layla Issa, Husam Najm, and Joe Davis,		8. Performing Organization Report No. FHWA-NJ-2006-011
9. Performing Organization Name and Address Dept. of Civil & Environmental Engineering Center for Advanced Infrastructure & Transportation (CAIT) Rutgers, The State University Piscataway, NJ 08854-8014		10. Work Unit No.
		11. Contract or Grant No.
12. Sponsoring Agency Name and Address New Jersey Department of Transportation PO 600 Trenton, NJ 08625	Federal Highway Administration U.S. Department of Transportation Washington, D.C.	13. Type of Report and Period Covered Final Report 01/01/06 – 10/31/06
		14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Bridges are among the most visible targets for terrorists since their destruction will have an immediate as well as long-term economical and psychological impact on the nation. Enhancing bridge security is key to improving homeland security and it entails several steps including on-site assessment, analysis of different security components, and implementing some mitigation measures that will enhance bridge security. Current guidelines for bridge security assessment are insufficient. Several sessions were initiated by the FHWA, AASHTO, and ASCE to provide Federal and State Departments of Transportation (DOT's) with general guidelines for safety and security assessment of bridges. Literature review of bridge security showed that there is a need to develop methods to identify critical bridges for security hazards and to provide engineering standards and guidelines for bridge security design to reduce their vulnerability to attacks. In particular, there is a need to better understand structural response of key components of a bridge to mitigate collapse, loss of life, and disruption of traffic. A simple bridge security checklist was developed to provide on-site assessment of bridge security. The developed checklist was implemented on a Tablet PC and applied to various bridge case studies to assess their vulnerability and security risk.

17. Key Words Bridge Structure, Security, Inspection, Checklist, Database, Threat.	18. Distribution Statement

19. Security Classif (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No of Pages 47	22. Price

Acknowledgements

The authors would like to thank the New Jersey Department of Transportation (NJDOT) and staff for their help and support of this project: Ed Kondrath, Harry Capers, Jr. (retired), Jose Lopez (retired), and Richard Dunne, for their help and assistance throughout the project. Thanks are due to Harold Neil (retired) and Kenrick Layne from the New Jersey Office of Homeland Security and Preparedness (OHSP) for their comments and suggestions. Also, the assistance of John Abruzzo from Thornton Tomasetti and Rutgers student Suhail Al-Bhaisi are thankfully acknowledged.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Bridges are among the most visible targets for terrorists since their destruction will have an immediate impact on the nation with long-term economical and psychological impacts. The terrorist attack on September 11th, 2001 crippled the PATH commuter rail that carried 67,000 passengers each weekday for two years resulting in relocation of office space and jobs to New Jersey[1]. Since then, funding for homeland security has increased by approximately 8.6 percent for the fiscal year 2006, in which 38.6 percent are allocated for Border and Transportation Security[2]. Bridge security is important enough to be a matter of state and national security. Bridges are lifeline structures for the state and the federal transportation system that need to be protected against terrorist threats.

The Blue Ribbon Panel on Bridge and Tunnel Security had provided recommendation and guidelines to assist State DOT's implement transportation infrastructure security[1]. The guidelines divided the security program into seven approaches: 1) Strategy for Bridge and Tunnel Security, 2) Planning, Design, and Engineering, 3) Prioritization and Risk Assessment, 4) Threats, 5) Damage, 6) Countermeasures, and 7) Code and Specification. They recommended the use of prioritization and risk assessment methods to enhance bridge and tunnel security. The prioritization and risk assessment should be based on the National Bridge Inventory System (NBIS) for bridge structures by using information such as location, traffic volume, structure type, span, significance, criticality, etc. They also formulated a risk factor, which is a function of occurrence, vulnerability, and importance. This included a list of critical bridge components that were prone to blast load, and how to determine the magnitude of threats by listing possible scenario of threats and their corresponding magnitude. Additionally, examples of mitigation were also described. To achieve an acceptable and reliable level of bridge security, several steps have to be taken. They include: (1) establishing security hazard and performance levels, (2) analysis of vulnerable bridge components and member details, (3) on-site assessment through security checklist, and finally (4) implementing some mitigation measures that will enhance bridge security.

The objective of this project will be to establish a simple security checklist that can provide accurate security assessment for each individual bridge. The objective is to be implemented by developing a Tablet PC-based system that could be downloaded into a bridge security database.

Despite the details contained in various published literature, there is insufficient information for what bridge inspectors should be looking for and what a bridge security checklist should include. There is a need for a detailed checklist for security inspection based upon which vulnerability assessment as well as mitigation plans can be planned. A review of the literature of bridge security showed that there is a need to develop methods to identify critical bridges for security hazards, to provide engineering standards and guidelines for bridge

security design in order to reduce their vulnerability to attacks, and to better understand the structural response of key components of a bridge to mitigate collapse, loss of life and disruption of traffic. A comprehensive security checklist was developed to provide on-site assessment of bridge security and a Tablet PC-based checklist was also provided. The developed checklist will be applied to a bridge case study.

OBJECTIVES

The main objectives of this project are:

1. Establish security hazard levels and performance objectives for New Jersey bridges in coordination with NJDOT Office of Transportation Security (OTS) and the Office of Homeland Security and Preparedness (OHSP).
2. Identify critical components in a typical bridge that are vulnerable to blast and impact loads.
3. Develop a simple bridge security checklist to perform on-site assessment of bridge components based on the results of Tasks 1 and 2.
4. Develop a Tablet PC-based program of the security measures checklist developed in Task 3 that can be downloaded into an NJDOT bridge security database.
5. Apply developed checklist to bridge case studies.

BACKGROUND

Bridge security is important enough to be a matter of state and national security. Bridges are lifeline structures for the state and the federal transportation system that need to be protected against terrorist threats. Current guidelines for bridge security assessment are considered insufficient due to the lack of established guidelines for security inspection. Review of the literature revealed that there is no clear and specific guides or methodologies available to assess the vulnerability of bridges to the effects of blast loads. Moreover, infrastructure systems constitute a major part of the national investment, which are critical for the mobility of our society as well as its economic growth and prosperity. The U.S.A. has an estimated $25 trillion investment in civil infrastructure systems, including all installations that house, transport, transmit, and distribute people, goods, energy, resources, services and information. Bridge structures, considered one of the most important components of this infrastructure system, are considered assets that should be protected and properly secured. Yet, the risk of exposure to natural as well as malicious disasters, coupled with the degree of deterioration, is dangerously high. Critical decisions must be made to allocate the available, but limited funds, for securing, safeguarding, and maintaining New Jersey’s infrastructure bridge network. This study will focus on developing simple inspection checklist for assessing the vulnerability of bridges due to malicious attack from blast, fire, and impact.

As the nation's most densely populated state and a hub for the nation's transportation, agricultural, petrochemical and other critical infrastructures, and a neighbor of the major cities, New York and Philadelphia, New Jersey is both vulnerable to terrorism and an ideal test bed for new methods and tools in security assessment of bridges and other type of structures. The need for efficient (accurate, inexpensive, non-obstructive to occupants or users) security assessment checklist is obvious. Various organizations such as FHWA/USDOT, NJDOT, NSF, and AASHTO/NCHRP are supporting major initiatives in the area of homeland security and vulnerability assessment for various infrastructure applications. The basis for these decisions should be based on an accurate assessment of the actual needs and status of various bridge structures.

Transportation infrastructure is one of most visible targets for terrorists since its destruction does not only cause an immediate impact on the nation, but also long-term economical impact. The terrorist attack on September 11th, 2001 crippled the PATH commuter rail that carried 67,000 passengers each weekday for two years resulting in relocation of office space and jobs to New Jersey[1]. Since then funding for homeland security has increased by approximately 8.6 percent for the fiscal year 2006, in which 38.6 percent are allocated for Border and Transportation Security[2]. However, spending alone is not the solution since both Federal and State agencies have modest expertise in implementing security for the nation's infrastructures. Thus, an initiative by AASHTO to provide Federal and State Departments of Transportation (DOT's) with general guidelines for safety assessment[1, 3]. The Blue Ribbon Panel on Bridge and Tunnel Security had provided recommendation and guidelines to assist State DOT's implement transportation infrastructure security[1]. The guideline divided the security program into seven approaches: 1) Strategy for Bridge and Tunnel Security, 2) Planning, Design, and Engineering, 3) Prioritization and Risk Assessment, 4) Threats, 5) Damage, 6) Countermeasures, and 7) Code and Specification. They recommended the use of prioritization and risk assessment methods to enhance bridge and tunnel security. The prioritization and risk assessment should be based on the National Bridge Inventory System (NBIS) for bridge structures by using the information such as the location, traffic volume, structure type, span, significance, criticality, etc. They also formulated a risk factor, which is a function of occurrence, vulnerability, and importance. This included a list of critical bridge components that were prone to blast load and how to determine the magnitude of threats by listing possible scenario of threats and their corresponding magnitude. Additionally, examples of mitigation were also described. Despite the details contained in the document, there is insufficient information for what bridge inspectors should be looking for and what a bridge security checklist should include. There is a need for a detailed checklist for security inspection based upon which vulnerability assessment as well as mitigation measures can be planned.

LITERATURE SEARCH

The American Association of State Highway and Transportation Officials (AASHTO) and the Federal Highway Administration (FHWA) assembled a blue-ribbon panel (Bridge and Tunnel Security 2003) of engineers, researchers, contractors, and owners and operators of infrastructure to discuss how to protect the nation's bridges and tunnels. The panel had provided recommendations and guidelines to assist State Department of Transportation (DOT) implement transportation infrastructure security. The guideline divided the security program into seven approaches:

1. **Overall Strategy of Bridge and Tunnel Security** – it includes a broad range of issues that must be addressed to ensure that adequate measures are taken to protect the asset and the people and goods that utilize the asset.
2. **Framework for Planning, Design, and Engineering** – it considers determining the damages and identifying critical bridges/tunnels through prioritization and risk assessment.
3. **Prioritization and Risk Assessment** – this will identify the likely targets and select methods to defeat the attack. There is also a need to determine the financial impact to deter and provide defense compared to the facility and social cost from the loss and allocate available funds appropriately.
4. **Threats** – different types of threat need to be considered in order to identify the design loads.
5. **Damage** – considers anything that would result in replacement of the facility or major repairs, closure of the facility for more than a month, or any catastrophic failure resulting from an attack.
6. **Countermeasures** – grouped into actions or technologies to deter attack, deny access, detect presence, defend the facility, or design structural hardening to minimize consequences to an accepted level.
7. **Codes and Specifications** – touches on how to employ hardening design, how to quantify blast-related demand, and how to determine the capacity of components exposed to high-pressure transients.

The Blue Ribbon Panel (2003) also recommended the use of the National Bridge Inventory (NBI) maintained by FHWA for prioritization and risk assessment. NBI contains data about bridges including location, structure type, span characteristics, average daily traffic volume, military significance, and others. According to FHWA (The Blue Ribbon Panel on Bridge and Tunnel Security 2003), there are about 600,000 bridges in the United States, raising the question on how to decide which bridges are more at risk and which ones should receive attention first. They then formulated a ***risk factor*** (which is a function of occurrence – that is the likelihood that a basic threat will occur against a given structure), ***vulnerability of the structure*** (how much damage or destruction and what effect that destruction would have), and ***importance of the structure*** (which measures the consequences to the region or the nation in the event that the structure is destroyed or rendered unusable).

Similar findings were also described by Rowshan et. al (2003) by highlighting five steps for conducting a highway vulnerability assessment: 1) Identify Critical Assets, 2) Assess Vulnerabilities, 3) Assess Consequences, 4) Identify Countermeasures, and 5) Review Security Operational Planning. They also derived critical asset and vulnerability factors to help in prioritizing highway infrastructures. Additionally, they developed three levels of countermeasures: 1) Deterrence, 2) Detection, and 3) Defense. They also suggested to link countermeasures with their associated cost and recommended that State DOT's develop a plan for training their staff on how to implement bridge security.

Anderson et. al (2005) used a model called the Inoperability Input-Output Model (IIM) to calculate the losses and to describe the impact from an attack. The model was developed by Nobel Prize-winning economist Wassily Leontief. The term inoperability stands for the level of the system's dysfunction. It is assumed that the bridges are completely inoperable which means there is 100% loss and it will take one year to recover. This results in two major types of losses: 1) transportation loss – taken from the average daily traffic data published by Virginia DOT and 2) workforce loss – the amount of hours of work missed by individuals if they could not use the bridge. After calculating the losses, six characteristics were introduced to help develop risk: 1) prevention, 2) detection, 3) hardening, 4) preparedness, 5) response, and 6) recovery. Risk management techniques were also used to identify and quantify risks to three bridge-tunnels (selected as examples for this study) as well as measure the costs and benefits.

Leung et. al (2004) presented a two level risk assessment system: (1) system level, and (2) asset-specific level. This will help experts and decision makers within the transportation organization to determine which assets should be considered critical and therefore need to be protected. The process of this framework is called the Risk Filtering, Ranking and Management (RFRM) method (see Figure 1). It builds on Hierarchical Holographic Modeling (HHM) to identify risks, then filters and ranks the sources of risks, allowing experts to focus on the most critical one. The prioritized risks are further evaluated in the risk management phase. Finally, the process is reviewed and improved, if necessary.

The main goal and purpose of the National Infrastructure Protection Plan (NIPP) is to:

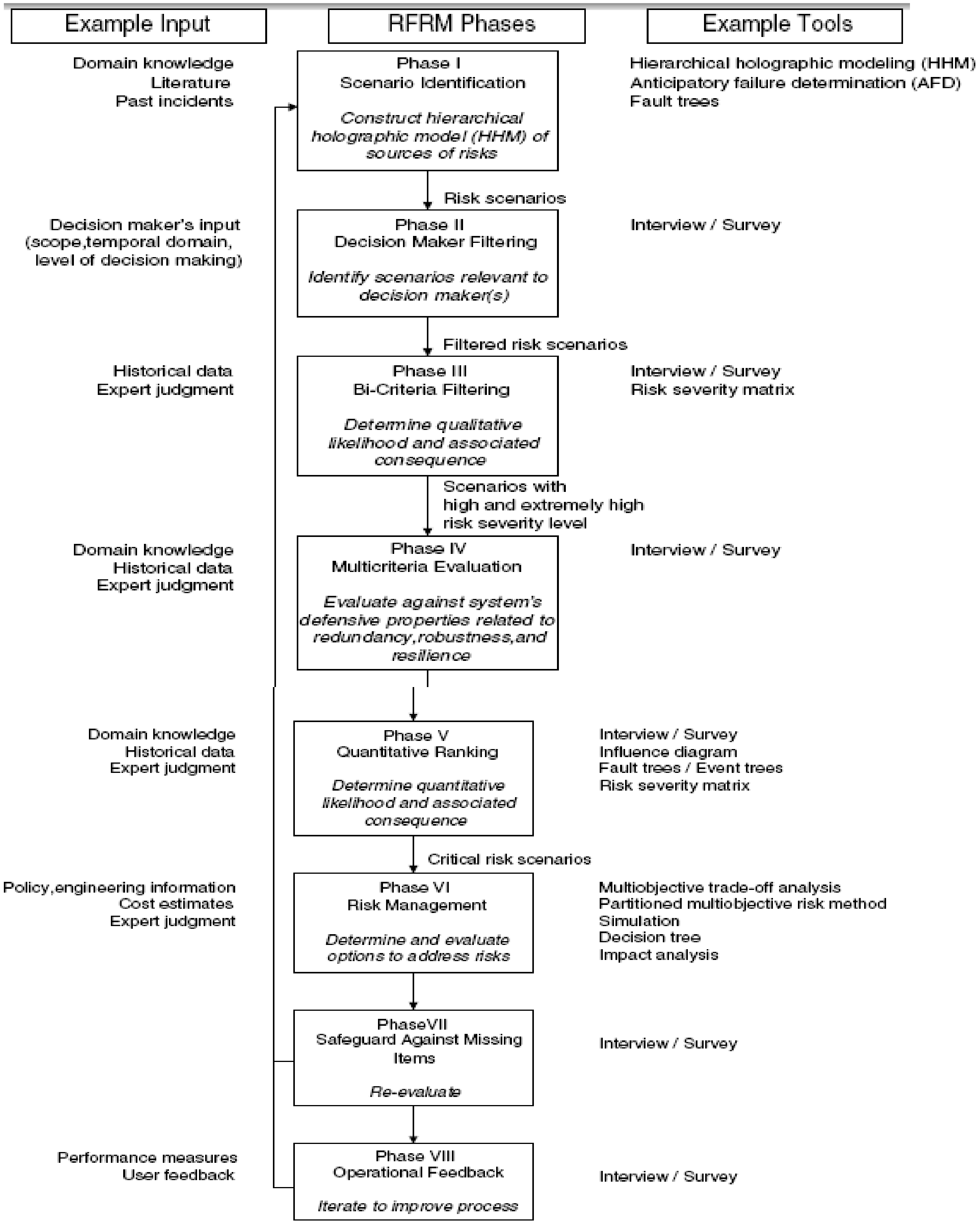

Example Input
RFRM Phases
Example Tools
Domain knowledge
Literature
Past incidents
Phase I
Scenario Identification
Construct hierarchical holographic model (HHM) of sources of risks
Hierarchical holographic modeling (HHM)
Anticipatory failure determination (AFD)
Fault trees
Risk scenarios
Decision maker's input (scope,temporal domain, level of decision making)
Phase II
Decision Maker Filtering
Identify scenarios relevant to decision maker(s)
Interview / Survey
Filtered risk scenarios
Historical data
Expert judgment
Phase III
Bi-Criteria Filtering
Determine qualitative likelihood and associated consequence
Interview / Survey
Risk severity matrix
Scenarios with high and extremely high risk severity level
Domain knowledge
Historical data
Expert judgment
Phase IV
Multicriteria Evaluation
Evaluate against system's defensive properties related to redundancy,robustness,and resilience
Interview / Survey
Domain knowledge
Historical data
Expert judgment
Phase V
Quantitative Ranking
Determine quantitative likelihood and associated consequence
Interview / Survey
Influence diagram
Fault trees / Event trees
Risk severity matrix
Critical risk scenarios
Policy,engineering information
Cost estimates
Expert judgment
Phase VI
Risk Management
Determine and evaluate options to address risks
Multiobjective trade-off analysis
Partitioned multiobjective risk method
Simulation
Decision tree
Impact analysis
PhaseVII
Safeguard Against Missing Items
Re-evaluate
Interview / Survey
Performance measures
User feedback
Phase VIII
Operational Feedback
Iterate to improve process
Interview / Survey

Figure 1: Risk Filtering, Ranking, and Management (RFRM) Method (Leung 2004)

"Build a safer, more secure, and more resilient American by enhancing protection of the Nation's critical infrastructure and key resources (CI/KR) to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency" (NIPP 2006).

Blast-resistant design has traditionally been considered only for essential government buildings, military structures, and petrochemical facilities. Recently, increased attention has been given to bridges. However, engineers have not considered security in the design process. More research will be done to enhance physical security, improve structural response, or mitigate the consequences of an attack. Barrier protection for impact is considered in highway design and for protection of piers in navigable waterways. Nevertheless, these are intended for accidental collision and not malicious attacks.

Figure 2 illustrates the type of protections needed to manage risks and actions that should be implemented (NIPP 2006).

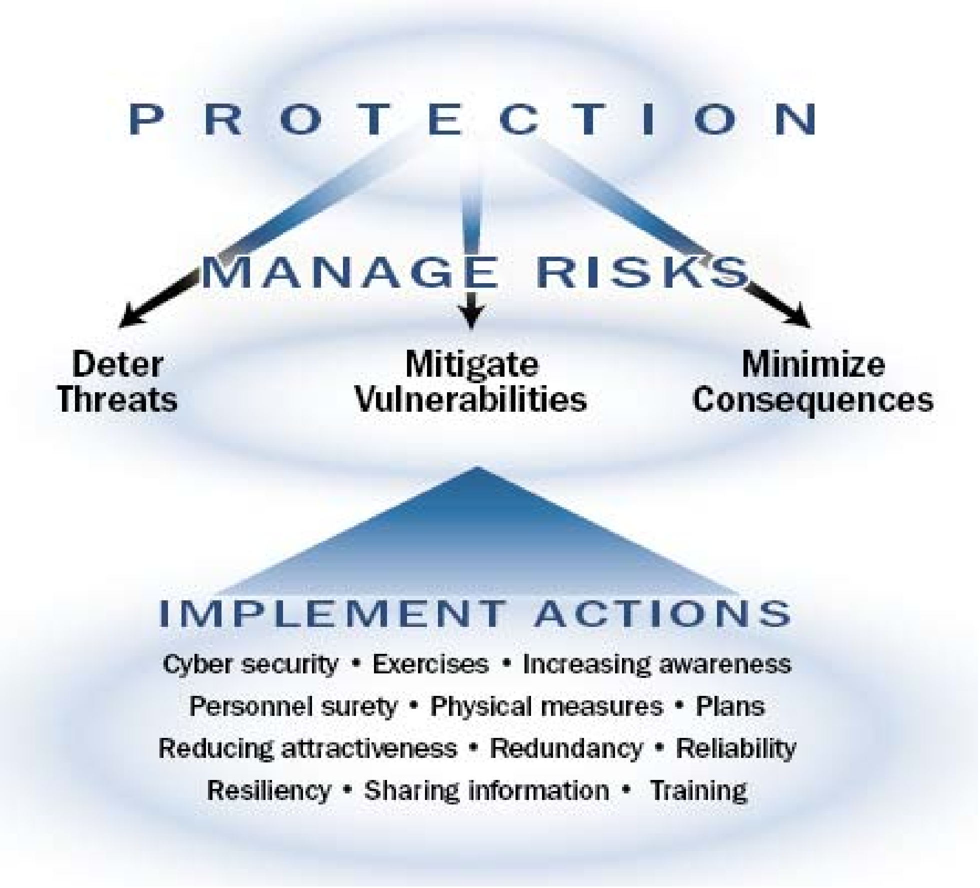

PROTECTION
MANAGE RISKS
Deter Threats
Mitigate Vulnerabilities
Minimize Consequences
IMPLEMENT ACTIONS
Cyber security • Exercises • Increasing awareness
Personnel surety • Physical measures • Plans
Reducing attractiveness • Redundancy • Reliability
Resiliency • Sharing information • Training

Figure 2: Protection Flow Chart (NIPP 2006)

According to Müllers and Vogel (2005), the vulnerability of flat slab structures made out of reinforced concrete is very important to investigate because the collapse of such a building can lead to fatal consequences. Even though this addresses buildings and not bridges, the analysis is very similar because it deals with column failure. Column failure is hazardous since it could end in a progressive collapse. Hence, investigations are made and key parameters, such as failure time, physical non-linearity, geometrical non-linearity, damping and/or strain-rates are identified with the aid of simple mechanical model. It was assumed that the failure time would be close to zero. A non-linear structural behavior was considered and damping and strain-rate effects were neglected for calculations of forces. This resulted in three methods for column failure design of a structure: 1) a displacement-based design analyzed by energy balance, 2) a capacity design according to seismic design methods, or 3) a non-linear dynamic finite element analysis. From that model, it was concluded that the column failure time influences the effect of actions in the remaining structure significantly.

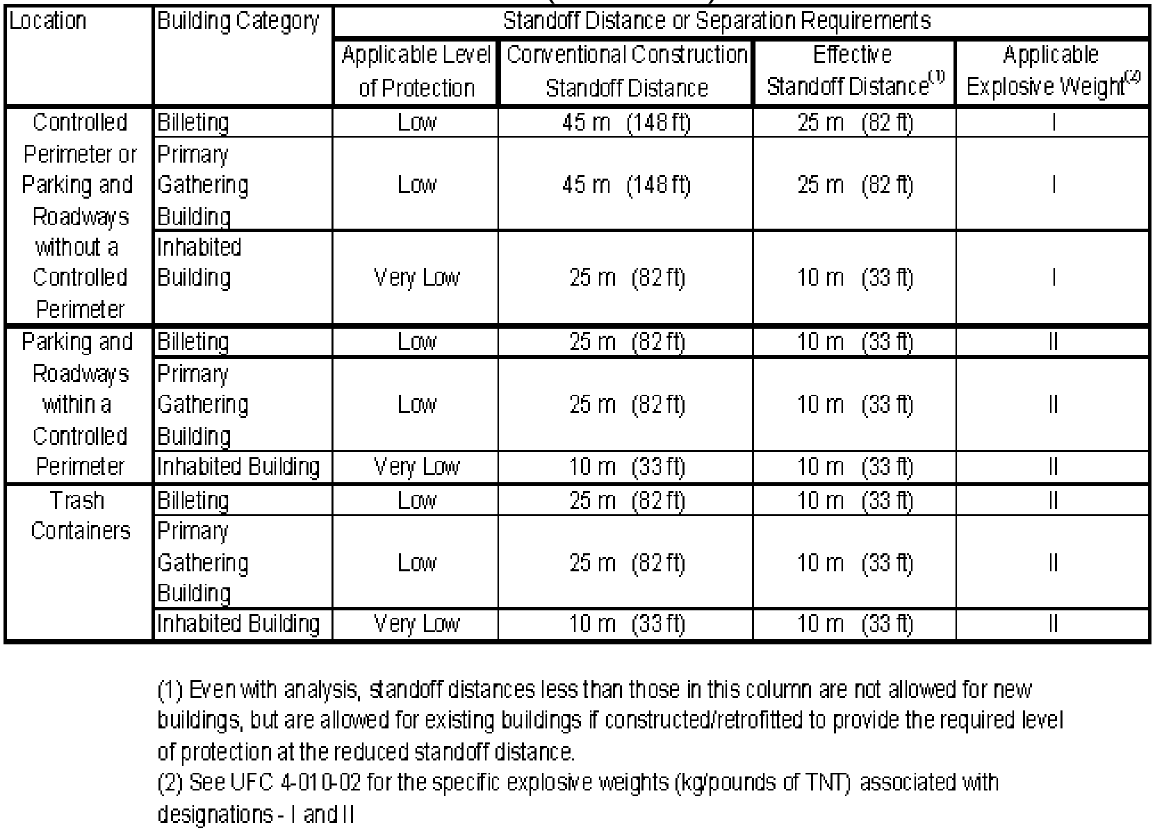
Winget et. al (2005) indicated that developing an understanding of the principles of blast wave propagation and its potential effects on bridge structures is the first step that should be taken before engineers can begin to design bridges to withstand blast loads. A project manager or a security professional should perform a preliminary risk assessment to determine which threats the bridge may face. Once the potential threats have been identified, measures can be implemented to mitigate those risks. These measures can be used to displace the threat to less attractive targets, increase the likelihood of terrorists being detected and identified, keep casualties to a minimum, improve emergency response time, increase public confidence, improve structural response, or a combination of these events (Jenkins 2001).

In their paper, Winget et. al (2005) mentioned that the most common analysis method used in practice is a single- or multiple-degree-of-freedom, uncoupled, nonlinear dynamic analysis. BlastX version 4.2.3.0 (BlastX 2001) was used to generate loads. To calculate the reduced area of the columns due to local blast damage, empirically based spall and breach equations developed by Marchand and Plenge (1998) were used. To predict the local breaching damage for counterforce scenarios on small diameter piers, the rule of thumb in FM 5-250 (Department of the Army 1992) was used, which indicates the amount of TNT per foot for concrete to be breached. To calculate the flexural response of the piers to vehicle blast loads, SPAn32 version 1.2.7.2 (SPAn32 2002) was used. After the analyses were made, the results showed that bridge geometry could significantly affect the blast loads that develop below the deck. For bridges with deep girders, confinement effects can greatly enhance the blast loads acting on the girders and tops of the piers. In some cases effects may result in more damage than an explosion occurring on top of the deck. Higher clearances result in lower average loads on the piers due to the larger volume of space under the bridge and the increased average standoff distance to a given point on the pier.

Explosions occurring near sloped abutments could possibly result in more damage than an explosion at midspan due to the confinement effects at the abutments. In addition, round columns will experience lower loads due to the increased angle of incidence from the curved surface.

Prior to September 11, 2001, the Department of Defense and other agencies of the U.S. Government had developed a number of engineering design documents that provided guidance for protection of government assets against terrorist and criminal acts (Betts 2005). Including in these documents, Table 1, which discusses the standoff, distances at which construction can resist the minimum explosive weights and achieve the minimum levels of protection. Table 2 describes the levels of protection associated with 1) Potential Structural Damage, 2) Potential Door and Glazing Hazards, and 3) Potential Injury.

Table 1: Minimum Standoff Distances (Betts 2005)



Location	Building Category	Standoff Distance or Separation Requirements			
		Applicable Level of Protection	Conventional Construction Standoff Distance	Effective Standoff Distance[1]	Applicable Explosive Weight[2]
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Billeting	Low	45 m (148 ft)	25 m (82 ft)	I
	Primary Gathering Building	Low	45 m (148 ft)	25 m (82 ft)	I
	Inhabited Building	Very Low	25 m (82 ft)	10 m (33 ft)	I
Parking and Roadways within a Controlled Perimeter	Billeting	Low	25 m (82 ft)	10 m (33 ft)	II
	Primary Gathering Building	Low	25 m (82 ft)	10 m (33 ft)	II
	Inhabited Building	Very Low	10 m (33 ft)	10 m (33 ft)	II
Trash Containers	Billeting	Low	25 m (82 ft)	10 m (33 ft)	II
	Primary Gathering Building	Low	25 m (82 ft)	10 m (33 ft)	II
	Inhabited Building	Very Low	10 m (33 ft)	10 m (33 ft)	II

(1) Even with analysis, standoff distances less than those in this column are not allowed for new buildings, but are allowed for existing buildings if constructed/retrofitted to provide the required level of protection at the reduced standoff distance.
(2) See UFC 4-010-02 for the specific explosive weights (kg/pounds of TNT) associated with designations - I and II

Table 2: Qualitative Levels of Protection (Betts 2005)

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Below AT standards	Severely damaged. Frame collapse/massive destruction. Little left standing	Doors and windows fail and result in lethal hazards	Majority of personnel suffer fatalities
Very Low	Heavily damaged - onset of structural collapse: Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements.	Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards.	Majority of personnel suffer serious injuries. There are likely to be a limited number (10% to 25%) of fatalities.
Low	Damaged - unrepairable. Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely.	Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel suffer serious injuries. There may be a few (<10%) fatalities.
Medium	Damaged - repairable. Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members.	Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable.	Some minor injuries, but fatalities are unlikely.
High	Superficially damaged. No permanent deformation of primary and secondary structural members or non-structural elements.	Glazing will not break. Doors will be reusable.	Only superficial injuries are likely.

Mays and Smith (1995) introduced in their paper the standoff distances of an explosion that will produce internal flying glass in a building. This is illustrated below in Table 3.

Princehorn et. al (2005) compared in Table 4 the effects of a blast and earthquake on a reinforced concrete or steel structures. Analyses concluded that earthquake designs typically focus on the performance of upper levels of buildings, whereas blast-resistant designs should focus on the lower stories, which are subjected to higher force levels.

Table 3: Stand-off Distances to Produce Internal Flying Glass (Mays and Smith 1995)

Device	Stand-off (in meters) to shatter 4mm annealed glass
Small package	10
Small briefcase	14
Large briefcase	20
Suitcase	26
Car	60
Small van	120
Large van	140
Small truck	160
Large truck	200

Unlike natural disasters, man-made attacks are unpredictable and it can summarized by the following statement: “To manage risk, one must measure it” (Haimes 2002). To calculate the likelihood that such an act would take place at a certain time and place is beyond possibilities. However, to simplify things, different approaches were taken to calculate risk. Haimes (2002) introduces a model of homeland and terrorist networks (see Figure 3) as a system. Its outputs are the same as the four sources of risk that constitute the input to the homeland system. These sources are as follows:

- Risk to human lives and to individual property, liberty, and freedom;
- Risk to organizational-societal infrastructures, and to the continuity of government operations, including the military and intelligence-gathering infrastructures;
- Risk to critical cyber-physical infrastructures; and
- Risk to economic sectors.

Table 4: Comparison of Blast and Earthquake Effects on Reinforced Concrete or Steel Structure (Princehorn and Laefer 2005)

Blast	Earthquake	Implications
Adjacent structures are susceptible. Floor slabs and beams most vulnerable to upward pressure and may shatter. Weaker columns may be destroyed, but larger, heavily loaded columns are often not initially shattered.	Damage to brittle vertical supporting elements, while floor slabs and beams usually have minimal initial damage.	Seismic column designs may be applied to blast designs, but seismic beam and floor slab design would be inappropriate.
Pressures radiate from point of detonation and decay rapidly with distance and time. As shock wave passes over building, pressure direction may change.	Affects entire structure and damage occurs because of mismatches in the strength/ stiffness ratio of structural members. Irregularities focus the damage on more vulnerable areas (softer and higher stories, and longer columns). Shaking matches earthquake duration; may exceed 60sec.	Blast resistance should focus on lower and exterior portions of the building, whereas seismic intervention is focused on upper levels and is more uniform in impacting all structural components.
Shattered floors reduce lateral support that can lead to adjacent columns buckling and then the collapse of bays in the structure. If columns are shattered, floor collapse is inevitable.	High lateral loads can compromise or damage vertical supports. Without enough vertical support, relatively undamaged floors will fall onto one another, causing a pancake type collapse.	Hardening lateral elements are higher priority in blast design. Seismic design requires lateral loads to be transferred/absorbed without significantly mitigating vertical structural components.
Secondary collapse is possible especially if rescue operations require removal of collapsed slab structures that have become the temporary lateral bracing to the remaining, free standing columns.	Aftershocks will cause additional lateral loading, which may readjust load paths, causing a secondary collapse.	Progressive collapse analysis is typically performed for seismic designs and can, therefore, be applied to blast designs.

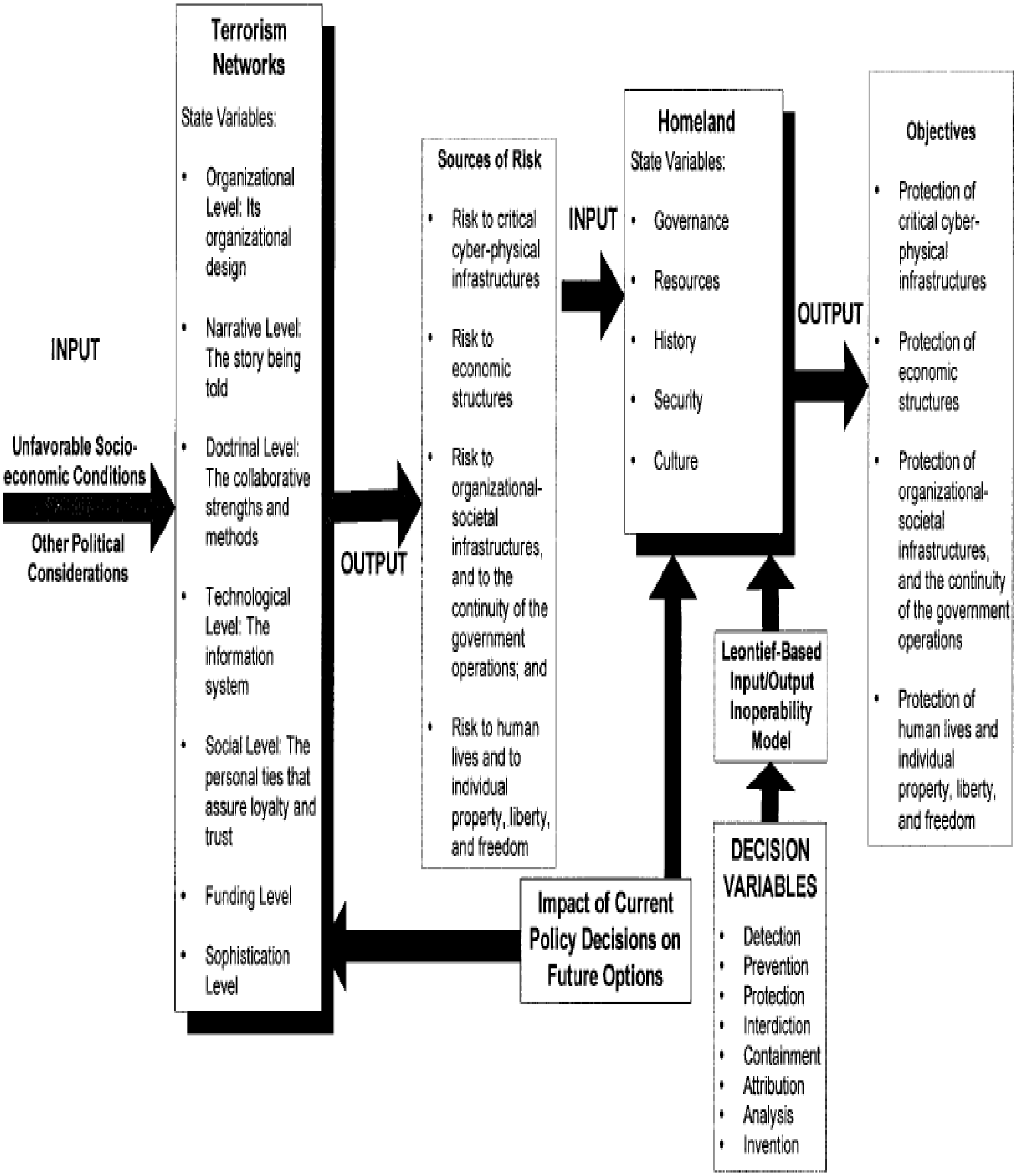

Terrorism Networks
State Variables:
• Organizational Level: Its organizational design
• Narrative Level: The story being told
• Doctrinal Level: The collaborative strengths and methods
• Technological Level: The information system
• Social Level: The personal ties that assure loyalty and trust
• Funding Level
• Sophistication Level
INPUT
Unfavorable Socio-economic Conditions
Other Political Considerations
OUTPUT
Sources of Risk
• Risk to critical cyber-physical infrastructures
• Risk to economic structures
• Risk to organizational-societal infrastructures, and to the continuity of the government operations; and
• Risk to human lives and to individual property, liberty, and freedom
INPUT
Homeland
State Variables:
• Governance
• Resources
• History
• Security
• Culture
OUTPUT
Objectives
• Protection of critical cyber-physical infrastructures
• Protection of economic structures
• Protection of organizational-societal infrastructures, and the continuity of the government operations
• Protection of human lives and individual property, liberty, and freedom
Leontief-Based Input/Output Inoperability Model
DECISION VARIABLES
• Detection
• Prevention
• Protection
• Interdiction
• Containment
• Attribution
• Analysis
• Invention
Impact of Current Policy Decisions on Future Options

Figure 3: Model of Homeland and Terrorist Networks System (Haimes 2002)

Probabilistic Risk Assessment (PRA) is typically characterized as the quantification of the likelihood and severity of an adverse outcome. PRA-based prioritization techniques are well developed for natural and accidental hazards (Basoz 1995), but not to hazards related to man-made destructions. Even though there are differences between security and natural hazard risk, the PRA-based approach could be used to quantify risk and provide information needed to make rational and cost-effective risk management decisions.

King et al. (2005) measures risk by decomposing it into three components that can be quantified: O (Occurrence), V (Vulnerability), and I (Importance). Risk is written as the product of the three components as follows:

$$\text{Risk} = O \times V \times I$$

According to King et. al (2005), Occurrence (O) is the hazard model used to characterize the probability of an initiating event occurring. There are no extensive historical databases for security related hazards due to their subjective and dynamic nature. For this reason, occurrence is taken as the relative likelihood of occurrence rather than a probability in some future time period. Vulnerability (V) is the damage or fragility model used to characterize the outcome or consequences of the event's occurrence. Importance (I) is used to characterize the criticality or the social and economic impact of a facility's operation on the region, the owner, and the society at large.

The majority of the publicly available security risk assessment methods can be characterized as one of the following three general types (Kings and Isenberg, 2005):

1) Scoring/screening techniques;
2) Event and fault tree approaches; and
3) Scenario-based analyses.

Scoring techniques are most often used for cursory evaluation of a large range of facilities and screening or prioritizing a sub-set for further assessment or mitigation considerations. An example of a scoring/screening method is the AASHTO Guide to Vulnerability Assessment for Critical Asset Identification and Protection (AASHTO, 2002). Figure 4 shows a scatter plot of Criticality versus Vulnerability that is used to identify the facilities with the highest risk.

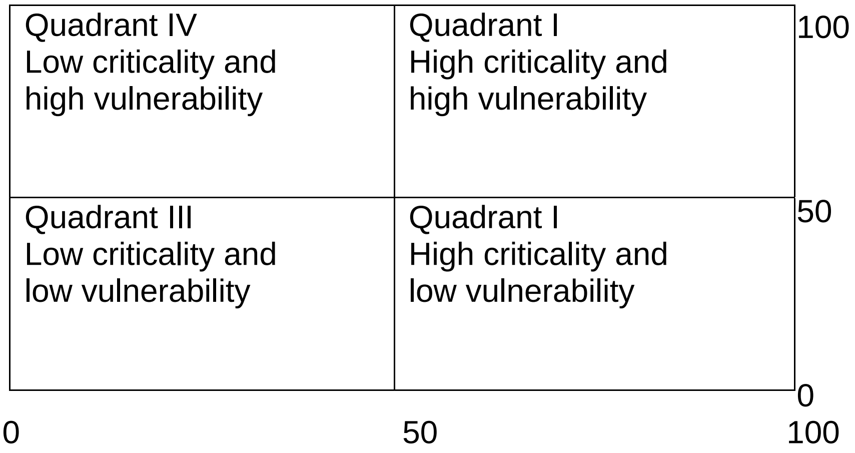
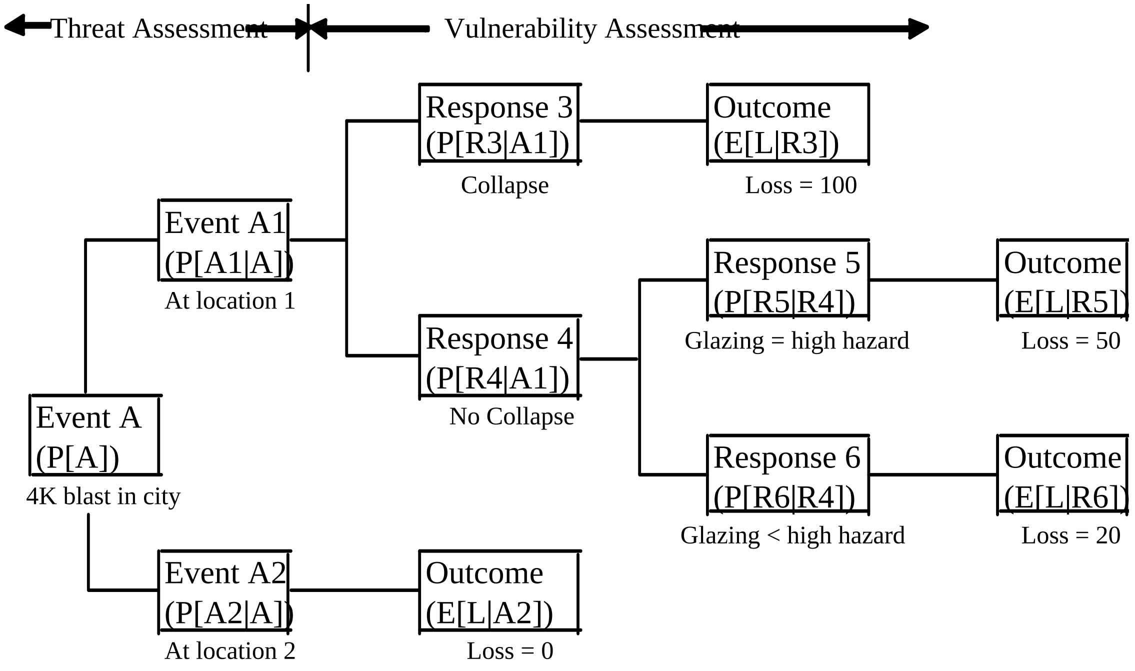


Figure 4: Criticality and Vulnerability Scatter Plot

Event tree analysis and fault tree analysis are quantitative risk assessment techniques often used to evaluate risk for natural or accidental hazards to individual facilities. However, they could be used for security risk assessment since they provide a means for modeling of the basic components of risk. Figure 5 shows an example of an event tree analysis for a security risk application.



Risk = E[Loss] = P[A]xP[A1|A]xP[R3|A1]x100
+ P[A]xP[A1|A]xP[R4|A1]xP[R5|R4]x50
+ P[A]xP[A1|A]xP[R4|A1]xP[R6|R4]x20
+ P[A]xP[A2|A]x0

Figure 5: Event Tree Analysis Applied to Security Risk (AASHTO 2002)

In the scenario-based analysis, the basic components of risk are modeled explicitly following the above risk equation. The basic components in the method are described below.

Importance

- *Vehicles Directly Impacted*: a function of average daily traffic, length, deck, width, average traffic speed, and feature crossed.
- *Anticipated Economic Loss*: a function of average daily traffic, time for complete replacement, and cost of complete replacement.
- *Vehicle Detour Miles*: a function of average daily traffic, detour length, and usage type.
- *Defense/Emergency/Evacuation Route*: a function of usage type and feature crossed.
- *System Redundancy*: a function of priority and redundancy.
- *Attached Utilities*: a function of the type and number of utilities.

Occurrence

- Level of access for attack.
- Level of security against attack.
- Visibility or attractiveness of facility as a target.
- Capability of aggressor to initiate attack.

Vulnerability

- Expected damage to the bridge (% of total replacement value cost)
- Expected downtime or closure of the bridge (number of days)
- Expected casualties (number of people)

Ray et. al (2007) describes in his paper a risk-based methodology that was developed to facilitate prioritization of a threat mitigation strategies on individual bridges and the risk associated with each of their own individual structural components. A general equation, which is normally used for natural hazard risk assessment, was used for mitigation prioritization of individual bridge components as follows:

$$\text{Risk} = \text{OVI}$$

Where,

O = occurrence – measures the relative likelihood of a basic threat actually occurring against a given component;
V = vulnerability – captures the relative vulnerability of a given component given the occurrence of the basic threat;

I = importance – measures the importance of an individual component to the bridge.

According to Ray et al. (2007), in this case, risk is not an actual probability, but a measure of the subjective expectation of a total bridge collapse from a given threat against a given component. The location of some components and the type of threat applied to a certain component may make them more critical to the survival of the structure than others. The following points will be discussed further more in the sections ahead:

1. Analysis of different types of possible threats.
2. Analysis of different types of critical components of a single bridge.
3. Effect of certain bridge components subjected to a specific type of threat.

On the other hand, in the context of Homeland Security and the National Infrastructure Protection Plan (NIPP) (U.S. Department of Homeland Security 2006), risk is defined as the expected magnitude of loss (e.g., deaths, injuries, or economic damage) due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss. With this definition, risk is a function of consequence, vulnerability, and threat:

$$\text{Risk} = f\ (C,V,T)$$

Where,

C = consequence: the loss of human lives and the negative effects on public health and safety and the economy that can be expected if a bridge was destroyed or disrupted by a terrorist attack, or other incident;

V = vulnerability: the likelihood that a bridge will be susceptible to destruction, by terrorist or other intentional acts;

T = threat: the likelihood that a bridge will suffer an attack or incident. The estimate of this is based on the analysis of the intent and the capability of an adversary.

The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) conducts integrated threat analysis for all CI/KR sectors. Figure 6 shows how HITRAC develops analytical products by combining intelligence expertise based on all source information and threat assessments.

Once the three components of risk – consequence, vulnerability, and threat – have been assessed for a given asset, system, or network by sector, region, or nationally, they are factored numerically and combined mathematically to give an estimate of the expected loss considering the likelihood of an attack or other incident. Calculating a numerical risk score using comparable, credible methodologies provides a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions.

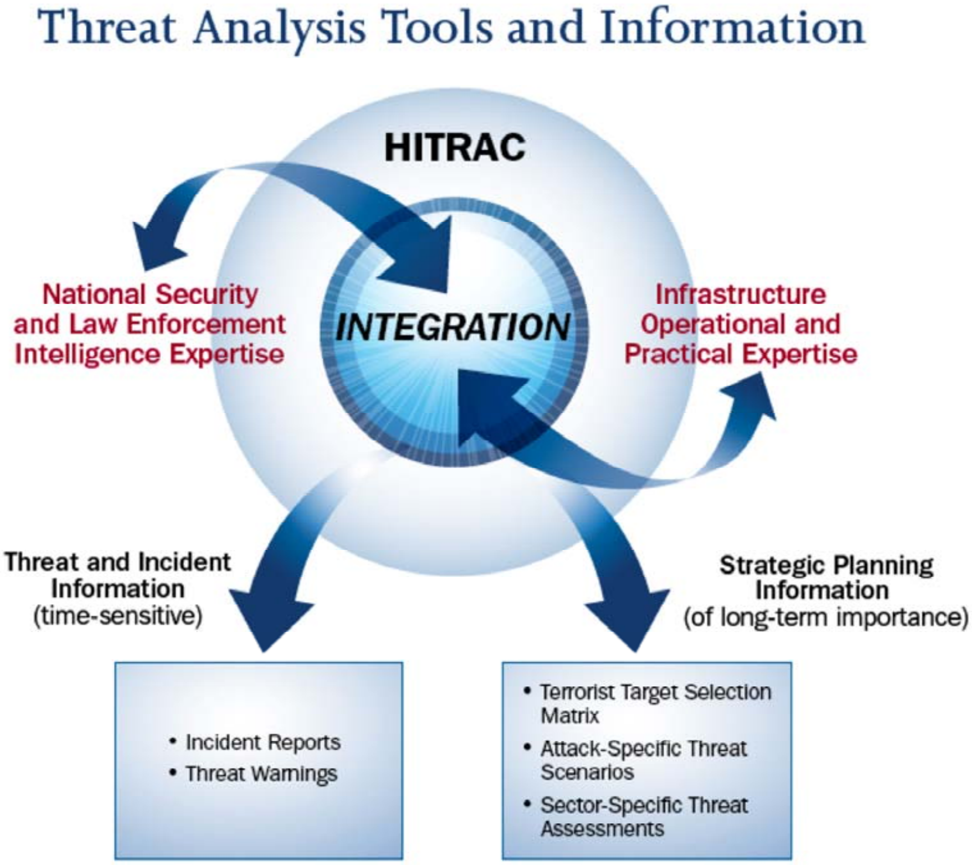

Threat Analysis Tools and Information
HITRAC
INTEGRATION
National Security and Law Enforcement Intelligence Expertise
Infrastructure Operational and Practical Expertise
Threat and Incident Information (time-sensitive)
Strategic Planning Information (of long-term importance)
• Incident Reports
• Threat Warnings
• Terrorist Target Selection Matrix
• Attack-Specific Threat Scenarios
• Sector-Specific Threat Assessments

Figure 6: Threat Analysis (NIPP 2006)

Consequence Analysis

In the context of NIPP (2006), consequence is measured as the range of loss or damage that can be expected.

- Human Impact: Effect on the life of humans; fatalities and injuries.
- Economic Impact: Effect on economy such as cost to rebuild asset, cost to respond to and recover from attack, cost resulting from disruption of product or service, long term costs due to environmental damage.
- Impact on Public Confidence: Effect on public morale and confidence in national economic and political institutions.
- Impact on Government Capability: Effect on the government’s ability to maintain order, ensure public health and safety, deliver essential public services, and carry out national security related missions.

Vulnerability Analysis

Vulnerability assessment process consists of the following steps:

- Determining an appropriate vulnerability assessment strategy.
- Identifying a methodology/tool appropriate for the particular type of asset, system, or network under consideration.
- Identifying and grouping vulnerabilities using common threat scenarios.
- Identifying dependencies and interdependencies with other assets and sectors.
- Considering vulnerabilities associated with physical, cyber, and human elements.
- Analyzing benefits of existing protective programs.
- Assessing residual gaps to determine unresolved vulnerabilities.

Threat Analysis

When it comes to terrorist risk assessment, threat is calculated based on the likelihood of a terrorist attack method on a particular asset, system, or network. On the other hand, if we are dealing with natural disaster or accident, then threat is based on the probability of occurrence. The incident management, disaster response, public safety, and other communities have developed and used various tool to estimate the threat of natural disasters and accidents. However, similar models are not yet in broad use for terrorist threats. For this reason, NIPP provides an augmented framework for the terrorist aspects of threat analysis.

Furthermore, Jaeger et. al (1998) introduces the risk equation based on Sandia's approach (Sandia is the national laboratory at the Security Systems and Technology Center in Albuquerque, New Mexico).

$$\text{Risk} = (P_A)\ (1-P_E)\ (C)$$

Where,

P_A is the likelihood of occurrence that comes from the analysis of the threat.

P_E is the system effectiveness which is the product of two parts: P_I (the probability of interruption) indicates how effective the protective system is in interrupting an adversary attack, and P_N (the probability of neutralization) is a measure of how well the response forces do in force-on-force conflicts with the adversary given interruption.

C is the consequence that considers impact, criticality, and cost.

BRIDGE TYPES

According to the interim report on bridges published on August 9, 2007 by the New Jersey Department of Transportation, there are about 6,433 highway carrying bridges over 20 feet long in New Jersey's Bridge Inventory. Figure 7 shows the distribution of NJ bridges owned by different sectors.

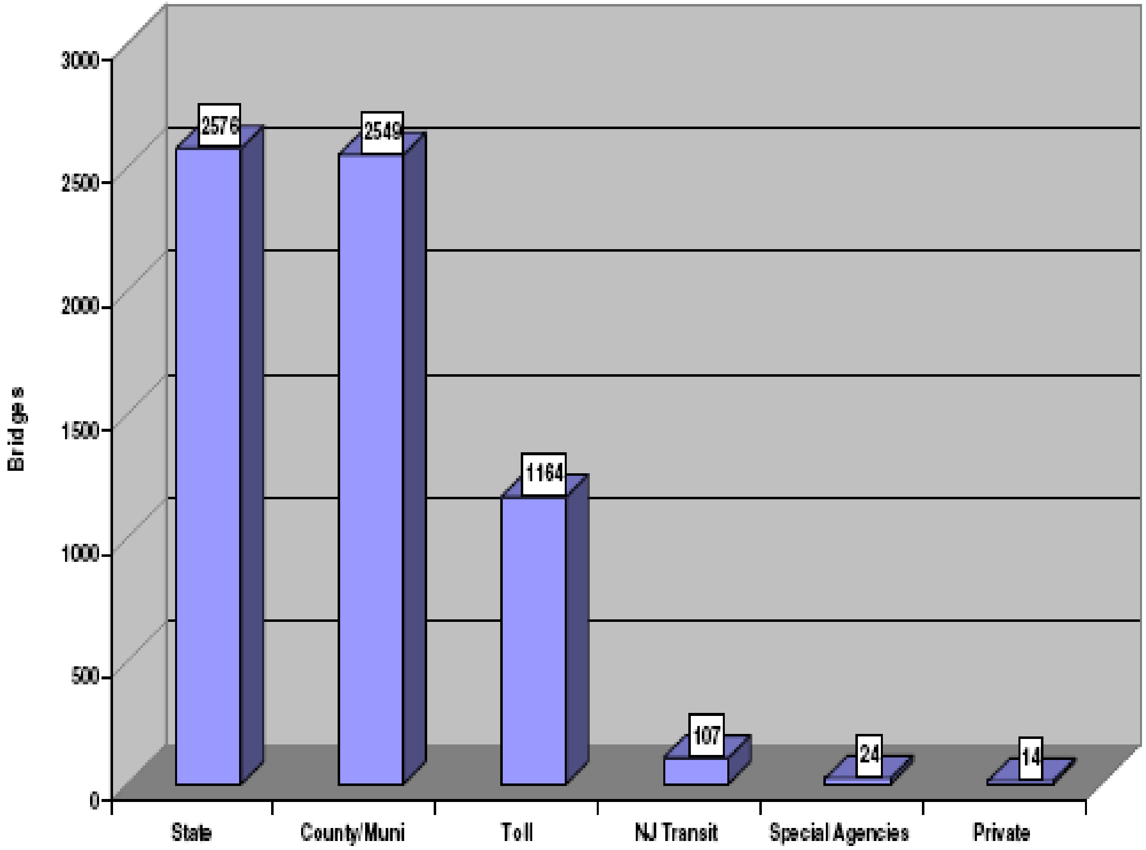


Figure 7: Number of NJ bridge owned by different sectors

The interim report provides an overview of the condition of New Jersey's bridges. The majority (5,125 bridges) are owned by the New Jersey Department of Transportation (NJDOT), county and municipal governments. The report concludes that 66% (4,196) of New Jersey's bridges are neither structurally deficient nor functionally obsolete. 23% (1,502) are functionally obsolete; 6% (396) are load posted which limit the weights of trucks using the bridges. Structurally deficient bridges are those that are restricted to light vehicles, require immediate rehabilitation to remain open, or are closed. Functionally obsolete bridges are those with deck geometry (e.g., lane width), load carrying capacity, clearance, or approach roadway alignment that no longer meet the criteria for the system of which the bridge is a part. Moreover, Figure 8 shows the different material types of bridges in New Jersey and the percentage of bridges per material. Figure 9 and Figure 10 show the percentage of bridges in New Jersey by types in Relation to the state and the nation. A detailed table can be found in Appendix A.

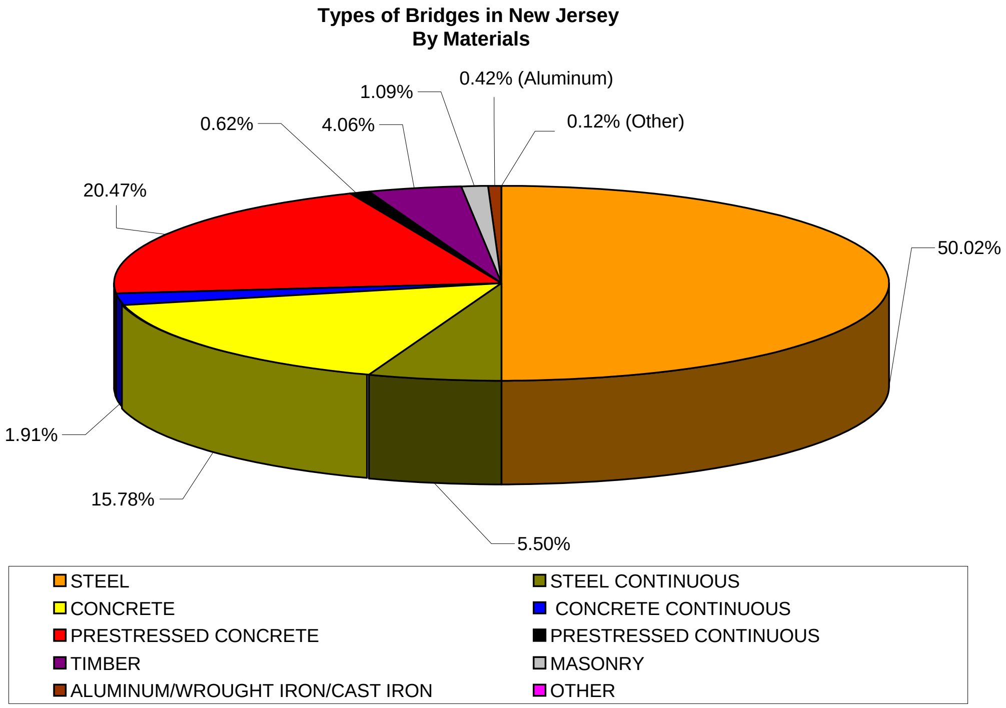


Figure 8: Percentage of Bridge Materials in NJ

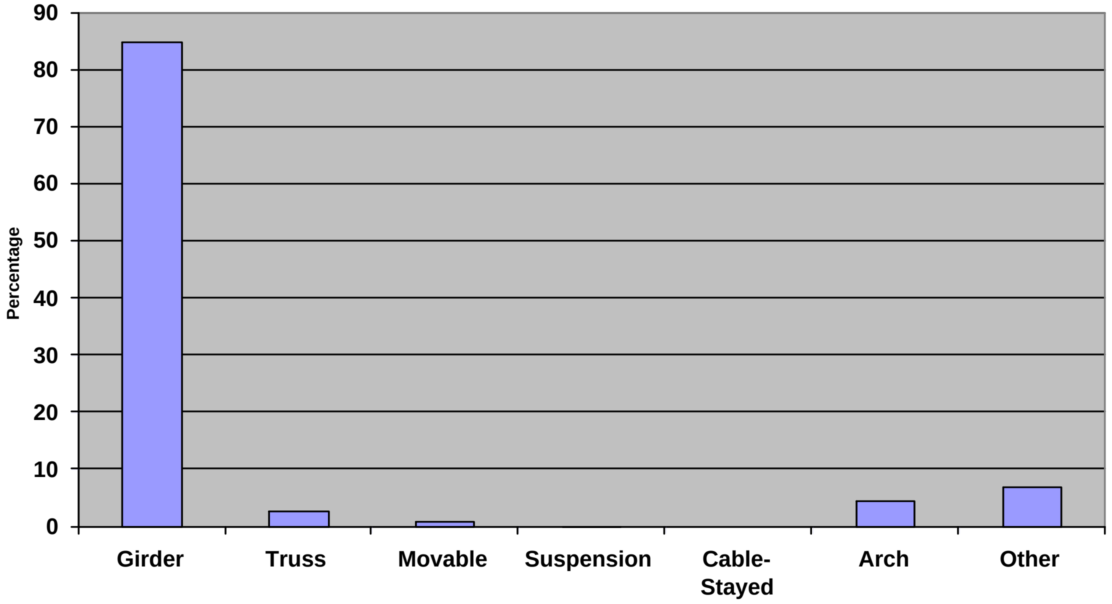


Figure 9: Percentage of Bridges in NJ by Types

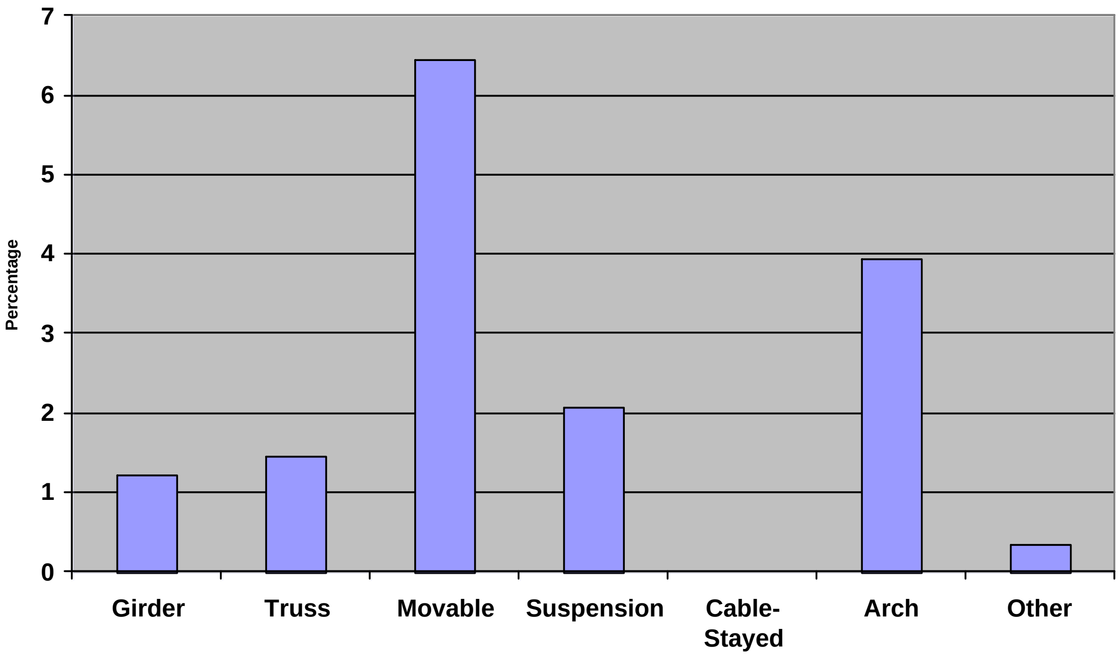


Figure 10: Percentage of Bridges in NJ by Types in Relation to the United States

THREAT LEVEL RISK AND VULNERABILITY ASSESSMENT

Before attempting to develop a bridge security assessment checklist, security hazard levels and performance objectives needed to be established. These hazard levels need to take into account the probability of occurrence of terrorist attack (blast and impact loadings) its associated risks, the magnitude of these loading, the permissible extent of damage, and the expected condition of the bridge after an attack. It is essential for any successful bridge security system to have risk management and vulnerability assessment plan. Risk management and vulnerability assessment for bridge security should include the following:

1. Bridge Identification (Critical Bridges, Other Bridges).
2. Security Hazard Level or Threat Identification and its Probability of Occurrence
3. Bridge Vulnerability Assessment (Performance Criteria And Acceptable Damage Levels)
4. Bridge Security Prevention Measures
5. Response Schemes (Coordination And Planning)

Figure 11 shows a flow chart with the FHWA and AASHTO Recommendations for vulnerability assessment.

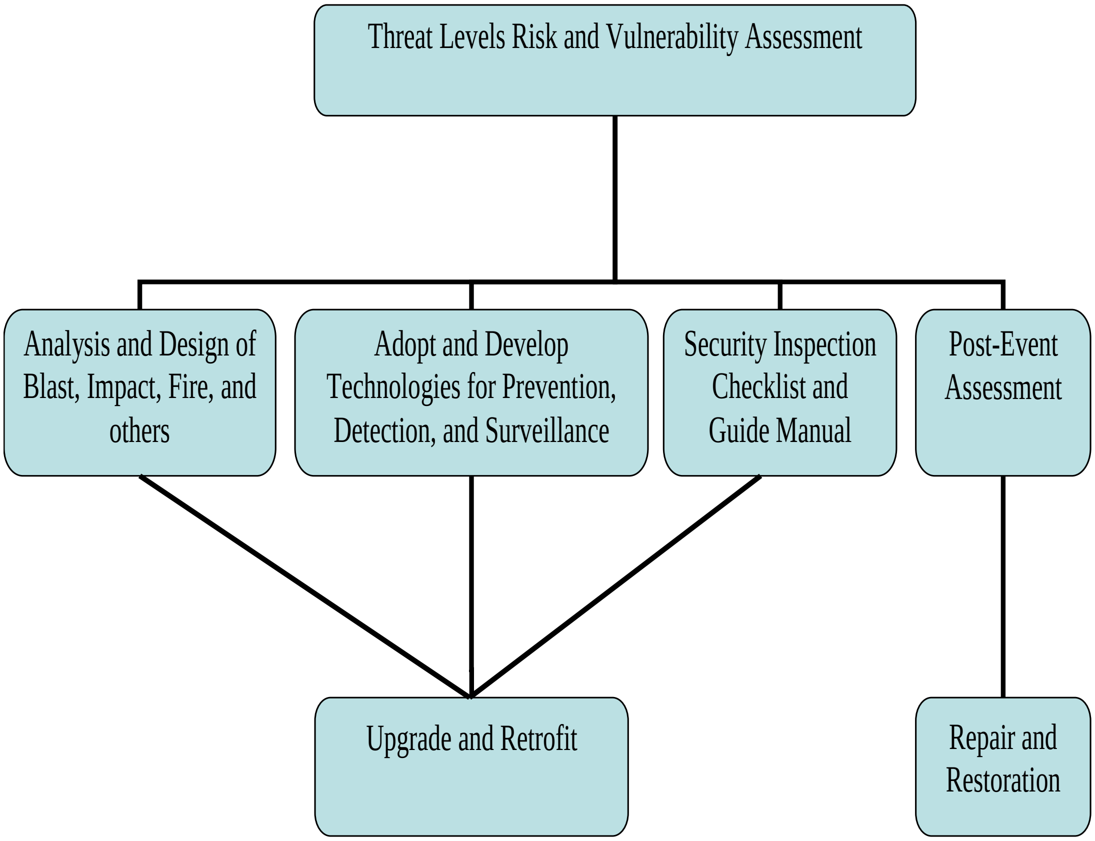

Threat Levels Risk and Vulnerability Assessment
Analysis and Design of Blast, Impact, Fire, and others
Adopt and Develop Technologies for Prevention, Detection, and Surveillance
Security Inspection Checklist and Guide Manual
Post-Event Assessment
Upgrade and Retrofit
Repair and Restoration

Figure 11: Flow Chart for Risk and Vulnerability Assessment (FHWA and AASHTO[1])

In order to establish these security hazard levels and performance criteria a quantitative assessment of the probability of occurrence, vulnerability, and importance of the bridge need to be defined. The probability of occurrence of a security hazard or an attack can be attributed to many factors such as history of previous of attacks, data available from security agencies, nature, visibility, importance of the bridge, accessibility, and many other factors that need to be included. Therefore, the predictability of such an attack is a complicated process that involved many parameters. The other factor needed to quantify risk assessment is the vulnerability of the bridge. Bridge vulnerability depends on many factors and can be estimated by conducting bridge security inspection using the NBSI checklist. Among these factors is the type of threat attacks and the magnitude of the explosive devices used in the attack. The development of security hazard levels and performance objectives is essential to properly design bridges for various security threat levels.

Once these security hazard levels and performance criteria are established, bridge components that are vulnerable to blast and impact need to be identified based on standoff distance, strength, ductility, allowable movement, and other available protection measures of these components should be established. Many bridges in New Jersey have design and construction details that may not be adequate to resist forces from blast loads and maintain integrity during such an event. Therefore it is important to identify these security deficient bridges, evaluate the extent of possible damage, and establish a program to reduce their security risk.

To establish risk levels and the probability of terrorist attacks on bridges and to define the acceptable level of service required following a terrorist attack on a bridge, a risk management plan for security hazards need to be developed with coordination with NJDOT Bureaus of Structural Engineering and Transportation Security the Office of Homeland Security, and Law Enforcement Agencies. This should include development and implementation of a comprehensive risk and loss characterization for the New Jersey Bridges and identifying and modeling a variety of attack (blast/impact load) scenarios to determine the risk and consequences of these events. Data needs to be collected on all bridges in New Jersey such as geometry, traffic volume, location, height, material type, bridge use, cost, proximity to police and fire stations, etc….

In addition to security hazards, bridges are also exposed to other natural or man-made hazards such as earthquakes, vessel impact, flooding, scour, and fire. Since most of these hazards require risk assessment and management plans similar to bridge security, it is more rational and cost effective to use a multi-hazard approach for designing and retrofitting bridges to withstand these hazards.

HAZARDS AND THREATS

Critical infrastructures are being targeted to achieve important types of effects such as creating physical destruction and disruption, creating fear among civilians and causing interruption of our every day business life. A wide array of tactics and techniques are in being used in conducting an attack. There are unlimited possibilities as to the types of threats that could be brought against bridge structures. However, it is impossible to design all bridges to withstand all possible combinations of attacks that may occur. Below is a list of the most likely tactics and threats:

- Vehicle-borne Improvised Explosive Device (VBIED): These include both land-borne vehicles (i.e. truck bombs) that would be deployed against components reachable by land and waterborne vehicles (i.e. boat bombs) that would be deployed against any components reachable by water.
- Hand Emplaced Improvised Explosive Device (HEIED): These include contact explosive devices such as satchel demolition charges and shaped

charges that are commonly used by military engineers and civilian demolition experts to precisely cut/sever structural member.

- Non-Explosive Cutting Device (NECD): These include any non-explosive devices such as saws, grinders, and torches that can be used to cut/sever structural members.
- Vehicular Impact (VI): Similar to the VBIEDs, these include both land-borne and waterborne vehicles depending on the location of the component of concern.
- Fire: Size of fire and duration can cause structural members to lose both their stiffness and strength. Thus, fire caused by a ruptured tanker truck on the deck of a bridge, adjacent to key components or in the water adjacent to piers or towers, is of great concern.

The Federal Highway Administration (FHWA) presented in Table 5 a summarized version of threats and their potential magnitude.

Table 5: Magnitude of Threats (FHWA 2002)

Threat Type	Largest Possible	Highest Probability
Conventional explosives	Truck*: 20,000 lbs Barge: 40,000 lbs	Car bomb*: 500 lbs
Collision to structure (i.e., the size of a vehicle that could collide with a structure)	Truck: 100,000 lbs GVW Water Vessel: depends on waterway	Truck: H-15 Water Vessel: (see AASHTO spec. LRFD on vessel impact)
Fire	Largest existing fuel or propane tank Largest fuel vessel or tanker	Gasoline truck (3S-2) Fuel barge
Chemical/biological HAZMAT	These threats exist; however, the panel is not qualified to quantify them. Therefore, other experts should assess these threats in this way.	

* *Largest possible conventional explosive – for a truck, based on largest truck bomb ever donated internationally by a terrorist act. For a barge, based on the assumption that it is the largest explosive that could pass by unnoticed by current security at place at major waterways.*

In order to reach a certain level of satisfaction, terrorists will study the behavior of a bridge; which components are more critical if subjected to a blast, how much explosive loads need to be placed next to a certain component to cause enough destruction, etc. Winget et. al (2005) studied the components of a bridge subjected to blast loads. Results from this study have shown that bridge geometry can significantly affect the blast loads that develop below the deck. For bridges with deep girders, confinement effects can greatly enhance the blast loads acting on the girders and tops of the piers and in some cases may result in more damage than an explosion occurring on top of the deck. The clearance can also have a large impact on the results, as increasing the distance from the explosion to the deck can result in more damage to the girders. However, higher clearances result in lower average loads on the piers due to the larger volume of space (less confinement) under the bridge and the increased average standoff distance to a given point on the pier. Explosions occurring near sloped abutments could possibly result in more damage than an explosion at midspan due to the confinement effects at the abutments. Finally, round columns will experience lower loads due to the increased angle of incidence from the curved surface.

CRITICAL BRIDGE COMPONENTS AND VULNERABILITY ASSESSMENT

It is anticipated that any assessment and implementation of security measures for bridge should address the critical bridge components that are vulnerable to terrorist threats and blast loadings. There are two approaches to defend and protect critical bridge components against security threats:

1. Standoff Distances and Secured Access
2. Structural Toughening

There are many bridge components that are considered critical for bridge integrity and acceptable performance.

To assess the capacity of above-mentioned critical bridge components for a blast and impact loads, computer simulations will be used. The cost of designing such components to withstand large blast loads may prove to be prohibitive. First, the magnitude of the blast/impact load needs to be established with its probability of occurrence. Second, simulation models of blast loading will be run to determine the magnitude of the blast load and response of the bridge component to the applied loads in terms, shears, moments, deflections, and damage.

An analysis of typical bridge details and elements will be necessary to develop a checklist of relevant metrics to be used to assess bridge vulnerabilities to classes of threats. A simple analysis of typical bridges can be used to develop predictors of performance and governing modes of failure. Metrics such as span, stiffness, and mass, modes of vibration, material properties and load types can be identified or associated with modes of failure. In this way, the vulnerability or susceptibility of a bridge to a series or class of threat can be identified more accurately. Identifying these metrics will enhance the security checklist.

Winget et al (2005) indicated that developing an understanding of the principles of blast wave propagation and its potential effects on bridge structures is the first step that should be taken before engineers can begin to design bridges to withstand blast loads and terrorist attacks. A project manager or a security professional should perform a preliminary risk assessment to determine which threats the bridge may face. Once the potential threats have been identified, measures can be implemented to mitigate those risks. These measures can be used to displace the threat to less attractive targets, increase the likelihood of terrorists being detected and identified, keep casualties to a minimum, improve emergency response time, increase public confidence, improve structural response, or a combination of these events (Jenkins 2001). In their paper, Winget et. al (2005) mention that the most common analysis method used in practice is a single- or multiple-degree-of-freedom, uncoupled, nonlinear dynamic analysis. BlastX version 4.2.3.0 (BlastX 2001) was used to generate loads. To calculate the reduced area of the columns due to local blast damage, empirically based spall and breach equations developed by Marchand and Plenge (1998) were used. To predict the local breaching damage for counterforce scenarios on small diameter piers, the rule of thumb in FM 5-250 (Department of the Army 1992) was used, which indicates the amount of TNT per foot for concrete to be breached. To calculate the flexural response of the piers to vehicle blast loads, SPAn32 version 1.2.7.2 (SPAn32 2002) was used. After the analyses were made, the results showed that bridge geometry could significantly affect the blast loads that develop below the deck. For bridges with deep girders, confinement effects can greatly enhance the blast loads acting on the girders and tops of the piers and in some cases may result in more damage than an explosion occurring on top of the deck. Higher clearances result in lower average loads on the piers due to the larger volume of space under the bridge and the increased average standoff distance to a given point on the pier. Explosions occurring near sloped abutments could possibly result in more damage than an explosion at midspan due to the confinement effects at the abutments. In addition, round columns will experience lower loads due to the increased angle of incidence from the curved surface.

It is anticipated that many of the existing bridges will need to be upgraded to the acceptable performance levels for security. There is a need to evaluate the various security countermeasures that can be used to upgrade and protect vulnerable bridge components based on cost and ease of installation.

Figure 12 and Figure 13 show vulnerability of bridge piers to moving trucks and in remote areas, respectively. In some cases protective measures should be considered similar to those used in the design for vessel collision where the piers are typically protected by islands, dolphins, and fender systems. In other cases, a restriction on size of vehicles and their proximity to critical bridge components should be established.

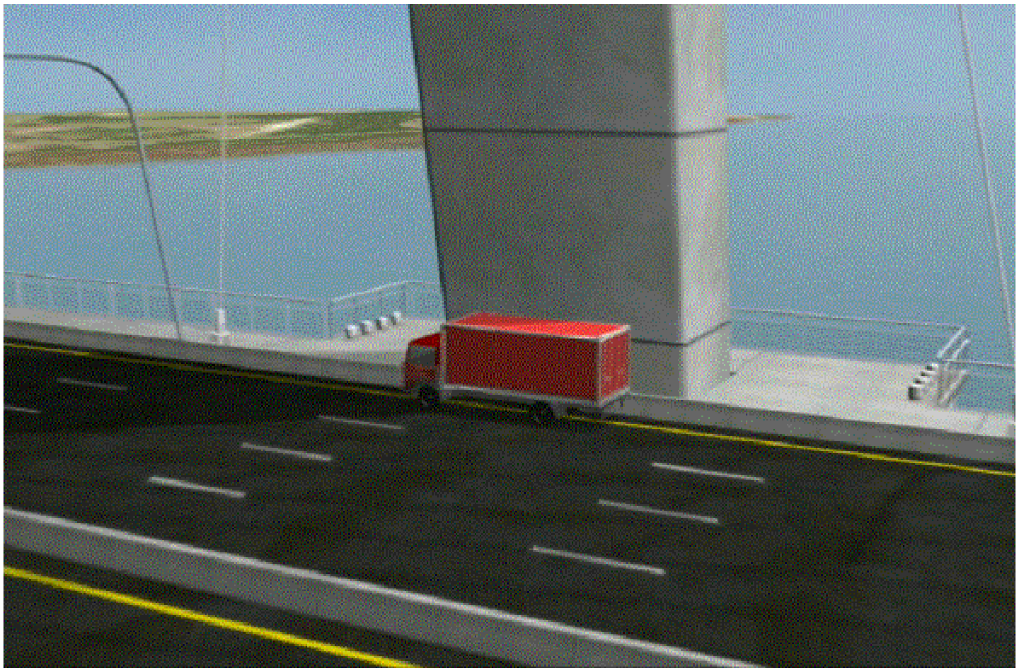


Figure 12: Vulnerability of bridge piers to moving trucks.

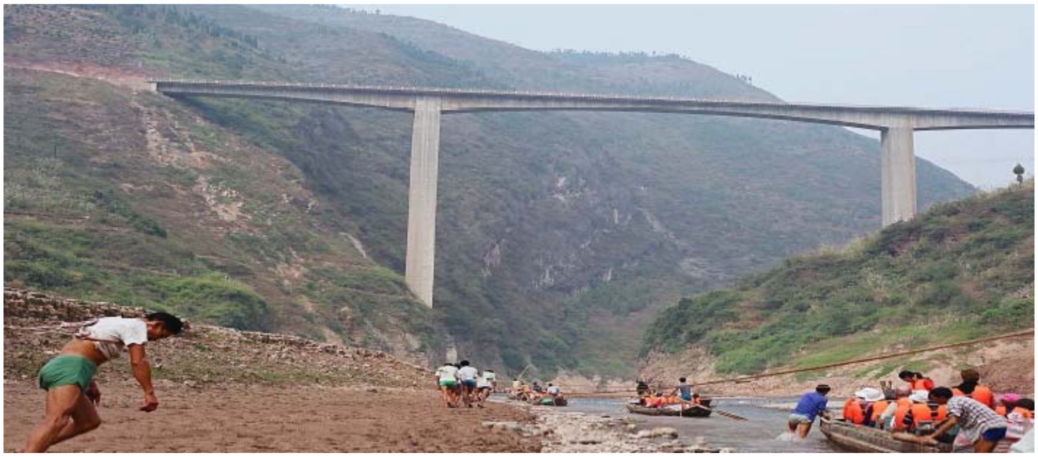


Figure 13: Vulnerability of bridge piers in remote areas.

Williamson et. al (2005) proposed a brief sample list of possible threats at specific locations on or near a bridge component.

For critical components, the following actions should be considered for security protection:

1. Provide enough standoff distances from these critical components.
2. Restrict access to travelers near these components.
3. Provide surveillance under and around the structure.
4. Upgrade these components using strengthening and confining techniques.

Table 6 and Table 7 give approximate minimum and desired standoff distances for moving trucks near piers.

Table 6: Desired Barrier Standoff Distances from Piers (*FHWA Blue Ribbon Workshop (2003)).*

Desired Barrier Standoffs* from Bridge Piers (Measured in ft from face of pier to front of barrier)					
Threat Type	Explosive Weight (lbs TNT)	Pier Thickness (ft)			
		~3’	~4’	~7’	> 8’
Sedan	1,000	15	12	10	10
Passenger Van	4,000	50	35	25	25
Box Truck	10,000	100	100	45	35
Moving Van/Water Truck	30,000	200	150	100	100

**These are estimated values. A structure specific assessment should be done to determine actual standoff distances. FHWA Blue Ribbon Workshop (2003).*

Table 7: Minimum Barrier Standoff Distances from Piers (*FHWA Blue Ribbon Workshop (2003)).*

Minimum Barrier Standoffs* from Bridge Piers (Measured in ft from face of pier to front of barrier)					
Threat Type	Explosive Weight (lbs TNT)	Pier Thickness (ft)			
		~3’	~4’	~7’	> 8’
Sedan	1,000	8	8	8	8
Passenger Van	4,000	35	25	16	16
Box Truck	10,000	75	75	25	22
Moving Van/Water Truck	30,000	150	100	75	75

**These are estimated values. A structure specific assessment should be done to determine actual standoff distances. FHWA Blue Ribbon Workshop (2003)*

RISK ASSESSMENT

Terrorism has surely existed since before the dawn of recorded history (Merrari and Friedland 1985). However, over the past 20 years the number of threats and man-made acts has increased. There are many types of threats that could be classified in the following ways:

1. **Domestic** – in own country against own people.
2. **International** – in another country by non-state actors.
3. **State sponsored** – by a government against their own people or in support of international terrorism. For example when a ruling regime provides funds, intelligence or material resources to terror groups, usually operating outside their borders.
4. **Political** – for ideological and political purposes. Groups that focus on gaining power or supremacy, removing government intrusion, or on changing beliefs.
5. **Non-political** – for private purposes or gain.
6. **Quasi-terrorism** – skyjacking and hostage taking.
7. **Limited political** – ideological but not revolutionary.
8. **Official or state** – used by nation against nation or people.
9. **Revolutionary** – aims to overthrow or replace an existing government.
10. **Nationalist** – promotes the interests of an ethnic or religious group that is seen as being persecuted by another.
11. **Cause based** – groups devoted to a social or religious cause using violence to address their grievances.
12. **Environmental** – groups dedicated to slowing down development they believe is harming animals.
13. **Genocide** – when a government seeks to wipe out a minority group in its territory.

Focusing on infrastructure and specifically bridges, malicious acts would take place for the following reasons:

1. Kill as many civilians as possible, so they might consider attacking a bridge during morning or afternoon rush hour.
2. Disrupt the commute of civilians by bombing a bridge span which could create a gap between two major cities where people would have to find different routes to commute to their jobs
3. Impact the economy resulting from the large cost and time it would take to repair or replace a bridge, weaken the government and set fear in peoples' lives.
4. Get the media's attention in order to become famous around the world of what have been caused.

After understanding the behavior of bridge components under blast loads, a set of questions was developed that will mainly categorize all bridges in New Jersey according to the most risky and the likelihood that a certain bridge will get attacked. The questions are categorized into three sections:

Occurrence Factor (O)

As mentioned previously, the occurrence factor measures the relative likelihood of a basic threat actually occurring against a given component on the bridge. The occurrence factor consists of multiple sub-factors:

- Threat Likelihood: the likelihood that a certain type of threat will be chosen instead of another one. From various lists of incidents collected for this study, it has shown the most preferred method of weapon is to use hand-emplaced explosive devices and vehicle-borne explosive devices both land-borne and waterborne such as truck bombs and boat bombs.
- The likelihood of a given threat against a given component: similar to the above sub-factor, however it narrows down the choice of a specific type of threat used at a certain component of the bridge. For example, a non-explosive cutting device is less likely chosen to attack a reinforced concrete pier.
- Visibility or attractiveness of a component: The likelihood that a bridge component will be recognized as critical to the structural stability.
- Access to a component: this deals with how easy it is to access a certain component such as bearings or a deck.

Vulnerability Factor (V)

The vulnerability factor is the likelihood that a bridge will be susceptible to destruction by a given threat. One important aspect is the resistance of a component to a type of threat such as vehicle-borne explosive devices or hand-emplaced devices. This means how much destruction a component will face if subjected to a specific amount or size of explosives. Terrorists will try to get as close as possible to a component when using their threat. However, to make it easier and have more time efficient, they will not carry large explosives to place them in certain areas.

Importance Factor (I)

The importance factor measures the importance of an individual component to the bridge. The following sub-factors are considered:

- Structural importance of component: this deals with the importance of a component to the overall stability of the bridge. Looking for specific components that if attacked, will result in complete collapse and destruction of the bridge is something to consider. For this matter, this is the most important sub-factor and will be given a higher weight.
- Historical/symbolic importance of the component: this applies to components of the bridge being historic or well known after a famous engineer.

- Relative repair cost for the component if damaged: this relates to if a component was attacked and got damaged, however the bridge did not completely collapse. Nonetheless, it will cost a fortune to repair the component and get the bridge back to service.
- Relative time out of service for the bridge if component is damaged: similarly, this deal with the actual time the bridge will be out of service until the component is fully repaired.

According to Ray et. al (2007) the weight for each sub-factor (shown in Table 8) was derived using the pairwise comparison procedure of the analytical hierarchy process. Knowledgeable sources were asked to assign numeric value to the relative importance of one sub-factor over another.

Table 8: Weight for sub-factors (Ray et. al (2007))

Risk Factor	Sub-factors	Weight
Occurrence	Threat likelihood in general	0.11
	Threat likelihood against component	0.25
	Visibility and attractiveness of component	0.09
	Easy access to component	0.54
Vulnerability	Resistance of component to basic threat	1.00
Importance	Structural importance	0.56
	Historic/symbolic importance	0.06
	Repair cost if damaged	0.26
	Time out of service if damaged	0.12

The checklist consists of several questions that were categorized into the different factors of the risk equation. The choice of the type of questions was taken from the study and analysis of the type of threats, the critical components of a bridge, and security-based questions. The New Jersey Office of Homeland Security and Preparedness (OHSP) retains the checklist for internal use only.

TABLET PC - BASED BRIDGE SECURITY CHECKLIST FOR ON-SITE ASSESSMENT

The checklist needs to be implemented for on-site assessment. There are many ways someone can think of doing that will facilitate the use of the checklist. One of them is to use a portable electronic device called a tablet notebook computer that will process the checklist. The Table PC (Figure 14) has all of the capabilities of a notebook computer plus the ability to fold the screen flat and interact using a digital stylus. A Table PC uses the Windows XPTM operating system. All of the user interfaces and file formats are the same as any typical desktop computer. The user can exchange files directly without additional conversion or adapters. Furthermore, the Table PC can store other necessary reference documents and multimedia for instant use in the field. Bridge plans, inspection manuals, previous inspection reports, photos and others are ready at the touch of a screen. In terms of security, Table PCs are available with the latest digital encryption with fingerprint or password protection. Table PCs feature high-speed USB ports and BlueTooth^{TM} connectivity. Peripherals such as digital cameras can be connected to upload field photos and add to the inspection files.

Table PCs are more versatile and less expensive than in the past. A fully charged internal lithium ion battery can power the tablet for up to four hours. Extra batteries can easily be swapped for extended inspections. Tablet PCs are also highly portable. A typical size is 10x12x1.5 inches weighing about 4 pounds. Ruggedized models are available at a higher cost, but will survive more abuse.

Since the Table PC is a full-featured notebook computer, there is no need for a separate desktop computer. The inspector can use the Tablet in the field to collect information and later use the same computer to prepare the final report. Additionally, the answers to the questions and the calculated risk could automatically be transferred and stored in a database file at the State DOT even while still at the field.

Future versions of the checklist can take advantage of the handwriting recognition. Extra notations can be made in writing instead of time-consuming keyboard entry. Quick sketches of bridge details can be made. A built-in microphone could also record voice messages to be transcribed later. GPS receivers can be added to record geospatial information such as the location of structure features. The GPS data can be processed with common mapping software to provide maps of inspection information. The location data can also be synchronized with Geographic Information Systems (GIS).

Figure 14: Table PC

COUNTERMEASURES

After completion of the risk assessment and identifying the critical bridges in New Jersey, appropriate countermeasures need to be considered. There are a variety of countermeasures that can be used to reduce attractiveness and/or vulnerability of a bridge or to reduce consequences if an attack occurs. New technologies are available to deter attacks, deny access, detect presence of terrorists, defend the facility, or design structural hardening.

Capers et. al (2005) suggested the following countermeasures:

- Restrict parking under a bridge structure.
- Installation of surveillance cameras.
- Restrict the placement of vegetation.
- Restrict access to ventilation machinery in tunnels.
- Detail installation of emergency shut-off mechanisms.
- Restrict access to key details.
- Restriction of access to movable bridge machinery and operator's housing.

- Detail the lighting to ensure surveillance.
- Detail all components so that no component is concealed from view.
- Prohibit the use of non-redundant members.
- Protect all main load-carrying members from direct impact.
- Locate utilities as to minimize their potential use as weapons.

The Federal Highway Administration provided recommendations and countermeasures for bridge and tunnel security (Bride and Tunnel Security 2003). Some of those recommendations were divided into the following two categories:

- Approaches to mitigate threats
- Establish a secure perimeter using physical barriers.
- Provide inspection surveillance, detection and enforcement, and closed circuit television (CCTV).
- Provide visible security presence.
- Minimize the time on target.
- Approaches to mitigate consequences
- Create standoff distance- incorporating sufficient standoff distances from primary structural components will help resistance from blasts.
- Add design redundancy – this will help limit collapse in the event of severe structural damage from unpredictable terrorist acts.
- Hardening/strengthening the elements of the structure – this will minimize damage and complete collapse of the structure.
- Develop an accelerated response and recovery plan – alternative routes and evacuation plans should be established.

NIPP (2006) introduced an effective, efficient program over the long term. Five steps, described below, were used for this program.

- Building national awareness – this could be done by organizing workshops about bridge security and bring in experts that could present new things.
- Enabling education, training and exercise programs – bridge inspectors need to be trained to use the checklist. Community residents need to be educated by preparing them for any threat and be aware of any suspicious act.
- Conducting research and development and using technology – for this research a checklist was developed and new technological devices were used.
- Developing, protecting, and maintaining data systems and simulations – this means that for example the developed checklist will only be provided to certain agencies.
- Continuously improving the checklist and associated plans and programs through ongoing management and revision, as required.

Furthermore, Winget et. al (2005) recommended that design and retrofit options for girders should include the use of fiber reinforced polymers (FRPs). Fiber-reinforced polymers are robust materials that are highly resistant to corrosive action, have a high strength to weight ratio and are well suited for assembly line production into modular components that can be rapidly erected. However, FRP material costs are significantly greater than traditional concrete and steel materials. Therefore, cost savings due to either reduced weight, increased speed of construction or lower maintenance and increased life expectancy must offset this higher cost to make sensible use of FRP materials. Additional steel reinforcement using blowout panels on the decks to help vent loads are also recommended. To prevent a span collapse, the girders and deck can be restrained at the supports with steel cables, or hinge restrainers can be used to hold the deck to the columns. Abutment seat sizes can be increased or hinge seat extensions can be used under expansions joints. For piers lateral bracing could be included and minimum pier diameters and reinforcement could be established.

CONCLUSIONS

A bridge security checklist has been presented in this research to provide identification of critical bridges throughout New Jersey. After evaluating all bridges in New Jersey, security measures and hardening of the structure will take effect for the top 10 percent. Based upon the analysis of bridges evaluated in this study, the methodology has proven very useful and provided consistent and reliable results. The use of the security checklist in a spreadsheet format makes it easy and timely efficient for engineers and inspectors to evaluate the bridges. The checklist is enhanced by links to help type functions that provide images or explanations to provide the bridge inspector with unambiguous directions. The tablet PC is a lightweight device where the answers to the questions and the calculated risk could automatically be transferred and stored in a database file at the State DOT even while still at the field.

The checklist was closely coordinated with the NJ Office of Homeland Security and Preparedness (OHSP) and NJDOT Bridge Bureau. Various NJ bridge inspectors were selected to review and apply the checklist to a bridge in NJ. The experienced inspectors provided the team some important feedback on the applicability of the checklist. They found no difficulty in answering the questions because the answers were provided in a drop down list format. The checklist and discussion related to its development are not included in this report.

For future implementation of the project, the inspectors will be trained in a classroom workshop on the use of the checklist. They will learn where to look on the bridge and easily identify the critical components. Inspectors will be asked to provide detailed comments on the ease of use, applicability, and changes needed to improve the checklist or on the PC programming. The comments will be compiled and reported to the NJDOT Project Manager for further refinement and/or development.

Bridges are not only public structures used to commute from and to cities, but they also carry symbolic references as well as serve utilitarian purposes. These great structures of humankind give us a real, physical reminder of who we are and what we can achieve. It is very important to provide a vulnerability assessment of the most important bridges. The methodology presented in this research has much room for continued improvement.

BIBLIOGRAPHY

AASHTO, “A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection.” Washington, D.C. American Association of State Highway and Transportation Officials. 2002.

AASHTO, “Standard Specifications for Highway Bridges.” American Association State Highway and Transportation Officials, Washington, D.C., 1994.

Anderson, C.W., Courain, D.J., Edmonds, P.A., Gouldey, A.C., Ward, N.T., “A Risk-Based Methodology for Modeling, Assessing, and Managing Risks to the Hampton Roads Bridge Tunnels.” Systems and Information Engineering Design Symposium, 2005, pp. 34-39.

Baker. “Route 52 Causeway Replacement Project. Ocean City, Cape May County. Somers Point, Atlantic County.” Homeland Security Letter Report, 2007.

Basoz, N. and Kiremidjian, A.S., “Prioritization of Bridges for Seismic Retrofitting, Report No. 114.” Stanford, CA. John Blume Earthquake Engineering Center, Department of Civil Engineering, Stanford University. 1995.

Behe C., “Haupt Truss Bridge Graphic by Historic American Engineering Record, National Park Service, record PA-207, dated 1991.” Last modified on January 2008. Accessed on March 2008. Online at http://www.trainweb.org/horseshoe curve-nrhs/Haupt.htm.

Betts, C.P., “U.S. Department of Defense Guidance for Security Engineering.” Structures April 2005.

Capers, H.A., Neil, H., “The Challenge of Economically Balancing Security and Mobility Needs of New Jersey’s Bridge Infrastructure.” 3rd New York City Bridge Conference, September 12-13, 2005.

Cunningham, J.T., “New Jersey: America’s Main Road.” Garden City, N.Y., Doubleday and Company, 1966.

DeLony, E., “Landmark American Bridges.” Boston, Little Brown and Company, 1992.

Eytan, R., “Cost Effective Retrofit of Structures against the Effects of Terrorist Attacks –the Israeli Experience.” Eytan Building Design, Tel Aviv, Israel, (2003)

Feldman, S., “Digital Image by Kodak DC-4800.” May 2001. Accessed on March 2008. Online at http://www.trainweb.org/railpix/njtpix/D-delair1-5-31-01.jpg.

Forster. P.M., “An Introduction to the Psychology of Terror.”

Google Image. “New Jersey by Counties.” Accessed on March 2008. Online at http://www.shotcredit.com/images/statemaps/New_Jersey_Counties.png

Jaeger, C.D., Duggan, R.A., William, K.P., “Risk Analysis Tools for Force Protection and Infrastructure/Asset Protection.” Security System and Technology Center, June 1998.

King, S.A. and Isenberg, J., “Assessment of Urban Transportation Infrastructure for Terrorism Risk Management.” Proceedings Ninth International Conference on Structural Safety and Reliability. Rome, Italy, June 19-23, 2005: 2773-2780.

King, S.A., Pachakis, D., Fallon, T., and Powell, A.J., “Techniques for Quantifying Security Risk for Bridges.” Third New York City Bridge Conference, September 12-13, 2005. Bridge Engineering Association.

Kolluri, K., “Interim Bridge Report, Presented to Governor Jon S. Corzine.” New Jersey Department of Transportation, August 2007.

Leung, M., Lambert, J.H., and Mosenthal, A., “A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks.” Risk Analysis, Vol. 24, No. 4, 2004, pp. 963-984.

Little, R., “Capital Improvement Program Bridging the Past and Future.” Delaware River Joint Toll Bridge Commission, p.3. Online at http://www.ibtta.org/files/PDFs/ Little_Roy.pdf

Mays, G.C. and Smith, P.D., “Blast Effects on Buildings – Design of Buildings to Optimize Resistance to Blast Loading.” Thomas Telford, London. 1995.

Middleton, W.D., “Landmarks on the Iron Road.” Bloomington and Indianapolis, Indiana University Press, 1999.

Mineta, N.Y., Presentation given by U.S. Transportation Secretary at the Proc. National Transportation Security Summit, 2001.

Merrari, A., and Friedland, N. “Social Psychological Aspects of Political Terrorism”.Applied Social Psychology Annual 6, 1985, pp.185-205.

Mullers. I., and Vogel. T., “Vulnerability of Flat Slab Structures.” American Society of Civil Engineers, April 2005.

Princehorn, M. and Laefer, D., “Cost-Effective Decision for Blast Mitigation.” Structures 2005.

Ray, J.C., “Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges.” Journal of Bridge Engineering, March/April 2007, pp. 140-146.

Rowshan, S., Smith, M.C., Krill, Jr., S.J, Seplow, J.E., and Sauntry, W.C., “Highway Vulnerability Assessment. A Guide for State Department of Transportation.” Transportation Research Record, No. 1827, TRB, National Research Council, Washington, D.C., 2003, pp. 55-62.

The Blue Ribbon Panel on Bridge and Tunnel Security, “Recommendations for Bridge and Tunnel Security.” Report FHWA-IF-03-036, AASHTO, Washington, D.C., September 2003.

Tobin, M. “Bridge Data in New Jersey.” New Jersey Department of Transportation. October 2007.

U.S. Census Bureau. “Total Population Per Square Mile. New Jersey by County.” Online at http://factfinder.census.gov/servlet/ThematicMapFramesetServlet?_bm=y&-geo_id= 04000US34&tm_name=DEC_2000_SF1_U_M00090&ds_name= DEC_2000_SF1_U&-_MapEvent=displayBy&-_dBy=050&-_lang=en&-_sse=on

U.S. Department of Homeland Security. “National Infrastructure Protection Plan.” 2006,pp. 1-179.

Whipple, S. “Bridge Building.” Albany, N.Y., 1869. Online at http://bridges.lib.lehigh. edu/books/book2301.html.

Williamson, E., Winget, D., “Risk Management and Design of Critical Bridges for Terrorist Attacks.” Journal of Bridge Engineering, Jan/Feb 2005, pp. 96-106.

Winget, D.G., Marchand, K.A., Williamson, E.B., “Analysis and Design of Critical Bridges Subjected to Blast Loads.” Journal of Structural Engineering, August 2005, pp. 1243-1255.