

ABSTRACT

Title of Document: CRITICAL ASSET AND PORTFOLIO RISK ANALYSIS FOR HOMELAND SECURITY

William L. McGill, Doctor of Philosophy, 2008

Directed by: Professor Bilal M. Ayyub, Department of Civil and Environmental Engineering

Providing a defensible basis for allocating resources for critical infrastructure and key resource protection is an important and challenging problem. Investments can be made in countermeasures that improve the security and hardness of a potential target exposed to a security hazard, deterrence measures to decrease the likeliness of a security event, and capabilities to mitigate human, economic, and other types of losses following an incident. Multiple threat types must be considered, spanning everything from natural hazards, industrial accidents, and human-caused security threats. In addition, investment decisions can be made at multiple levels of abstraction and leadership, from tactical decisions for real-time protection of assets to operational and strategic decisions affecting individual assets and assets comprising a regions or sector.

The objective of this research is to develop a probabilistic risk analysis methodology for critical asset protection, called Critical Asset and Portfolio Risk Analysis, or CAPRA, that supports operational and strategic resource allocation decisions at any level of leadership or system abstraction. The CAPRA methodology consists of six analysis phases: scenario identification, consequence and severity assessment, overall vulnerability assessment, threat probability assessment, actionable risk assessment, and

benefit-cost analysis. The results from the first four phases of CAPRA combine in the fifth phase to produce actionable risk information that informs decision makers on where to focus attention for cost-effective risk reduction. If the risk is determined to be unacceptable and potentially mitigable, the sixth phase offers methods for conducting a probabilistic benefit-cost analysis of alternative risk mitigation strategies. Several case studies are provided to demonstrate the methodology, including an asset-level analysis that leverages systems reliability analysis techniques and a regional-level portfolio analysis that leverages techniques from approximate reasoning.

The main achievements of this research are three-fold. First, this research develops methods for security risk analysis that specifically accommodates the dynamic behavior of intelligent adversaries, to include their tendency to shift attention toward attractive targets and to seek opportunities to exploit defender ignorance of plausible targets and attack modes to achieve surprise. Second, this research develops and employs an expanded definition of vulnerability that takes into account all system weaknesses from initiating event to consequence. That is, this research formally extends the meaning of vulnerability beyond security weaknesses to include target fragility, the intrinsic resistance to loss of the systems comprising the asset, and weaknesses in response and recovery capabilities. Third, this research demonstrates that useful actionable risk information can be produced even with limited information supporting precise estimates of model parameters.

CRITICAL ASSET AND PORTFOLIO RISK ANALYSIS FOR
HOMELAND SECURITY

By

William L. McGill

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2008

Advisory Committee:

Professor Bilal M. Ayyub, Chair
Professor Amde M. Amde
Associate Professor Michel Cukier
Professor Mohammad M. Modarres
Professor Ali Mosleh

© Copyright by
William L. McGill
2008

Dedication

To my wife Jinny and our sons Keith and William

Table of Contents

Dedication	ii
Table of Contents	iii
List of Tables	vi
List of Figures	ix
Chapter 1. Introduction	1
1.1. Motivation and Problem Description	1
1.2. Objectives and Scope	2
1.3. Outline of Dissertation	4
Chapter 2. Literature Review	6
2.1. Risk Analysis for Security	6
2.2. From Cause to Consequence: Initiating Events and Dimensions of Loss	9
2.2.1. Risk Analysis for Decision Support: The Role of World View	10
2.2.2. The Nature of Threat and its Assessment	11
2.2.3. The Nature of Consequence and its Assessment	18
2.2.4. Screening of Initiating Events	21
2.2.5. Risk and Surprise	22
2.2.6. Levels of Analysis	26
2.3. Notions and Measures for Security Risk Analysis: Threat and Vulnerability	29
2.3.1. The Nature of Vulnerability	30
2.3.2. Probability of Occurrence for the Initiating Event	35
2.3.3. Previous Methodological Work	36
2.4. Actionable Risk Information	40
2.5. Risk Management: Countermeasures and Mitigation	40
Chapter 3. Methodology	44
3.1. Risk Analysis Framework	44
3.2. Scenario Identification	46
3.3. Consequence and Severity Assessment	49
3.4. Overall Vulnerability Assessment	50
3.4.1. Protection Vulnerability	53
3.4.2. Response Vulnerability	60
3.4.3. Overall Vulnerability	63
3.5. Threat Probability Assessment	65
3.5.1. The Basic Model	65
3.5.2. Proportional Attractiveness Model	68
3.5.3. Aggregate Vulnerability	78
3.6. Actionable Risk Assessment	81
3.6.1. Expressing Risk	81
3.6.2. Loss Accumulation	81
3.6.3. Sensitivity Analysis	84
3.7. Benefit-Cost Analysis	85
Chapter 4. Case Study – Asset Analysis	87
4.1. Problem Description	87
4.2. Scenario Identification	88
4.3. Consequence and Severity Assessment	97

4.4. Overall Vulnerability Assessment	98
4.4.1. Security System Effectiveness	98
4.4.2. Target Accessibility	106
4.4.3. Target Hardness and System Response	107
4.4.4. Response and Recovery	110
4.5. Threat Probability Assessment	111
4.6. Actionable Risk Assessment.....	117
4.7. Benefit-Cost Analysis	119
4.8. Discussion	123
Chapter 5. Case study – Regional Risk Analysis	128
5.1. Problem Description	128
5.2. Threat Characterization.....	138
5.3. Asset Characterization	142
5.3.1. Relevant Attack Modes.....	142
5.3.2. Maximum Potential Loss and Value of Disruption	143
5.3.3. Security System Effectiveness (Asset)	144
5.3.4. Probability of Successful Attack Execution	159
5.3.5. Asset Fragility Matrices.....	160
5.3.6. Basis Loss	167
5.3.7. Asset Visibility.....	170
5.4. Regional Characterization.....	170
5.4.1. Response and Recovery Effectiveness - Fatalities.....	170
5.4.2. Interdependency Analysis.....	178
5.4.3. Probability of Adversary Success in Region	182
5.5. CAPRA Risk Assessment.....	185
5.5.1. Consequence and Severity Assessment	186
5.5.2. Overall Vulnerability Assessment: Security Vulnerability Assessment... 190	
5.5.3. Conditional Loss Given Attack.....	191
5.5.4. Threat Probability Assessment	192
5.5.5. Regional Risk Profiles and Actionable Risk Information.....	196
5.6. Discussion	206
Chapter 6. Conclusions and Future Work	210
6.1. General Discussion	210
6.2. Avenues for Future Research.....	213
Appendix A. Fuzzy Sets, Fuzzy Logic, and Evidence Theory	217
A.1. Fuzzy Numbers and their Membership Functions	217
A.2. The Extension Principle.....	220
A.3. Constructing a Fuzzy System.....	221
A.4. Fuzzification and Rule Matching.....	224
A.5. Fuzzy Inference: Evidence Theory Approach	226
A.6. Fuzzy Inference: Standard Additive Model Approach	235
A.7. Arithmetic on Random Sets with Unknown or Uncertain Dependence	237
Appendix B. Results of the Regional Case Study.....	241
B.1. Conditional Public Health & Safety Loss Distribution Given Successful Attack	241
B.2. Conditional Disruption Loss Distribution Given Successful Attack	251

B.3. Conditional Aggregate Loss Distribution Given Successful Attack.....	261
B.4. Conditional Aggregate Loss Given Attack: By Attack Profile.....	271
B.5. Conditional Loss-Exceedance Given Attack.....	281
Appendix C. Publications Resulting From This research.....	286
C.1. Accepted Publications to Peer-Reviewed Journals.....	286
C.2. Publications Submitted for Peer Review.....	286
C.3. Book Chapters.....	286
C.4. Conference Proceedings.....	287
C.5. Presentations.....	287
Appendix D. Curriculum Vitae.....	290
Bibliography.....	294

List of Tables

Table 2-1. Partial list of naturally occurring and anthropic events.....	14
Table 3-1. Target susceptibility matrix for a notional asset.....	47
Table 3-2. Expanded target susceptibility and risk screening matrix based on a hybrid FMECA/CARVER method with notional entries.....	48
Table 3-3. Crisp loss dimensions and associated units of measure	50
Table 3-4. Attack profile compatibility matrix for an initiating event	57
Table 4-1. Explosive attack modes and expected loss given success.....	91
Table 4-2. Hybrid FMECA/CARVER model parameters and interpretation.....	94
Table 4-3. Scoring scheme for each probability parameters of the hybrid approach	94
Table 4-4. Scoring scheme for each consequence parameter of the hybrid approach	95
Table 4-5. Scoring scheme for the recoverability parameter.....	95
Table 4-6. Hybrid FMECA/CARVER assessment for the notional chemical facility	96
Table 4-7. Maximum potential loss and loss conversion factors.....	98
Table 4-8. Attack profile compatibility matrix for explosive attack against the tank farm	105
Table 4-9. Security system performance attributes for each security zone	106
Table 4-10. Summary of results for the explosive attack against tank farm event.....	106
Table 4-11. Probability of successful execution for each of the five delivery systems..	107
Table 4-12. Fragility of system response to different attack intensities	108
Table 4-13. Aggregate fragility of system response to different attack intensities	109
Table 4-14. Expected aggregate loss give successful attack against the tank farm for both the independent and dependent case	111
Table 4-15. Notional perceived probability of successful capability acquisition.....	112
Table 4-16. Assessed visibility of tank farm attack profiles.....	112
Table 4-17. Summary of results from the sensitivity analysis.....	119
Table 4-18. Alternative risk mitigation options.....	121
Table 5-1. Target Capabilities List (DHS 2006c; DHS 2007).....	132
Table 5-2. Relevant of capabilities to CAPRA model variables	137
Table 5-3. Delivery system types for IED events (Neale 2008).....	140
Table 5-4. Notional perceived probability of acquisition and capability.....	141
Table 5-5. Attack profile compatibility matrix for the five regional assets.....	143
Table 5-6. Maximum potential loss for each asset	144
Table 5-7. Daily value of total disruption for each asset	144
Table 5-8. Asset Defensive criteria for probability of adversary success assessment (Morgenson et al. 2006).....	145
Table 5-9. Security system effectiveness assessment for the office building.....	155
Table 5-10. Security system effectiveness assessment for the hospital.....	156
Table 5-11. Security system effectiveness assessment for the train station	157
Table 5-12. Security system effectiveness assessment for the stadium.....	158
Table 5-13. Security system effectiveness assessment for the electric power substation	159
Table 5-14. Probability of successful execution for each of the five delivery systems..	160

Table 5-15. Probability of damage subject to different size IED attacks for the office building.	161
Table 5-16. Probability of damage subject to different size IED attacks for the hospital.	162
Table 5-17. Probability of damage subject to different size IED attacks for the train station.	163
Table 5-18. Probability of damage subject to different size IED attacks for the stadium.	164
Table 5-19. Probability of damage subject to different size IED attacks for the electric power substation.	165
Table 5-20. Probability of damage states for each asset and attack mode combination.	166
Table 5-21. Basis loss for each damage state (disruption).	168
Table 5-22. Basis loss for each damage state (fatalities)	169
Table 5-23. Notional regional Capability Assessment	177
Table 5-24. First-order regional asset interdependency matrix	181
Table 5-25. Regional Defensive criteria for probability of adversary success assessment	183
Table 5-26. Notional rules for security system effectiveness assessment in the region.	184
Table 5-27. Assessed values for the regional defensive criteria for each attack mode ..	185
Table 5-28. Date on value of statistical life (Viscusi and Aldy 2003).	188
Table 5-29. Rules for threat probability / recurrence reduction.	195
Table 5-30. Matrix of levels of loss for different pignistic percentile distributions and degrees of probability of exceedance.	199
Table 5-31. Sensitivity of the risk results to favorable changes in each regional capability	200
Table A-1. $\gamma(b)$ for selected continuous bell-shaped functions (McGill and Ayyub 2008)	229
Table B-1. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (office building).	242
Table B-2. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (hospital).	244
Table B-3. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (train station)	246
Table B-4. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (stadium).	248
Table B-5. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (power substation)	250
Table B-6. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (office building)	252

Table B-7. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (hospital)	254
Table B-8. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (train station).....	256
Table B-9. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (stadium)	258
Table B-10. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (power substation).....	260
Table B-11. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (office building).....	262
Table B-12. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (hospital)	264
Table B-13. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (train station).....	266
Table B-14. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (stadium)	268
Table B-15. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (power substation).....	270
Table B-16. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (office building)	272
Table B-17. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (hospital)	274
Table B-18. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (train station).....	276
Table B-19. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (stadium)	278
Table B-20. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (power substation).....	280

List of Figures

Figure 2-1. Vulnerability as the mapping between initiating events (i.e., cause) to resulting degree of loss (i.e., consequence)	9
Figure 2-2. DHS National Planning Scenarios (US Department of Homeland Security 2006c)	16
Figure 2-3. Some sources of surprise in risk analysis for critical infrastructure protection (McGill and Ayyub 2008b).....	23
Figure 2-4. Hierarchy of ignorance types highlighting those types that contributes to overall vulnerability to surprise	24
Figure 2-5. Notional portfolio of assets in a state (Ayyub et al. 2005).....	28
Figure 2-6. Notional portfolio of assets in a nation (Ayyub and McGill 2007)	28
Figure 2-7. Various asset portfolios defined by locale, sector, etc.	29
Figure 2-8. DHS target capabilities list (US Department of Homeland Security 2006c). ..	43
Figure 3-1. Framework for asset- and portfolio-level risk analysis.....	44
Figure 3-2. Mapping from event type (threat item) to targetable element via risk agents (phenomenologies).....	49
Figure 3-3. Logical sequence of interventions between initiating event (cause) to resulting degree of loss (consequence)	52
Figure 3-4. Cross-section of an intrusion path.....	56
Figure 3-5. Possibility tree for threat probability assessment.....	68
Figure 4-1. Site plan for the notional chemical facility	88
Figure 4-2. Threat intensity distribution for a given attack mode	90
Figure 4-3. Possibility tree for the hybrid FMECA/CARVER method.....	93
Figure 4-4. Event tree for assessing security system effectiveness	100
Figure 4-5. Representative intrusion paths into the chemical facility	104
Figure 4-6. Intrusion paths to a chemical tank.....	105
Figure 4-7. Probability density and cumulative distribution functions for loss.....	110
Figure 4-8. Threat probabilities without visibility for different values of b (for the independent and perfectly dependent cases).....	113
Figure 4-9. Probability distribution over attack profiles with and without considering visibility ($b=2$) (for the independent and perfectly dependent cases).....	114
Figure 4-10. Individual and aggregate loss distributions for tank farm attack profiles (shown only for the independent case)	115
Figure 4-11. Individual and aggregate probability density and cumulative distribution functions considering tank farm and main building attack profiles.....	116
Figure 4-12. Percentile loss-exceedance curves for explosive attacks afflicting the chemical facility (shown only for the independent case).....	118
Figure 4-13. Cumulative probability distributions for accumulated benefit associated with each risk mitigation action tabulated expected benefits	122
Figure 5-1. Five infrastructure assets in the study region.....	129
Figure 5-2. Implementation of CAPRA for regional risk analysis	131
Figure 5-3. Schematic of the fuzzy system architecture for security system performance assessment.....	148

Figure 5-4. Membership functions for the fuzzy numbers representing degree of effectiveness on a constructed scale	149
Figure 5-5. Membership functions for some fuzzy numbers representing probability of adversary success	149
Figure 5-6. Exhaustive set of fuzzy inference rules for a hand emplaced explosive attack	152
Figure 5-7. Exhaustive set of fuzzy inference rules for a ground vehicle and waterborne vehicle explosive attack	153
Figure 5-8. Exhaustive set of fuzzy inference rules for an aerial vehicle explosive attack	154
Figure 5-9. Notional conditional possibilistic loss exceedance curve given successful attack	172
Figure 5-10. Membership functions for states of the input capability variables	174
Figure 5-11. Membership functions for states of the input loss variable.....	174
Figure 5-12. Membership functions for states of the output reduction variable.....	175
Figure 5-13. Conditional rules bases for fatality loss reduction. Each circle maps a rule number to an output state R_i	176
Figure 5-14. Conditional cumulative distribution on public health and safety loss for the office building subject to a ground vehicle attack	178
Figure 5-15. Conditional cumulative distribution on disruption loss for the office building subject to a ground vehicle attack.....	181
Figure 5-16. Membership functions of different states for regional defensive criteria ..	183
Figure 5-17. Output fuzzy sets for the regional security model.	184
Figure 5-18. Fuzzy value of life (FVOL) derived from data of Viscusi and Aldy (2003)	187
Figure 5-19. Conditional cumulative distribution on aggregate loss valued in dollars for the office building subject to a ground vehicle attack	190
Figure 5-20. Probability of attack for alternative attack modes for each asset.....	193
Figure 5-21. Relative probability of attack for each asset in the region.....	193
Figure 5-22. Output sets for % reduction in threat probability or recurrence rate.....	195
Figure 5-23. Possibilistic conditional aggregate loss-exceedance curve given an attack in the region	197
Figure 5-24. Membership function for the conditional mean aggregate loss in the region given attack	198
Figure 5-25. Possibilistic loss-exceedance curve in light of explosive attacks occurring in the region against one of the five assets in the next 5 years	198
Figure A-1. Fuzzy numbers for selected probability words	218
Figure A-2. Approximation of a function $Y = f(x)$ with a set of fuzzy rule patches	223
Figure B-1. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (office building)	241
Figure B-2. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (hospital).....	243
Figure B-3. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (train station)...	245

Figure B-4. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (stadium)	247
Figure B-5. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (power substation)	249
Figure B-6. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (office building).....	251
Figure B-7. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (hospital).....	253
Figure B-8. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (train station)	255
Figure B-9. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (stadium).....	257
Figure B-10. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (power substation)	259
Figure B-11. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (office building).....	261
Figure B-12. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (hospital).....	263
Figure B-13. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (train station)	265
Figure B-14. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (stadium).....	267
Figure B-15. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (power substation)	269
Figure B-16. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (office building).....	271
Figure B-17. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (hospital).....	273
Figure B-18. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (train station)	275
Figure B-19. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (stadium).....	277
Figure B-20. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (power substation)	279
Figure B-21. Possibilistic conditional loss-exceedance curve given attack (office building).....	281
Figure B-22. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (office building)	281
Figure B-23. Possibilistic conditional loss-exceedance curve given attack (hospital) ...	282
Figure B-24. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (hospital)	282
Figure B-25. Possibilistic conditional loss-exceedance curve given attack (train station)	283
Figure B-26. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (train station)	283

Figure B-27. Possibilistic conditional loss-exceedance curve given attack (stadium) ...	284
Figure B-28. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (stadium)	284
Figure B-29. Possibilistic conditional loss-exceedance curve given attack (power substation).....	285
Figure B-30. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (power substation).....	285

Chapter 1. Introduction

1.1. Motivation and Problem Description

Providing a defensible basis for allocating resources for critical infrastructure and key resource protection is an important and challenging problem. Investments can be made in countermeasures estimated to improve the security and hardness of a potential targets exposed to a variety of security events, deterrence measures to decrease the likeliness of a such events, and capabilities to mitigate human, economic, and other losses following an incident. Multiple types of initiating events must be considered, including naturally occurring phenomena, technological accidents, and malicious attacks. In addition, investment decisions can be made at multiple levels of abstraction and leadership, from tactical decisions for real-time protection of assets to strategic decisions affecting asset portfolios, regions, and infrastructure systems. To accommodate the complexity of the decision variables, the multitude and uncertain nature of possible threats, and the need for defensible risk results to better inform resource investment decision making at all levels, a mathematically sound methodology that quantifies knowledge and expresses uncertainty in a meaningful way, accounts for all major risk contributors, and can be scaled to accommodate different levels of abstraction is required (Garrick et al. 2004).

Decisions to enhance the protection of critical infrastructure and key resources center of choosing from among a variety of preventive, protective, response, and recovery strategies to meet risk reduction objectives given finite available resources. Risk management strategies are of two general types – strategies to reduce the frequency

of adverse events and strategies for mitigating the ensuing consequences given their occurrence (Pate-Cornell 1986). While both natural and anthropic (i.e., human-caused) events are within the scope of homeland security, particularly troublesome are those intentional attacks initiated by an adversary that has motivation (e.g., selfish, political, economic, and religious), possesses variable and broad capabilities (e.g., weapons, manpower, and education), and is adaptive by being responsive to countermeasures (Hoffman 1998; Jackson 2001; Sandler and Lapan 1988). To the decision maker's benefit, there are many options available for mitigating security risks than those arising from natural hazards given that both probability and consequence can be affected through risk reduction strategies, such as through a combination of enhanced security and deterrence at critical sites and measures to maintain continuity of lifeline services before, during, and following a malicious attack. Many of these options have a collateral effect of reducing risks attributable to naturally occurring events, such as hazard neutral emergency response measures. In order to quantitatively evaluate the effectiveness of risk mitigation strategies across all hazards, levels of leadership and system abstractions, a common analytical framework is needed that accommodates all-hazards risk analysis.

1.2. Objectives and Scope

In order to provide defensible risk information that facilitates judgments of risk acceptance or non-acceptances and benefit-cost analysis while accommodating all uncertainties, a quantitative framework for risk assessment and management is needed. The overarching objective of this research is to develop a quantitative risk analysis methodology for critical asset protection in light of security events, terrorist attacks in

particular, that supports operational and strategic resource allocation decisions at any level of abstraction.

Risk studies help decision makers cope with the uncertainties present in their strategic environment. Accordingly, the results from any risk assessment methodology must, in general, (1) be aligned to produce information that is timely and relevant to the needs of the decision maker, and (2) follow from a process that is meaningful and acceptable to the consumer (Blockley 1992). Prior to the establishment of any risk analysis process, the questions and issues demanding the attention of a decision maker needs to be identified. The nature of these issues drives the appropriate mathematical structure to use so as to provide meaningful results with sufficient resolution to support decision making. The following general requirements can be established for a quantitative risk analysis framework that supports critical asset protection decisions:

- The methodology must be designed to inform resource allocation decisions for critical asset and portfolio protection by producing actionable risk information. That is, the methodology must be tailored to answer the question “where should decision makers focus their attention to achieve cost effective risk reduction?” and then provide the means to evaluate alternative risk reduction strategies.
- The methodology must build upon current accepted thinking and practices in security risk analysis. Accordingly, the methodology must consider all relevant aspects of the security risk analysis problem (i.e., threat, vulnerability, and consequence). Clear operational definitions of model parameters to facilitate their interpretation, analysis, and measurement must be specified.

- The mathematical structure must be sound, logical, and transparent to explain all relationships between cause (initiating events) and consequence. Moreover, it must produce risk information that properly propagates all uncertainties present in the inputs (i.e., the methodology should be faithful to the information provided).
- The methodology must be scalable to accommodate the needs of decision makers at all levels of abstraction and leadership, including operational and strategic asset, sectoral, and regional analysis. While there is no expectation that needs of each decision maker will be the same, the general philosophy underpinning the methodology must be consistent and scalable. This feature promotes compatibility of risk information at various levels of abstraction under a common framework.
- In the case of malicious attacks where the initiating events demonstrate intent and choice, the methodology must accommodate the dynamic nature of human adversaries, particularly their tendencies to shift preferences in response to security investments. For strategic analysis, the methodology must capture the shifting of adversary attention from protected assets to less protected assets, from difficult to less difficult attack modes, etc.

1.3. Outline of Dissertation

The outline of this dissertation is as follows. Beginning with a comprehensive review of the research literature on risk analysis for infrastructure protection and related security problems in Chapter 2, this dissertation develops a quantitative methodology for critical asset and portfolio risk analysis (Chapter 3) that meets the requirements outlined

in the previous section. The sources of risk considered in this methodology are malicious security threats affecting the interests of those decision makers (e.g., asset owners, regional leadership, etc.) responsible for the proper functioning and operation of critical infrastructure and key resources and the health and safety of the people under their care. The proposed methodology is generic in that it identifies, at a high level, all relevant dimensions of risk and how they interact to describe risk. Moreover, the quantitative framework underlying the methodology can accommodate information on the constituent parameters expressed in a variety of quantitative forms and derived from different models which is then aggregated in a probabilistic framework. To demonstrate different qualities and aspects of the proposed methodology, Chapters 4 and 5 provide case studies applying the methodology to different problems. In particular, Chapter 4 applies a purely probabilistic implementation of the methodology to the analysis of a notional infrastructure facility (i.e., asset-level analysis), to include systems reliability modeling and the use of maximum entropy arguments to construct distributions from minimal data. Chapter 5 leverages techniques from approximate reasoning and imprecise probabilities to propagate highly uncertainty probabilistic information through an otherwise probabilistic framework to support analysis of a region containing multiple assets of concern to a regional decision maker. Chapter 6 concludes this dissertation with a summary of the research findings and directions for future work. Mathematical details to support the analysis in Chapters 4 and 5, which includes much of the author's own work, is provided in Appendix A.

Chapter 2. Literature Review

2.1. Risk Analysis for Security

Risk analysis is a technology for overlaying uncertainty about future events atop societal values to inform decisions on how to minimize the potential for undesirable impacts on people, property, and essential services. The philosophy of risk analysis, to include risk assessment and risk management among other risk-related activities (Society for Risk Analysis 2008), is embodied by the “six questions of risk” as follows (Kaplan and Garrick 1981; Haimes 1991; and later paraphrased by McGill and Ayyub 2007 and refined later by McGill 2008):

Risk Assessment

- (1) What are potential causes of harm?
- (2) What specific consequences are of concern?
- (3) How likely are these pairings of cause and consequence?

Risk Management

- (4) What can be done to reduce the potential for undesirable consequences or increase the potential for favorable outcomes?
- (5) What real options are available and what are their tradeoffs in terms of their associated benefits, costs, and risks?
- (6) What are the impacts of current decisions on future options?

In the context of homeland security and critical asset protection, the common conceptual expression for security risk, or the potential for harm of loss resulting from a the occurrence of a threatening event (e.g., natural, technological, accidental, or malicious) afflicting a valued target, system, or societal element, is traditionally written as (see Broder 1984; Matalucci 2002; Moteff 2005; Willis et al. 2005; US Department of Homeland Security 2006b):

$$Risk = Threat \times Vulnerability \times Consequence \quad (2-1)$$

where the total risk is the combination or Cartesian product of all relevant security events (the “threat”), system weaknesses (the “vulnerability”), and undesired outcomes resulting when these security events interact with or exploit the vulnerabilities (the “consequence”). With regards to the first three questions, risk assessment for security problems focuses on constructing a full suite of plausible initiating events or attacks, assessing their likeliness of occurring, and assessing the likeliness of various consequences given attack considering security countermeasures and consequence mitigation strategies (Broder 1984). Security risk is, then, a probabilistic statement centered on the intersection of a particular cause and a particular consequence, or more generally, as the uncertainty constructed on the consequence dimensions considering all relevant security events (i.e., risk as uncertainty of consequence per Aven 2003).

Risk, as Eq. 2-1 suggests, tells a series of stories of all that could go wrong from initiating event to final outcome, where the heart of these stories - the vulnerabilities - describe those weaknesses that must manifest in order to make this risk scenario true.

Here we define a *risk scenario* as the pairing of a particular event and a particular consequence. In this sense, vulnerability provides a mapping between the set of initiating events and the set of outcomes, such as is shown in Figure 2-1 (McGill and Ayyub 2007b). This interpretation is in agreement with Aven's (2008) definition of vulnerability as the uncertainty on consequence given the occurrence of an initiating event. Any statement of vulnerability or risk to a given initiating event must always be in reference to some adverse outcome or degree of loss, whether descriptive, qualitative or quantitative in nature. Generic statements, such as "my vulnerability is high" or "the risk is moderate" are inherently ambiguous unless they are associated with a specific cause and a particular consequence, if even expressed on an arbitrarily constructed or vaguely defined numeric scale (e.g., "my vulnerability to undesirable outcomes from my exposure to a hazard is high").

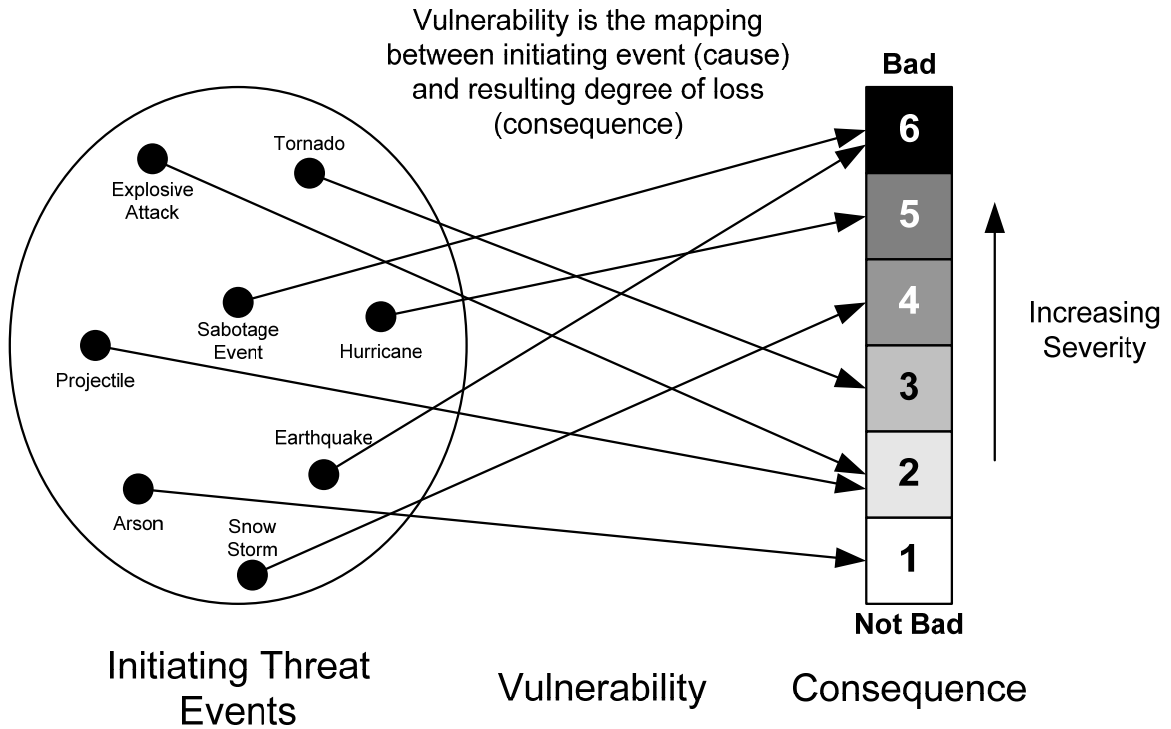


Figure 2-1. Vulnerability as the mapping between initiating events (i.e., cause) to resulting degree of loss (i.e., consequence)

2.2. From Cause to Consequence: Initiating Events and Dimensions of Loss

According to the conceptual security risk analysis formula in Eq. 2-1 and the discussion of risk in the previous section, any statement of risk, whether qualitative, descriptive, or quantitative, requires specification of a cause and a consequence, either of which may be vague or precise depending on the needs of the decision maker and the nature of the available information. This section briefly describes the role of decision maker world view in establishing the scope of a risk analysis and discusses the nature of threat and consequence and their relation to risk assessment.

2.2.1. Risk Analysis for Decision Support: The Role of World View

The role of the risk analyst is to provide sufficient and relevant information that empowers decision makers to exercise their own judgments (Pate-Cornell 2007), though risk reduction decisions must be made with or without formal deliberate analysis (Deisler 2002). As a decision support activity, risk analysis must be sensitive to the world view of the decision maker (Berresford and Dando 1978). World view is shaped by the decision maker's personal interests and that of his constituency (e.g., the people in a representative democracy). To narrow the scope of a risk analysis and tailor the process to meet the unique decision support needs of a decision maker, it is important to focus attention on those events that are plausible and relevant to a decision maker, and then study how these events can result in consequences deemed unfavorable. The key to generating all relevant pairings of cause and consequence, i.e., *risk scenarios*, is to first understand the needs of the decision maker (American Society for Industrial Security 2003).

Cox (2002) offers a technique for framing the interests of a decision maker to assist in defining risks. Referred to by its acronym *STEM*, this technique starts by defining the *sources* (S) of risk (e.g., hazards, initiating events) that are of concern to the decision maker, identifies the *targets* (T) that could be affected by one or more of these source of risk, identifies what the *effects* (E) out outcomes that can result when the source of risk afflicts a susceptible target, and seeks to describes the *mechanisms* (M) by which these effects our outcomes occur. A revised version of the STEM technique that is helpful for framing both risk assessment and risk management could be relabeled as the *VEST*, *POST* or *PEST* model for *variables* (or *parameters*) that characterize the decision maker's ability to act in his environment, *effects* (or *outcomes*) of concern, *sources* of risk

that could plausibly interact with vulnerabilities to yield these outcomes (e.g., event types), and *targets* that are susceptible to these sources of risk. Either the STEM or the VEST/POST/PEST techniques helps risk analysts establish the context from which to construct risk scenarios and carry out the risk analysis.

According to Ericson (2006), risk assessment is “an uncertainty knowledge claim about contingent future events that cannot be fully known,” and that any decision made in the process of risk management must “bear the uncertainty of false positives and false negatives.” In general, as suggested in the 2002 Department of Energy guideline for vulnerability assessment, the value added of performing a risk or vulnerability assessment is to build and broaden awareness of security and risk issues among senior management; establish or evaluate against a baseline; identify vulnerabilities and develop responses; categorize key assets and drive the risk management process; develop and build internal skills and expertise; promote action; and to kick-off an ongoing security effort (US Department of Energy 2002). Irrespective of the results generated by the assessment, at the very least risk studies offer a systematic process for building institutional knowledge of potential sources for harm and the manner in which such harm can be realized (Herabat 2003).

2.2.2. The Nature of Threat and its Assessment

In the security sense, threat has traditionally been defined as an intention and capability to undertake actions that are harmful or detrimental to an asset (US Department of Homeland Security 2006b; US Department of Defense 2005). Aven (2008) equates the words hazard and threat with initiating event, where the word hazard

is used to speak of naturally occurring phenomena and threat is used to speak of deliberate actions. Yet, it is common to speak of anything that exposes an individual to potentially unacceptable outcomes as a threat regardless of its nature. Building on the definition of a hazard as a source of risk (Ayyub 2003), a more general notion can be established for threat as a hazardous event (hereafter called an “initiating event”) with the potential to adversely affect those aspects of life that decision makers care about (e.g., health and safety, property, future revenue, essential services). That is, further qualifying a hazard as a threat implies that there is at least a possibility of the hazard adversely affecting the decision maker’s interests to result in undesirable outcomes. Take for example a strong hurricane, a peril that without question is a major source of risk in the United States. If one examines the meteorological record of the US to estimate probability or rate of recurrence for tropical storms in different geographical regions, strong hurricanes are threatening to residents of southeastern coastal communities, less threatening to more inland and northeastern coastal communities, and not threatening at all to individuals situated in the upper mid-western portion of the nation. From the regional decision maker’s point of view, if the likeliness of a strong hurricane afflicting is extremely rare, then it is not a threat despite being objectively labeled a hazard and regardless of whether the system is susceptible to harm if such an event were to occur. Yet, hurricanes are still objectively a hazard regardless of them not being a threat. Similarly, even if an event is frequent, it may not warrant being labeled a threat if the response and recovery capabilities of the afflicted system are sufficient to contain loss. For example, seismic building codes adopted by the State of California impose requirements that all structures be capable of withstanding minimal-defined loads

imposed by the ground motion of a large earthquake (Mileti 1999). Prior to the implementation of these codes, magnitude 6 earthquakes (on the Richter scale) were a major source of risk, whereas now the potential for loss given their occurrence is much less. Thus, from some decision makers' point of view, a magnitude 6 earthquake afflicting southern California is no longer a threat despite having been so in the not too distant past. In this case, the threat has been largely neutralized through improved engineering design, materials, and construction practices. This latter point echoes the sentiment of Arnold (2002) who reminds us that disasters and extreme events arise from some disequilibrium between environmental events and the vulnerabilities of human communities. As Haque and Etkin (2007) put it, humans cause disasters, not naturally occurring events. That is, we suffer from disasters because we create the conditions in which to experience disaster, whether unwittingly or deliberate; unless such extreme events affect people, they are merely events with no social significance.

The foregoing reasoning suggests that calling an event a threat imposes the subjective judgment of a decision maker atop an otherwise objective event according to its perceived likeliness for occurring and seriousness of the ensuing outcomes. Initiating events can take on many forms in the homeland security context. Classes of initiating events of concern to homeland security decision makers include, but are not limited to, naturally occurring phenomena (e.g., hurricanes, earthquakes, solar flares), industrial accidents and technological failures (e.g., chemical release, train derailment, refinery fire), and malicious attacks (e.g., bombing, sabotage, chemical attack). A listing of many, though by no means complete, initiating event types compiled from a variety of sources is provided in Table 3-1 divided into categories labeled "naturally occurring" for

those events due to acts of nature and “anthropic” for events derived from the behavior and artifacts of humans (Fontaine et al. 2007). The focus of the current research is on malicious anthropic events (explosive attacks, in particular), though the methodology developed in this research is broadly applicable to all types of events (Ayyub et al. 2007).

Table 2-1. Partial list of naturally occurring and anthropic events

Partial List of Naturally Occurring and Anthropic Events	
<p>Naturally Occurring</p> <ul style="list-style-type: none"> • Earthquake • Tropical Storm / Hurricane • Blizzard / Winter Storm • Tornado • Tsunami • Volcano Eruption • Landslide • Flooding • Wildfire • High Wind / Windstorms • Extreme Temperature • Disease Outbreak • Drought • Meteorite / Asteroid 	<p>Anthropic (Unintentional)</p> <ul style="list-style-type: none"> • Industrial Accident • Technological Failure <p>Anthropic (Intentional)</p> <ul style="list-style-type: none"> • Explosive • Projectile / Ballistic • Incendiary • Chemical • Biological • Radiological • Nuclear • Radiofrequency / EMP • Sabotage • Cyber • Laser

The description of an initiating event alone is insufficient to commence a risk analysis unless it is in reference to some target of its effects, whether physical, societal, logical, etc. The assessment of risk insists that it be placed into a decision making context that considers the unique interests and concerns of the decision maker. For decision makers charged with protecting infrastructure, whether at the asset, sectoral, or regional level, a prime concern is the impact of various initiating events on the performance of the elements that enable the asset to function, including hardware, time,

people, and information. Many risk-related methodologies spell out a process for “asset characterization” or “asset identification” whether as a specific step (see American Society for Industrial Security 2003) or part of some other step (such as scenario identification in McGill et al. 2007), as a prerequisite for a full scale risk or vulnerability assessment.

In the absence of reliable information or evidence supporting a judgment of which types of events are possible at a given location, a complete set of plausible initiating events can be identified based solely on the inherent susceptibilities of collocated system elements to a wide spectrum of plausible event types and without the need for intelligence supporting adversary intent. This style of analysis has been referred to as an *asset-driven* approach (McGill et al. 2007) or *asset-based* approach (Center for Chemical Process Safety 2002). An asset-driven analysis estimates the consequences and probability of adversary success for an exhaustive set of plausible initiating events without regard to their probability of occurrence, and then overlays their likeliness of occurrence if such information is available. As Lave (2002) suggests, asset-driven approaches search for sensitive points that adversaries can exploit to kill a lot of people and destroy a lot of property, that is, the focus is on finding and correcting vulnerabilities regardless of whether a specific type of event has occurred. In contrast, *threat-driven* or *event-driven* approaches employed in many risk assessment methodologies begin with a predefined set of initiating events based on assumed adversary capabilities (e.g., design basis threats such as in Center for Chemical Process Safety 2002) justified by intelligence or historical record, and proceeds through the remainder of the analysis constrained by the definition and scope of these events. For example, a threat-driven approach in the

context of regional and national preparedness planning might focus exclusively on the 15 national planning scenarios defined by DHS (US Department of Homeland Security 2006c) and shown in Figure 2-2. In fact, as Hollenstein (2002) showed, about 80% of the available models for vulnerability assessment (as of 2001) are designed for a specific combination of source and target. Event-driven approaches are appropriate for studying initiating events that are well understood and whose rate of occurrence can be reliably predicted from historical data; however, they ultimately fail to consider emerging or unrecognized threats devised by an innovative adversary or those naturally-occurring events for which there is no human-recorded record (Woo 1999). An asset-driven approach brings all plausible threat scenarios to the forefront in attempt to reduce ontological uncertainty and defeat the potential for surprise without limiting attention to only what is known about adversary intent.

- | | |
|------------------------------|-----------------------------------|
| 1. Improvised Nuclear Device | 9. Major Earthquake |
| 2. Aerosol Anthrax | 10. Major Hurricane |
| 3. Pandemic Influenza | 11. Radiological Dispersal Device |
| 4. Plague | 12. Improvised Explosive Device |
| 5. Blister Agent | 13. Food Contamination |
| 6. Toxic Industrial Chemical | 14. Foreign Animal Disease |
| 7. Nerve Agent | 15. Cyber |
| 8. Chlorine Tank Explosion | |

Figure 2-2. DHS National Planning Scenarios (US Department of Homeland Security 2006c)

The level of specificity and detail chosen to articulate each initiating event and consequence affects how likeliness is assessed (Kaplan et al. 2001). Given a collectively

exhaustive set of all possible distinct initiating events of specified type (e.g., explosive), highly detailed event descriptions are larger in number than more general events, require more analytical effort to ascertain and assess in terms of time and attention, but provide a high resolution account and understanding of total risk. In contrast, less specific event descriptions are fewer in number than specific ones, but coincide with greater uncertainty in the consequence dimension to accommodate the increased number of variations in the nature and sequence of events between cause and consequence. Moreover, meeting the exhaustiveness requirement for initiating events oftentimes requires one to include a residual, perhaps unknown, initiating event to account for all scenarios not otherwise stated (Hunter 1984). This residual event is a proxy for open-world thinking (Smets 1988) in a closed-world setting, and essentially accounts for all other events that can happen besides those that are explicitly articulated. Any probabilistic statement made in the absence of this residual event assumes a closed set, and is thus equivalent to a conditional probability given no residual event. The challenge for risk analysts is to construct a set of events that is general enough to be studied in a timely manner, yet is specific enough to support decision making with minimal potential for strategic surprise resulting from an unknown scenario (McGill and Ayyub 2008). As Aven (2008) suggests, the right balance must be struck between the need for precision and the need for decision support.

For example, consider the very specific scenario “a medium-sized car bomb attack occurring at the federal building in downtown at 9:00am on Thursday.” The details of this scenario permit a very good assessment of vulnerability to different degrees of loss given its occurrence, but to complete the overall risk picture requires the decision maker

to consider all event variations in time, date, location, delivery system, and threat type. A less specific version of this scenario such as “an explosive attack occurring in the region this year” is inclusive of all specific scenarios similar to the previous example, but as such it is difficult to make an assessment of aggregate vulnerability due to the wide variations, or uncertainty, in circumstances. Since vulnerability was defined to be a mapping from cause to consequence, it is thus important to construct scenarios that permit meaningful statements of vulnerability that can be used to inform risk management decisions.

2.2.3. The Nature of Consequence and its Assessment

According to mathematical logic, the consequent Y in a conditional statement of the form “if X then Y ” describes what is also true given that the premise X is true (Copi 1959). In the context of risk analysis, the premise X describes the initiating event and the consequent Y describes the outcomes given the occurrence of X . Since we are often uncertain as to what exactly Y will be given X , risk analysis considers all such statements “if X then Y ” for a given X and assigns a probability distribution over this set of such statements according to their likeliness of being the correct statement for a future context. The previous section (section 2.2.2) described the nature of the premises X ; this section describes the nature of the consequences Y of concern to homeland security decision makers.

Consequence in the homeland security context describes the undesirable outcomes following the occurrence of an initiating event. Since our present focus is on risk analysis for informing security decisions, the prime concern is negative or adverse

outcomes, that is, *pure risk* situations (Ayyub 2003) (this is in contrast to *speculative risk* where both positive and negative outcomes are considered). The focus on negative outcomes is appropriate for security analysis since from the decision maker's point of view, the primary concern with naturally occurring and anthropic events is whether his interests are protected against harm or loss (Purpura 2008). There is a wealth of research indicating positive externalities resulting from such harm or loss in the wake of a disaster (e.g., Skidmore and Toya 2002), or as the proverb goes, one man's loss is another man's gain (Oxford University Press 2004). However since risk analyses are tailored to meet the unique needs of a specific decision making body, these externalities are external to the scope of analysis and therefore are often not considered.

In general, one could identify an exhaustive or comprehensively nested set of undesirable outcomes following any initiating event (e.g., loss of containment, death of employees). These outcomes would initially assume the form of narratives, but could then map to a prescribed measure or representation of loss spanning one or more consequence dimensions (e.g., economic impact, property damage, loss of life, etc.). For example, the 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* articulates five dimensions of loss, to include impacts to public health and safety, the economy, public confidence, governance, and national security (White House 2003). Other methodologies prescribe different terms for consequence assessment, such as environmental damage (Moore et al. 2007) and aggregate regional and geographic impacts (US Department of Homeland Security 2006a). Some methodologies are less rigid in their specification for which consequence dimensions to consider; for example, the Center for Chemical Process Security

Vulnerability Assessment (SVA) methodology empowers SVA teams with the flexibility to define those dimensions that are relevant to each facility and decision maker (Center for Chemical Process Safety 2002).

The crispness of any consequence dimension is a property that characterizes how well it is understood and how well it can be assessed. A crisply defined consequence dimension possesses clear guidance on its assessment and can be extended to countable units of measure (e.g., dollars, time, lives, injuries). In contrast, a vaguely defined consequence dimension lacks clear units and often relies on subjective constructed scales for its assessment (Keeney 1981). For example, property damage, while qualitative in nature, is largely extendable to monetary measures despite the inherent ambiguities in the value of any given object or collection of objects. Loss of life and categories of injury are also largely extendable to countable units (e.g., number of people) at different subjectively assigned injury levels (e.g., the “abbreviated injury scale” or AIS described by Copes et al. 1969), and in some instances have been extended further to monetary measures via a statistical value of life for fatalities (Viscusi and Aldy 2003) or Quality Adjusted Life Years (QALYs) for injuries (Hammit 2002). In contrast, vaguely defined measures such as national security (Wolfer 1952) and public confidence (Baldwin et al. 2008) offer no clear definition for their measurement, though it should be noted that significant progress has been made in clarifying an interpretation of public confidence for practical use in national-level homeland security risk analysis.

The ultimate goal of consequence valuation is to provide a basis for assessing the severity of adverse outcomes valued in equivalent economic terms that can support meaningful benefit-cost analysis. The valuation or disutility of each consequence

dimension can be left in disaggregated form, or if desired by the decision maker, one could combine them to produce a single aggregate consequence metric using a multi-criteria decision analysis approach (Grabisch et al. 2007; Apostolakis and Lemon 2007). However, this approach begs for value judgments on how loss valued in one dimension (e.g., lives) equates to loss valued in another dimension (e.g., dollars), a task which extends beyond risk analysis into the realm of decision analysis (Pate-Cornell 2007). Consequence or loss conversion factors can be used for this purpose (Ayyub 2003). On the other hand, some risk studies may simply leave the results in terms of focused narratives, thus leaving it to the decision maker to assign a personal value to consequences and risk (Mairal 2008). Such an approach is common in the intelligence community where the reasoning and story is often more important than any expression of risk in qualitative or quantitative terms.

2.2.4. Screening of Initiating Events

Given a complete set of distinct initiating events, the determination of whether an event is a threat worthy of further analysis is typically done through the use of screening methods. A number of screening methodologies are available to help decision makers sort through typically expansive lists of risk scenarios to identify those for focused attention (National Infrastructure Institute 2006; Moore et al. 2007; among others). For example, McGill et al. (2007) outline a simple method for determining which initiating events are relevant to a decision maker according to the inherent susceptibilities of key elements to a variety of malicious anthropic events. According to this approach, initiating events are filtered in according to whether undesirable outcomes are achievable

when afflicting an asset. The list of relevant initiating event-asset pairings comprises an exhaustive set of threats for further consideration. The Risk Analysis and Management for Critical Asset Protection, or RAMCAP, methodology (Moore et al. 2007) also describes a screening process that focuses on the asset to determine whether its compromise warrants attention on the basis of perceived value to the decision maker and the nation. The CARVER methodology (US Department of the Army 1998; Vellani 2007) goes one step further by examining at a high-level the criticality, accessibility, recognizability, vulnerability, effects, and recuperability of an asset in light of a variety of attack modes to arrive at a relative rank ordering of initiating event-asset combinations on the basis of importance. Other more generic methods can be used for the purpose of screening and ranking, to include failure modes, effects, and criticality analysis or FMECA (Modarres et al. 1999) and hazard and operability analysis or HazOp (Haimes 2004). Hybrid models can also be used, such as one that merges concepts from both the CARVER and FMECA methodologies.

2.2.5. Risk and Surprise

A particularly menacing problem that exploits closed-world thinking is that of surprise. Surprise manifests itself in the unknown, unrecognized, and unrealized, and is a direct byproduct of a failure of imagination. According to Grabo (2002), surprise occurs when a defender is either unaware of potential hazards or unprepared to defend or respond to unexpected consequences from known, but ignored hazards. Each aspect of the security risk formula from Eq. 2-1 has elements that contribute to surprise, such as is shown in Figure 2-3 with a few examples (McGill and Ayyub 2008). The scenario may

be unexpected or the resulting consequences may be unanticipated (i.e., pure surprise), or the likelihood of its occurrence may be understated (i.e., as in a counterexpected event).

In general, surprise exploits defender ignorance, and may manifest by chance or the deliberate action of human adversaries. Figure 2-4 shows the various types of ignorance, all of which contribute to a defender's vulnerability to surprise (Ayyub 2001). Defeating surprise rests in a decision maker's awareness of possible scenarios and their outcomes, as well as in his preparedness to mitigate a full range of consequences following such events.

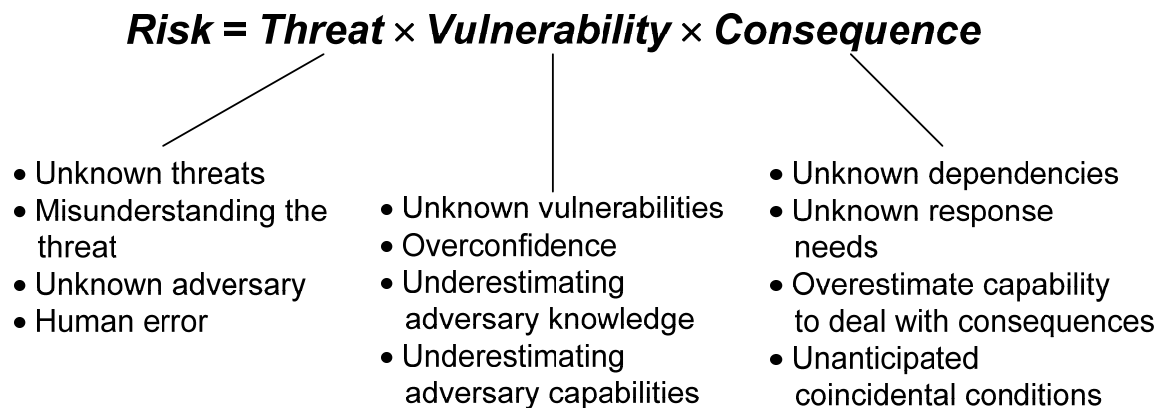


Figure 2-3. Some sources of surprise in risk analysis for critical infrastructure protection (McGill and Ayyub 2008b)

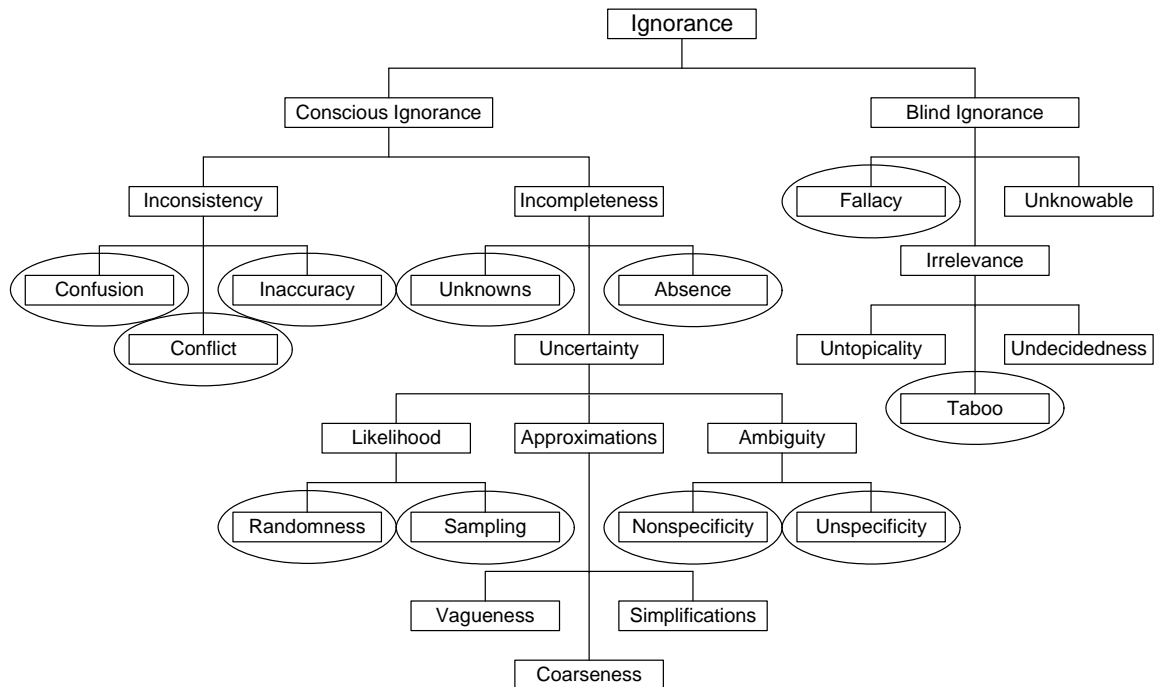


Figure 2-4. Hierarchy of ignorance types highlighting those types that contributes to overall vulnerability to surprise

A surprising event is one that is outside the realm of our expectations. Examples of surprise can be found in many areas related to homeland security. In the counterterrorism context, adversaries seek to leverage defender ignorance about their intent, capabilities, and operations to achieve an asymmetric advantage over their targets. For instance, the use of airplanes to attack the World Trade Center and Pentagon on 9/11 was arguably a surprise given that a majority of defenders were unaware that such vehicles would be used as projectiles to attack buildings (Kean et al. 2004). Other attack types discussed in the literature that are arguably potential sources of surprise for mainstream decision makers and security professionals include hemorrhagic fever (Borio et al. 2002), laser weapons (Bunker 2008), high-powered microwaves and intentional

electromagnetic interference attacks (Van Keuren et al. 1991; Parfenov et al. 2004), non-explosive radiological materials and particle accelerators (Acton et al. 2007; Chowdhury and Sarkar 2008), and forest fires (Baird 2006).

Manunta (1999a; 2002) highlights the propensity of adversaries to seek opportunities for achieving surprise, and argues that this behavior renders the security problem incompatible with the Bayesian analysis paradigm. In the international affairs arena, Cadell (2004) notes that potential adversaries engage in deception to deliberately mislead or confuse their opponents to prevent them from learning the deceiver's true intentions or activities. In this sense, deception thrives by manipulating uncertainty to affect a target, and surprise occurs when the actions of the deceived leads to them experiencing unintended and potentially undesired outcomes. For natural hazards, Woo (1999) asserts that "there are many arcane geological hazard phenomena which are beyond the testimony of the living, which would be met with incredulity and awe were they to recur in our own time. Such "black swans" are highly intense scenarios that are either unknown or have a perceived probability so low as to be considered negligible (e.g., counterexpected), yet would result in significant feeling of surprise were they to occur (Taleb 2007). In highly complex technical systems, Johnson (2006) suggests that surprise occurs due to unexpected emergent behaviors stemming from the interaction between system components and their environment. Critical infrastructure is among such highly complex technical systems, where unknown interdependencies between infrastructure services may lead to unpredictable cascading consequences (Rinaldi et al. 2001; see also Mendonca and Wallace 2006), some of which may cause the event to be labeled as extreme (Kunreuther 2002).

The primary source of surprise arises from an inappropriate or insufficient characterization of uncertainty, whether epistemic or ontological (Elms 2004). When a situation or decision problem is novel or unique, the challenge is to use the knowledge one has available to set bounds on the scope of imagined future outcomes (Chapman 2006); more knowledge reduces uncertainty, whereas lack of knowledge must entertain a wider range of possibilities. According to this point of view, all initiating events regarded as possible (e.g., non-zero probability) must at least be considered initially irrespective of the assessed magnitude of their likeliness. If the focus is on the outcomes of a scenario, the goal is then to mitigate or constrain the scope of possible consequences from a event-neutral point of view by structuring preparations and responses to cover a wide range of possibilities (Ackerman 2006).

2.2.6. Levels of Analysis

Risk assessment and management for critical infrastructure and key resource protection can be performed at a variety of levels (Ayyub et al. 2007). At the asset or facility level, a survey of an asset's mission critical elements coupled with knowledge of the consequences of disruption, physical and security vulnerabilities to a wide range of initiating events, and perceived attractiveness provides insight into actions an asset owner can take to reduce his overall risk exposure. An asset in this context is anything of value to its owner, such as a monument, vehicle, or facility. At the portfolio or system level, the total risk associated with a portfolio or system of assets (e.g., regional, national, sectoral) can be assessed in order to compare investment alternatives that aim to reduce overall portfolio risk. Figures 2-5 and 2-6 illustrate a portfolio of assets in a state and

nation, respectively. Figure 2-7 shows how single assets can belong to multiple different asset portfolios. A portfolio in this sense is a collection of assets with common attributes or linkages. Regional analysis, for example, would define a portfolio from the top-down by first identifying the critical functions and services of the region, and then assigning membership to regional assets that contribute directly to these mission areas. In contrast, a portfolio can be built from the bottom-up by first defining a set of assets, then examining how they relate with one another. In both cases, knowledge of the physical, geographic, cyber, and logical interdependencies among portfolio assets is important for assessing the potential for cascading consequences (Rinaldi et al. 2001).

To facilitate comparison of risk across sectors and aggregation of risk to higher levels of abstraction, risk analysis for critical asset protection at all levels should share a common analytical framework; this quality enables information collected at the asset-level to support decisions made at the portfolio-level and vice-versa. To date few methodologies claim to possess this characteristic, and this observed deficiency has in fact inspired attention toward standards for comparison and compatibility by professional security analysis societies (McGill and Pikus 2008).

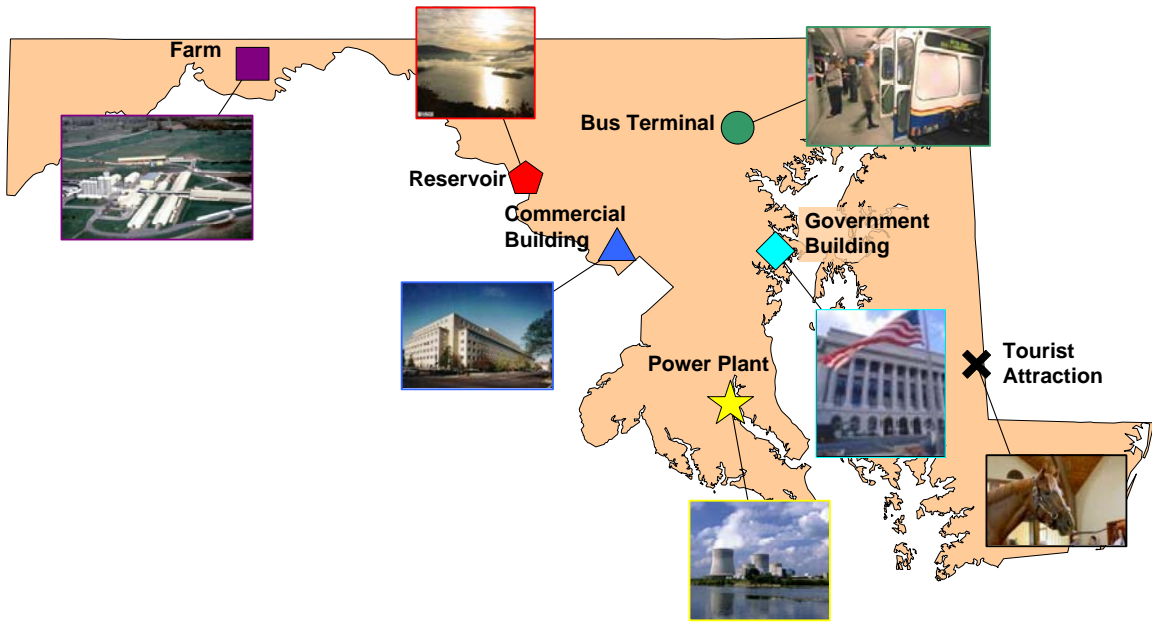


Figure 2-5. Notional portfolio of assets in a state (Ayyub et al. 2005)

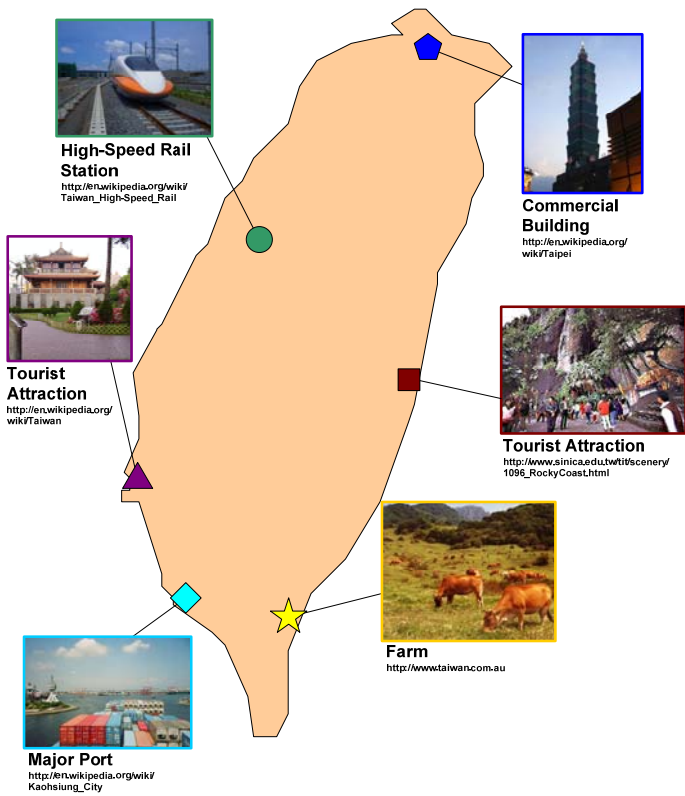


Figure 2-6. Notional portfolio of assets in a nation (Ayyub and McGill 2007)

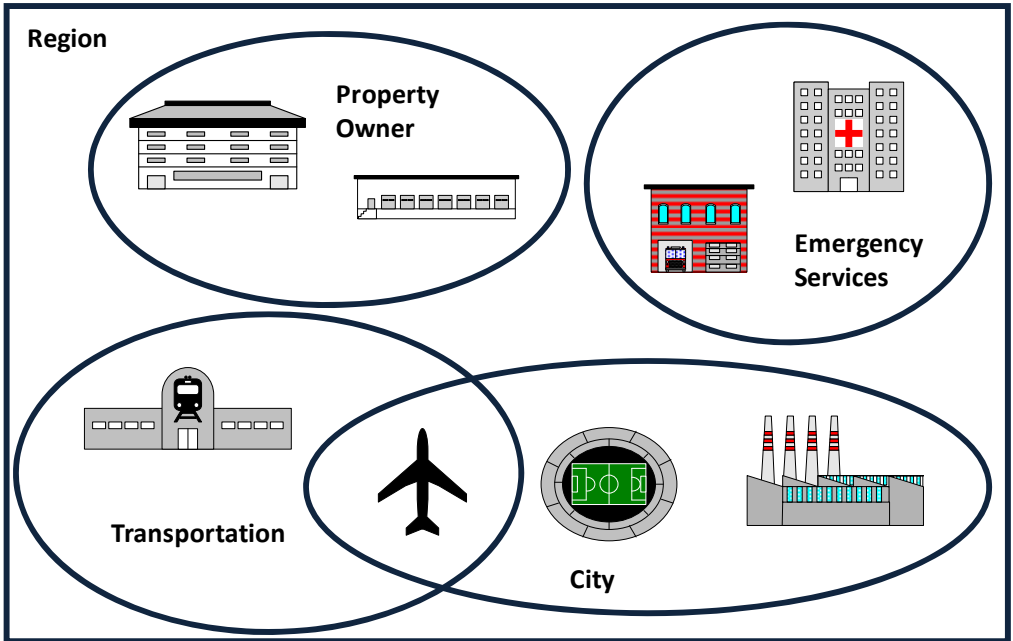


Figure 2-7. Various asset portfolios defined by locale, sector, etc.

2.3. Notions and Measures for Security Risk Analysis: Threat and Vulnerability

Given a pairing of cause e_i and consequence c_j , the risk R_{ij} can be expressed mathematically as the triplet of a initiating event, e_i ($i = 1, 2, \dots, m$), and the probability of this scenario, p_{ij} , and a particular consequence, c_j ($j = 1, 2, \dots, n$) as follows:

$$R_{ij} = \langle e_i, p_{ij}, c_j \rangle \tag{2-2}$$

The expression above defines the risk triplet (Kaplan and Garrick, 1981), where according to one interpretation (McGill and Ayyub 2007b) the initiating event describes the cause of loss, the consequence is a description or valuation on the final outcome resulting from this cause, and the probability measures the likeliness that initiating event

e_i will lead to the consequence c_j . The total risk, R , is the set of all ordered triples, i.e., $R = \{R_{ij}\}$. The probability term, p_{ij} , in Eq. 2-2 is the joint probability of e_i and c_j , or:

$$p_{ij} = \Pr(e_i, c_j) = \Pr(c_j | e_i) \Pr(e_i) \quad (2-3)$$

where the operator $\Pr(\cdot)$ denotes the probability of the event contained in the parentheses. Note that while the expression in Eq. 2-3 is represented in discrete form, c_j can represent the event that the loss exceeds some prescribed value C , and thus Eq. 2-3 offers an expression for exceedance probability given a continuous probability distribution on loss. Kept in discrete form, c_j can be a narrative of consequence, a consequence level from a finite set of bins, etc.

2.3.1. *The Nature of Vulnerability*

Vulnerability is the manifestation of the inherent states of a system, whether sociological, economic, technological, or a combination of these, that render it susceptible to harm or loss (Haimes 2006). Hollenstein (2005) characterizes vulnerability as the change in system states relative to a change in the intensity of the parameters of initiating events, that is, vulnerability considers the sensitivities of a system and its structures (Hollenstein 2002). This definition follows suit with vulnerability as the degree of loss attributable to a given element or set of elements at risk resulting from the occurrence of a hazard offered by Lamadrid (2002), which considers the characteristics of the system and its structures, way of life, demographic conditions and economic factors. McGill and Ayyub (2007b) proposed an operational definition for vulnerability

as the many-to-one mapping of initiating event to consequence, where the process of vulnerability analysis examines all the ways in which a system can induce harm or loss to society following the occurrence of an initiating event. According to their interpretation, a system is said to be vulnerable to a specified degree of loss following the occurrence of a specified event if there exists a potential for at least one array of system states to form a bridge from event to consequence.

According to Eq. 2-3, the term $\Pr(c_j | e_i)$ defines a probability distribution over C that accounts for all the variations in subsequent events that lead to similar consequences. In this view, $\Pr(c_j | e_i)$ gives the probability that an initiating event e_i will lead to a consequence c_j , or more generically, gives the probability that e_i will map to c_j . In light of the discussion on vulnerability as a mapping from cause to consequence in Section 2.1, it can be said that this probability is a measure of vulnerability with respect to consequence c_j due to an initiating event e_i , where $\Pr(c_j | e_i) = 1$ if e_i definitely leads to c_j (i.e., the decision maker is completely vulnerable), $\Pr(c_j | e_i) = 0$ if it is impossible for c_j to result from e_i (i.e., the decision maker is invulnerable), and $0 < \Pr(c_j | e_i) < 1$ according to degree of likeliness that e_i will lead to c_j in light of existing interventions. For example, in the case where there are no interventions to prevent or mitigate loss, such as a naked man standing in a remote open field during a lightning storm, vulnerability assessment is easy: given that an intense bolt of lightning aims for this man, there is nothing to stop it from striking, nothing on the man to minimize its effects, nor are there first responders nearby to treat the man once zapped. Thus, the man's probability of realizing the consequence $c_j =$ "immediate death" given that $e_i =$ "the man is struck by lightning" is high, perhaps around 0.9 (the residual probability of 0.1 is allocated toward

the complementary event “not immediate death,” which includes the consequences “delayed death” and “survival” with and without injury). Indeed, most practical situations encountered by homeland security practitioners are much more complicated than the “man in the field” scenario. Often, there are numerous interventions in place that seek to prevent a certain degree of loss following the occurrence of an initiating event, such as measures to harden critical assets against the damage-inducing effects of various threats, redundancies in the affected systems that isolate or limit cascading effects, response and recovery measures that seek to mitigate potential loss after an event, and measures to detect, respond to, and defeat adversaries in the case of malicious attacks.

Common representations of vulnerability include fragility curves, such as those used in engineering risk analysis for assessing the probability of different damage states as a function of hazard intensity. The insurance industry refers to fragility curves as vulnerability curves which characterize the mapping between hazard intensity and economic loss. Some risk methodologies interpret vulnerability in a general qualitative way using linguistic labels such as “Low,” “Medium” and “High” to characterize potential for realizing an undesirable end state, whether explicit (e.g., “adversary success”) or implied (e.g., net dissatisfaction). In general, any statement pertaining to the likelihood that some initiating event or cause will result in a particular undesirable consequence is a statement of vulnerability. In this light, the commonly encountered “probability of adversary success” is a quantitative statement of vulnerability, albeit narrow in the sense that the cause is an adversary attack and the consequence is adversary success where the undesirability of adversary success is implied but not valued. Similarly, a statement of

resilience, or “the ability to recover quickly from illness, change, or misfortune” in the narrow context of infrastructure (American Heritage Dictionary 2007), is also a statement about vulnerability, albeit in the positive sense. That is, resilience describes the likelihood that a system will return to a predefined functional state or better within a specified amount of time (consequence) given that it has been damaged or disrupted (cause). The equivalent statement of resilience in terms of vulnerability rephrases the consequence as the system not returning to a predefined state or better in an amount of time that exceeds some value.

The process of vulnerability assessment seeks out the various ways in which different states of a system align to render it susceptible to harm at either a micro (e.g., personal, asset) or macro (e.g., system, portfolio) level. Contributors to vulnerability include the ability of a security system to detect, engage, and defeat adversaries, the hardness of system elements, the importance of the elements to higher-level system functions, and the effectiveness of response and recovery capabilities (McGill and Ayyub 2007). A significant class of contributors to the vulnerability of an asset, region, sector or more generally a system to loss is the internal and external interdependencies among system elements (Rinaldi et al. 2001; Lee et al. 2007). While much attention has been afforded to “infrastructure interdependencies” in recent years (President’s Commission on Critical Infrastructure Protection 1997), dependencies that bear on system performance objectives of all sorts have been studied for decades using techniques such as event sequence diagrams (Swaminathan and Smidts 1999a; Swaminathan and Smidts 1999b), system block diagrams, and fault tree analysis (Modarres et al. 1999). Tools such as these, however, are typically used to study a system that is owned and operated

by a single decision making body. Yet, these smaller scale systems are, in actuality, subsystems or a larger interconnected network of systems that service society (e.g., a “meta-system” or “megastructure” per Amin 2002).

One cause for concern is the dependence between systems owned by one decision making body (e.g., asset owner) and systems owned by another with dissimilar interests (e.g., utility provider), both of which may service the same set of customers (e.g., the public, other asset owners). While system decomposition may be feasible at a small scale, it is much more difficult if not impossible to do in the context of a system of systems, particularly when some of these systems lack a deterministic logical structure (e.g., sociological systems, financial markets) that define how one system element relates to another, either directly or indirectly. To study such large scale systems, researchers typically infer system response and performance from statistical data describing past infrastructure performance, such as through the use of input-output matrices (Haines and Jiang 2002; Cheng et al. 2006). Recent work has attempted to study system interdependencies in a more analytic manner, such as through the use of linear programming models (Lee et al. 2007) or simple first-order interdependency matrices (Ayyub et al. 2007), the former being a rigorous approach for modeling physical interdependencies and the latter being a coarse but general approach for interdependencies of all types. Regardless of form, understanding how a system responds to events afflicting its elements is important for accurately describing the susceptibility of its elements and itself as a whole of to harm.

2.3.2. Probability of Occurrence for the Initiating Event

In contrast to naturally occurring, accidental or technological initiating events, security events are initiated by deliberate, innovative, and arguably unpredictable human adversaries that choose from among many possible targets and potentially innovative attack modes based on their perceptions of risk, reward, and opportunity (Hoffman 1998). Perpetrators of security events have an asymmetric advantage over a defender: whenever possible, potential adversaries will leverage the force multiplying effect of surprise to achieve success against defenders that are either unaware of the nature of the event or unprepared to defend themselves against unknown tactics (McGill and Ayyub 2008). Accordingly, the security threat landscape is constantly changing, and as such it is extremely difficult to forecast attacks since adversaries adapt by improving their tactics, enhancing their capabilities or developing new capabilities, and seek opportunities to catch their opponents off guard (Manunta 2002).

The probability of initiating event component of Eq. 2-1 is arguably the most uncertain aspect of the security risk problem. Actually, this argument holds for both naturally occurring and anthropic event, as the scientific community currently lacks reliable techniques to estimate the when and where the next event will occur for both categories (Woo 2002). Yet, unlike natural forces, adversaries have the freedom to choose an attack mode and target type that, when combined, come closest to meeting their goals (Fedra 2008). Consequently, recent events has prompted the security community to accept malicious attacks as a new species of trouble (Slovic 2002), which puts defenders in the frame of accepting malicious attacks as part of normal course of business (Resnyansky 2006). That is, the idea that a malicious attack will occur is often

taken as a given (e.g., the probability of attack is taken as one), and the emphasis is then placed on where attacks are likely to occur.

Assuming rational adversaries with specified goals, preferences, and attitudes (Hoffman 1998), several game theoretic analyses have shown that they shift their attention toward softer targets and less logistically complicated threat types in reaction to the security investments made by defenders (Sandler and Lapan 1998; Bier et al. 2005; Enders and Sandler 2005). Given a specified type of security event, one can assume that potential adversaries assign greater weight to assets with higher perceived utilities from the point of view of the defender with respect to their intentions and capabilities (Pate Cornell and Guikema 2002; Martz and Johnson 1987; Cox and Babayev 2003; Woo 2002). One must also consider the visibility of the asset and potential scenarios to the adversary; for example, it is reasonable to assume that an asset or plausible scenario with significant coverage in open-sources is more visible to potential adversaries than one with little or no coverage and that more visible assets are more likely to be chosen as targets for attack (Pluchinsky 2002; Department of Justice 2000). Security risk analysis must capture the changing preferences of an observant and creative adversary, and should recognize the fact that not all assets are necessarily visible to the adversary.

2.3.3. Previous Methodological Work

A number of qualitative, semi-quantitative, and quantitative approaches that touch on the threat and vulnerability aspects of Eq. 2-3 have been proposed in the last several decades. Martz and Johnson (1987) developed a model that focuses on theft of nuclear munitions by armed aggressors, and employs logical event tree modeling to assess the

probability of adversary success, a subcomponent of based on the effectiveness of available countermeasures to protect these assets. Dessent (1987) developed a similar model for prison security system design that focused on preventing prisoner escape. Both of these models consider the vulnerability portion of Eq. 2-1 (and Eq. 2-3) as a security problem, and divide it into measurable parameters such as probability of detection, adversary delay and defender response time; however, since the consequences of security system failure are implied for these problems (e.g., theft of nuclear materials, prisoner escape), neither model captures the non-security contributors to vulnerability, such as emergency response measures or lack thereof. The Center for Chemical Process Safety Security Vulnerability Assessment (SVA) methodology (Center for Chemical Process Safety 2002) is similar in this regard, but applies the so-called “security event” principle for assessing conservative (i.e., worst case) consequences given adversary success. The Common Risk Model developed by Morgeson et al. (2006) also does this in their definition of consequence as the “worst reasonable case” valuation for loss. In essence, these two methodologies assume a worst-case vulnerability condition following adversary success.

Pate-Cornell and Guikema (2002) proposed an overarching model for assessing terrorism risks where threat is taken as product of relative scenario attractiveness and probability of intent, vulnerability is taken as the probability of adversary success, and consequences are described by expected disutility associated with a threat scenario from the U.S. perspective. According to this model, the attractiveness of a scenario might decrease in response to security investments, thus giving rise to an increase in the relative attractiveness of alternative scenarios. This model seems to capture the behavior of

rational adversaries; however, since relative attractiveness is assessed with respect to a strict set of scenarios derived from threat intelligence (i.e., as in a threat-driven approach), the model may not capture plausible scenarios for which no supporting intelligence is available. Lack of awareness of plausible threat scenarios renders a decision maker susceptible to surprise, and thus contributes to overall vulnerability. Moreover, the utility of this threat model is predicated on accurate insight into adversary perceptions and motivations, which is often difficult to assess in general since all potential adversaries surely differ in their intent and capabilities. However, the general approach is in agreement with suggestions made by other leading researchers in the field (Cox and Babayev 2003; Woo 2002).

A number of other researchers, companies, non-profit organizations, and government entities have developed their own methodologies for assessing threat, vulnerability, consequence, and risk in the security context. These include a variety of qualitative and semi-quantitative vulnerability and risk assessment methodologies (Livermore 2002; American Chemistry Council 2002; American Petroleum Institute 2003; American Society for Industrial Security 2003; Association of Metropolitan Sewerage Agencies 2002; Barnett et al. 2005; US Federal Highway Administration 2003; Cepan et al. 2006; Chapman and Leng 2004; Chen et al. 2002; Chen et al. 2005; US Department of Homeland Security 2006a; Einarsson and Raussand 1990; US Federal Emergency Management Agency 2003; ExxonMobil 2002; Hart 2002; Gutting 2008; Herabat 2003; Karimi et al. 2005; Kemp 2007; Leone and Liu 2006; Masse et al., 2007; National Rural Water Association 2002; Ren 1999; Science Applications International Corporation 2002; Taylor 2002; Veatch et al. 2002; Flax et al. 2001; Moore 2006; Leung

et al. 2004; Wang and Liu 2006; Wu and Zhang 2005; Zhang et al. 2003; Zhang et al. 2004; Zhao et al. 2006), as well a quantitative methods based on an additive model (Ray 2007), geometric model (Kowalski 2002), multi-attribute utility theory (Apostolakis and Lemon 2005), project risk management (Rosoff and von Winterfeldt 2007), simple probability theory (Kaplan 2002; Matalucci 2002; Moore et al. 2007; Zhang et al. 2006), structural reliability analysis (Mahoney 2007; Stewart and Netherton 2007), simulation (Arboleda 2007), Markov models (Doyon 1981), evidence theory, possibility theory and fuzzy sets (Darby 2006; Eisenhower et al. 2003; Karimi 2006; Karimi et al. 2007), and so on. Notwithstanding the differences in opinion as whether and how numbers are assigned to the threat, vulnerability, and consequence components of their respective models (see Manunta 1999; Harris 2004), all of these methods in general share a philosophical basis for security risk analysis that is consistent with pre-2001 thinking (see US Department of the Army 1994; Ezell et al. 2000). However, what most of these models do not share is a common framework that promotes consistency across assets and aggregation to support decisions at higher levels of abstraction and leadership (as noted by National Research Council 2002), nor do most quantify risk in such a way that accommodates all sources of uncertainty and facilitates meaningful benefit-cost analysis. Thus, in order to quantify risk in a meaningful way as required by Homeland Security Presidential Directive Number 7 (Bush 2003) and to support defensible benefit-cost analysis for critical asset protection (US Department of Homeland Security 2006b), a general quantitative risk analysis framework that accommodates varying degrees of resolution, levels of abstraction and leadership, and produces meaningful measures of risks is required.

2.4. Actionable Risk Information

From the point of view of a homeland security decision maker, guidance on where to focus attention on reducing risk is at least as important as the risk results alone. For example, conveying insight into which risk contributors (variables) should be targeted for risk reduction is as important as the magnitude of risk. Borrowing on the concept of actionable intelligence (Kipfer 2005), *actionable risk assessments* produce actionable information that has practical and relevant use to the decision maker for the purposes of identifying viable options for risk reduction (Ayyub et al. 2007).

To provide actionable risk information means to provide both a measure of risk and suggestions on what to do about it, which essentially addresses the fourth question defining risk analysis in section 2.1. Making risk information “actionable” amounts to performing a sensitivity analysis as described in many books on probabilistic risk analysis for nuclear power plants (see Kumamoto and Henley 2000). Combined with the risk profiles determined for each initiating event, sensitivity and importance measures provide insight into which risk contributors should be targeted for cost-effective risk reduction, and thus communicate actionable risk information.

2.5. Risk Management: Countermeasures and Mitigation

The process of risk management begins immediately when a decision maker receives the results of a risk assessment. Given a baseline risk exposure as determined via risk assessment, there are four broad risk management options available to the decision maker: *accept* the risk either temporarily or permanently (tolerate the risk),

transfer the risk to someone else (e.g., insurance, such as described by Kunreuther 2002), *avoid* the risk (e.g., change design, do something different), or *manage* the risk through countermeasures and mitigation (Ayyub 2003). For risk management, Masse et al. (2007) citing a recent RAND study posed the following question for consideration by decision makers: “should resources be allocated based on risk, risk reduction, or something else?” In accordance with the fifth question of risk (section 2.1), the Department of Homeland Security’s response to this latter question advises decision makers to accept benefit-cost analysis as the prime determinant in homeland security decision making (US Department of Homeland Security 2006b). According to one interpretation, the benefit should be measured in terms of risk reduction and the costs measured in terms of life-cycle cost to implement and sustain the action in addition to the constraints the action places on future decisions (Ayyub 2003; Haimes 1991). McGill et al. (2007) also suggests that risk management decisions should also consider whether each alternative is affordable and whether it meets risk reduction objectives. Sandman (1989), however, cautions that any proposed objective risk reduction must also be mindful of stakeholder perceptions as these perceptions, however incorrect they are, are the dominant factor in risk reduction investments. Consequently, some decisions may limit the ability of a decision maker to act in the future (per the six question of risk in Section 2.1).

Options available to homeland security decision makers consist of any purchase, action, program, etc. that yields a favorable improvement in the parameters of Eq. 2-3. In the process of identifying options for risk reduction, the decision maker should consider ways to decrease the probability of occurrence of high risk events and decrease the

vulnerability of their system to highly unfavorable consequences by improving site security and reducing potential consequence. Bashor (1998) highlights that preparedness for terrorism and other threatening events should span three domains: prevention, preparedness, and response. Hammond (2005) echoes this sentiment in his suggestion that hospitals must improve their level of preparedness to respond to mass casualty and disaster incidents. DHS adhered to this guidance by offering disaster preparedness planners a framework for establishing protection priorities for regional planners in terms of a target capabilities list, or TCL (US Department of Homeland Security 2006c). The TCL provides a list of 37 capabilities spanning five broad categories – common, prevention, protection, recovery, and response – as shown in Figure 2-8 – with recommended target performance levels that provides a basis for assessment of current capabilities and a means for determining where improvement is needed. Other risk mitigation options includes physical security systems that lessen the chances of adversary success (Garcia 2006), deterrence measures aimed at dampening adversary attractiveness (Fuqua and Wilson 1977), measures to decrease the fragility of structures and systems (for example, see Newland and Cebon 2002), etc.

Target Capabilities List	
Common	Respond Mission Area
<ul style="list-style-type: none"> ● Planning ● Communications ● Risk Management ● Community Preparedness and Participation 	<ul style="list-style-type: none"> ● Onsite Incident Management ● Emergency Operations Center Management ● Critical Resource Logistics and Distribution ● Volunteer Management and Donations ● Responder Safety and Health ● Public Safety and Security Response ● Animal Health Emergency Support ● Environmental Health ● Explosive Device Response Operations ● Firefighting Operations/Support ● WMD/HazMat Response and Decontamination ● Citizen Protection: Evacuation and/or In-Place Protection ● Isolation and Quarantine ● Urban Search & Rescue ● Emergency Public Information and Warning ● Triage and Pre-Hospital Treatment ● Medical Surge ● Medical Supplies Management and Distribution ● Mass Prophylaxis ● Mass Care (Sheltering, Feeding, and Related Services) ● Fatality Management
Prevent Mission Area	
<ul style="list-style-type: none"> ● Information Gathering & Recognition of Indicators & Warnings ● Intelligence Analysis and Production ● Intelligence / Information Sharing and Dissemination ● Law Enforcement Investigation and Operations ● CBRNE Detection 	
Protect Mission Area	
<ul style="list-style-type: none"> ● Critical Infrastructure Protection (CIP) ● Food & Agriculture Safety & Defense ● Epidemiological Surveillance and Investigation ● Public Health Laboratory Testing 	
Recover Mission Area	
<ul style="list-style-type: none"> ● Structural Damage and Mitigation ● Assessment Restoration of Lifelines ● Economic & Community Recovery 	

Figure 2-8. DHS target capabilities list (US Department of Homeland Security 2006c)

Chapter 3. Methodology

3.1. Risk Analysis Framework

In the context of this research, risk is defined as the potential for harm or loss as perceived by the decision maker (Ayyub 2003). The following sections develop an event-tree or logically-driven security risk analysis framework for critical asset protection called *Critical Asset and Portfolio Risk Analysis* or CAPRA based on the view that $e_i \in E$ defines a set of initiating security events at a specified location where the probability $\Pr(e_i)$ is the probability that the initiating event will occur at this location in a specified time period, and $c_j \in C$ defines a set of consequences (finite or continuous) that could result from these initiating events where the vulnerability term $\Pr(c_j | e_i)$ gives the probability that consequence c_j follows from e_i . This framework consists of six phases as shown in Figure 3-1, namely *Scenario Identification*, *Consequence and Severity Assessment*, *Overall Vulnerability Assessment*, *Threat Probability Assessment*, *Actionable Risk Assessment*, and *Benefit-Cost Analysis*.

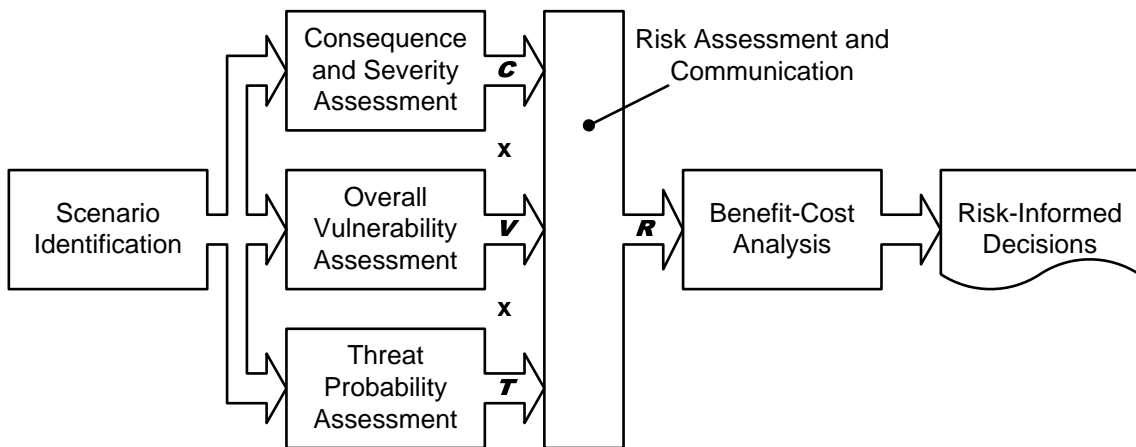


Figure 3-1. Framework for asset- and portfolio-level risk analysis

As required for any meaningful risk analysis (Elms 1992), the stated objective of the CAPRA methodology is to support operational and strategic resource allocation decisions at the asset or portfolio levels by providing meaningful measures of overall risk that lend themselves to a judgment of acceptability and, if necessary, quantitative benefit-cost analysis. Results from the first four phases produce information that combines in the fifth to make actionable statements about risk. The sixth phase provides tools for evaluating alternative strategies for managing risk if the assessed risk was determined to be unacceptable, unavoidable, and non-transferable.

Throughout the subsequent sections, values for all parameters of the CAPRA model, in principle, can be obtained via a combination of data analysis, systems modeling, expert elicitation, and evidential reasoning (Ayyub 2001; Cooke and Goosens 2004). The proposed framework adopts the view of information as a generalized constraint (Zadeh 2005), where such information is used to reduce the uncertainty on what values a model parameter can take. In the event of missing information, this methodology errs on the side of caution by assuming a default worst-case value (e.g., the probability of attack is one) unless less-conservative values can be justified on the basis of available information and judgment. Depending on the information available to support analysis, model parameters may be specified in terms of point estimates, moments, intervals, probability distributions, imprecise probabilities (Walley 1988), or hybrid numbers, and may be provided by various compatible models. The case studies in Chapters 4 and 5 demonstrate how the CAPRA framework can leverage information represented in various forms and from a variety of different compatible models to perform an asset-level assessment (Chapter 4, a traditional probabilistic analysis) and

portfolio-level assessment of regional assets (Chapter 5, with approximate reasoning and random sets) that expresses risk in a form that remains faithful to the real uncertainties present in the supporting information.

To accommodate the fact that many practical situations suffer from constraints (e.g., time, fiscal) on available resources for analysis, results may be screened to determine which threat scenarios warrant further analytical treatment. In lieu of a complete analysis in each stage, conservative values are employed by default to facilitate rapid completion of the analysis process. That is, by default the CAPRA approach assumes the worst-case values for each parameter. These conservatisms can be revisited later if they are determined to have a significant effect on the final results.

3.2. Scenario Identification

The scenario identification phase constructs an exhaustive set of plausible initiating events afflicting an asset or system based on the inherent susceptibilities of its constituent elements to the damaged-inducing mechanisms associated with a wide range of naturally occurring and anthropic events. The scenario identification process begins with a complete characterization of an asset or system, including its mission and key elements. Nominal performance of an asset or system can be described by a success scenario (Kaplan et al. 1999). Key elements are those whose compromise would disrupt the nominal performance of an asset or system, and can be identified from fault trees, reliability block diagrams, or other systems modeling techniques (Modarres et al. 1999). Once identified, each key element is classified according to its fundamental characteristics and functionality to facilitate mapping to relevant event types using a

target susceptibility diagram such as is shown in Figure 3-2 or a target susceptibility matrix such as the one shown in Table 3-1. An exhaustive partitioning of the event space into *initiating events* is generated using this procedure, where each event defines a unique combination of key element and threat type. Alternatively, one could define an initiating event as the combination of threat type and occurrence location, and only those events occurring in proximity to key elements would be in the set of relevant risk scenarios. These scenarios can be qualitatively screened-in based on the potential effects and their severity following an attack using such tools as a modified failure modes, effects and criticality analysis (FMECA) procedure to determine which scenarios warrant further consideration. An expanded target susceptibility and risk scenario screening matrix based on elements of the FMECA (Modarres et al. 1999) and CARVER (National Infrastructure Institute 2006; US Department of the Army 1998; US Food and Drug Administration 2007) methods is shown in Table 3-2.

Table 3-1. Target susceptibility matrix for a notional asset

Event Type	Key Element				
	HAZMAT Storage	Building	Pipeline	Rail Car	Computer Network
Explosive	X	X	X	X	X
Projectile / Impact	X	X	X	X	-
Incendiary	X	X	-	-	X
Chemical	-	-	-	-	-
Biological	-	-	-	-	-
Radiological	-	-	-	-	X
Laser	-	-	-	-	-
Radiofrequency	-	-	-	-	X
Cyber	-	-	-	-	X
Sabotage	X	-	X	X	X

Table 3-2. Expanded target susceptibility and risk screening matrix based on a hybrid FMECA/CARVER method with notional entries

Key Element	Recognizability	Accessibility	Failure Mode	Vulnerability / Shock													Outcomes of Failure	Severity					
				Explosive	Projectile	Incendiary	Chemical	Biological	Radiological	Nuclear	Radiofrequency	Sabotage	Theft	Cyber	Laser	Panic		Criticality		Effect	Recoverability	Risk Score	Relative Risk Priority Number
																		⚡	⚡				
HAZMAT Storage	10	10	Failure to contain hazardous materials	9/4	8/4	2/2	--	--	--	--	--	6/3	--	--	--	--	Release of hazardous materials followed by exposure of employees to lethal chemicals; damage to storage tank; disruption of mission	6	2	5	4	6.7	45
Building	10	10	Failure of building to house internal functions	8/3	3/1	7/2	--	--	--	--	--	--	--	--	--	--	Loss of building structure; injury or death of occupants	4	2	5	1	4.7	(2)
Pipeline	7	4	Failure to transit products from storage tank to rail cars	6/3	4/1	--	--	--	--	--	--	8/2	--	--	--	--	Loss of ability to transit materials from tank to rail car; environmental contamination	2	4	5	8	4.3	(5)
Rail Car	10	10	Failure to provide means for shipping chemicals to customers	4/3	5/1	--	--	--	--	--	--	7/5	--	--	--	--	Temporary loss of ability to ship materials to customers; environmental contamination	5	1	4	1	5.6	5
Computer Network	5	6	Failure to provide electronic means of communication	9/3	--	9/2	--	--	2/5	--	6/5	10/2	--	4/1	--	--	Lost ability to communicate between computers, store and recover data, communicate to the Internet	2	4	3	1	4.5	(3)
Criticality: Measure of public health and economic impacts of an attack				Accessibility: Ability to physically access and egress from target				Effect: Amount of direct loss from an attack as measured by loss in production															
Recognizability: Ease of identifying target				Vulnerability: Ease of accomplishing attack				Recoverability: Ability to recover from an attack				Shock: Shock value of the attack											

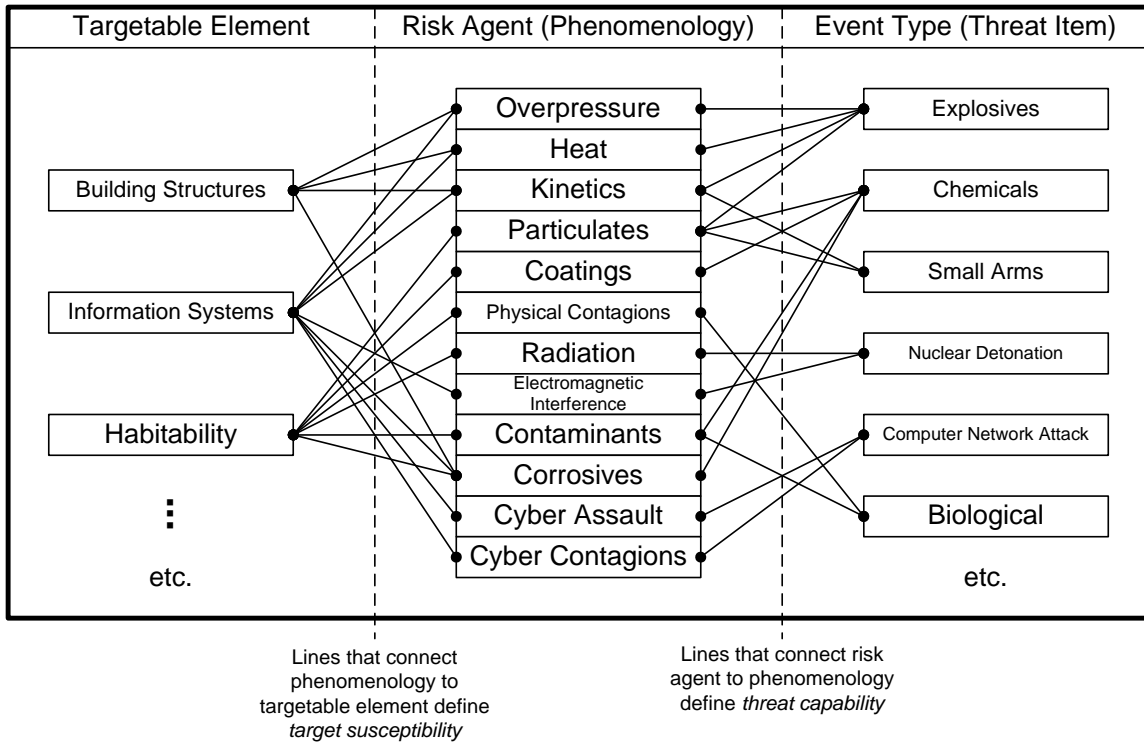


Figure 3-2. Mapping from event type (threat item) to targetable element via risk agents (phenomenologies)

3.3. Consequence and Severity Assessment

The consequence and severity assessment phase estimates the maximum potential loss for each consequence dimension of concern to the supported decision maker. That is, this phase bounds the scope of imagined outcomes for all dimensions of loss that are applicable in the current decision making context, whether crisp (e.g., fatalities, dollars) or vague (e.g., psychological, public confidence). The maximum potential loss is the worst case loss that would result in the worst possible circumstances (Ayyub 2003). Four “crisp” or “natural” dimensions of loss are initially considered as described in Table 3-3. These loss dimensions are crisp in the sense that their units of measure are natural and can be, in principle, expressed in consistent units such as dollars through the use of

appropriate loss conversion factors (Ayyub 2003; Viscusi and Aldy 2003). Meaningful measures for “softer” loss dimensions such as public confidence, governance and national security (White House 2003) remain elusive and are therefore not currently considered in this analysis.

Table 3-3. Crisp loss dimensions and associated units of measure

Loss Dimension	Description	Unit of Measure
Casualty	Measures the number of people injured or killed	Number of fatality equivalents (Ayyub 2003)
Economic	Measures direct economic damage including property loss, repair and cleanup costs, and environmental losses	Current Year Dollars
Mission Disruption*	Measures degree of mission disruption for each relevant mission	Percentage Reduction in Available Production Capacity
Recuperation Time*	Measures the time to reconstitute lost functionality and production capacity	Time (Days or Years as appropriate)

* Aggregate disruption is the product of mission disruption and recuperation time, and is expressed in units of %-time

3.4. Overall Vulnerability Assessment

As described in Chapter 2, Section 2.3, the overall vulnerability of an individual decision maker to a given consequence c_j due to the occurrence of an initiating event e_i can be viewed as the probability that e_i leads to c_j , or $\Pr(c_j | e_i)$. Given the occurrence of an initiating event, the assessment of overall vulnerability requires a thorough consideration of all intermediate interventions, whether active, passive, deliberate, or unintentional, between cause and consequence. The event tree shown in Figure 3-3 illustrates a high-level logical sequence of interventions that seek to limit loss following an initiating event. That is, loss following the occurrence of an initiating event requires that:

1. The attack defeats all security measures
2. The attacker successfully imparts a load on the target
3. The target suffers damage from this load
4. The system responds to this damage
5. Response and recovery fail to prevent this degree of loss

A quick observation of this event tree suggests that the vulnerability to a given degree of loss with respect to an initiating event requires all intermediate interventions between cause and consequence to fail. In other words, only one intervention needs to work (albeit perfectly) to prevent loss. In this context, the interventions behave in a manner consistent with a parallel systems reliability model (Modarres 1992), where total success of just one intervention prevents the specified degree of loss.

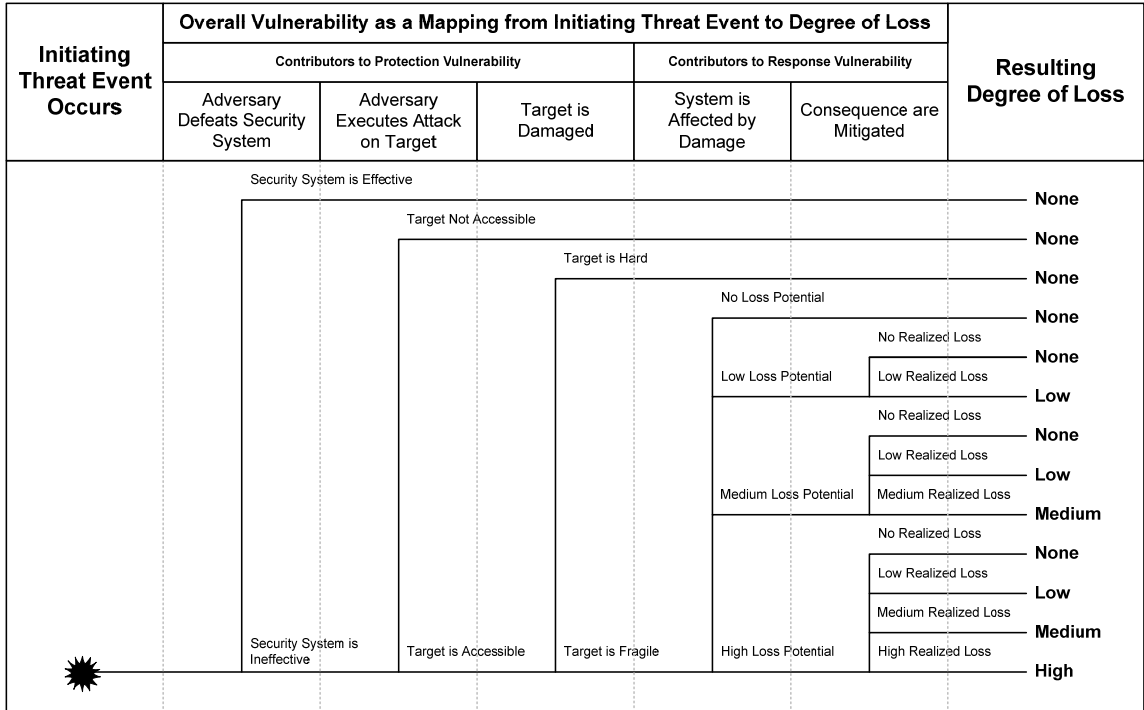


Figure 3-3. Logical sequence of interventions between initiating event (cause) to resulting degree of loss (consequence)

Upon observation of Figure 3-3, one can divide the scope of overall vulnerability into two categories: *protection vulnerabilities* and *response vulnerabilities*. This division is similar to the categorical make-up of the DHS Target Capabilities List (Department of Homeland Security 2006d) for dealing with the effects of an initiating event, where the protect mission area describes capabilities for decreasing protection vulnerabilities and the response and recovery mission areas describe capabilities for decreasing response vulnerabilities. Protection vulnerabilities include all weaknesses between the initiation of a security event and physical damage of the targets. Interventions in this category include countermeasures aimed at decreasing the probability of adversary success, denying access to critical targets, and measures to improve hardiness (or lessen the fragility) of

potential targets with respect to the damage-inducing mechanisms of the threat type. Response vulnerabilities include all deficiencies in responding to damage following exposure and damage which can be mitigated through such interventions as emergency response capabilities to treat injured survivors and measures to quickly reconstitute lifeline services following disruption. The following sections describe contributors to the overall vulnerability from each of these two categories and develop a mathematical expression for overall vulnerability that facilitates its quantitative expression.

3.4.1. Protection Vulnerability

Protection vulnerability describes the probability distribution over a range of possible damage states following the occurrence of an initiating event considering the fragility of critical elements, target accessibility, and security system weaknesses (McGill and Ayyub 2007b). This category of vulnerability considers all contributors to overall vulnerability between the initiating event and damage of targets. That is, given the occurrence of an initiating event, protection vulnerability measures the probability of suffering a specified level of damage, whether in terms of damage or compromise of afflicted elements or size of an exposed human population. If damage cannot be reliably prevented following an initiating event, then a target is vulnerable to any degree of loss unless the system compensates with suitable strategies to control the ensuing losses. According to the event tree in Figure 3-3, a simple mathematical expression for protection vulnerability, $V_p(e_i, d_k)$, to a specified level of damage, $d_k \in D$, where D is a set of damage states, can be obtained as follows:

$$V_p(e_i, d_k) = \Pr(S | e_i) \Pr(K | S, e_i) \Pr(d_k | K, S, e_i) \quad (3-1)$$

where $\Pr(S | e_i)$ is the probability of adversary success for initiating event e_i , $\Pr(K | S, e_i)$ is the probability that the adversary will successfully impart his load on the target given adversary success (i.e., accessibility), and $\Pr(d_k | K, S, e_i)$ is the probability that the target will then suffer damage d_k given adversary success and successful imparting of its load. According to this equation, an adversary must defeat a defender's security measures, successfully execute the damage-inducing mechanisms of the attack, and then damage or compromise the target at a specified level d_k to achieve success. Equation 3-1 assumes that failure of the attacker to overcome the security system *OR* failure of the attacker to successfully execute his attack given the opportunity *OR* failure of the attack to cause damage d_k will result in no loss. Expressed in terms of favorable defender characteristics where higher values for the descriptive parameters are desired, Eq. 3-1 can be rewritten as:

$$V_p(e_i, d_k) = (1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, d_k)) \quad (3-2)$$

where $I_S(e_i) = 1 - \Pr(S | e_i)$ is the effectiveness of security system interventions with respect to the initiating event e_i , $I_K(e_i) = 1 - \Pr(K | S, e_i)$ is the effectiveness of denial interventions (intrinsic and extrinsic) that seek to deny execution of the attack against the specified target according to e_i , and $I_H(e_i, d_k) = 1 - \Pr(d_k | K, S, e_i)$ measures the effectiveness of hardiness interventions (intrinsic and extrinsic) of the target to damage state d_k given exposure to the damage inducing mechanisms associated with e_i .

Based on Eqs. 3-1 and 3-2, the three primary dimensions of protection vulnerability are *security system weaknesses*, *target accessibility*, and *fragility of target elements*. In the case of no security, complete target accessibility, and fragile targets, $I_S = I_K = I_H = 0$ and $V_P = 1$. In contrast, the presence of just one perfect intervention (e.g., $I_S = 1$) results in $V_P = 0$. A discussion of each dimension of protection vulnerability is provided in the following sections.

3.4.1.1. Security System Weaknesses

In order to minimize the probability of adversary success given an attempt, the defender force must possess capabilities to effectively *detect*, *engage*, and *neutralize* determined adversaries considering a full spectrum of possible threat types and attack profiles. Security system effectiveness is based on the weakest link model – failure to detect, engage, or defeat a potential adversary amount to adversary success at overcoming security (Hicks et al. 1987), such as would be the case in the absence of effective security countermeasures. Furthermore, as with most technological systems, the reliability of a security system, in general, is a function of hardware, software, and human elements, all of which are intertwined in complex ways. Security is thus a complex function of characteristics associated with the asset, defender, adversary, and the situation at hand (Manunta 1999b).

The assessment of security system effectiveness begins by identifying a complete set of plausible *intrusion paths* leading to each key asset element. Intrusion paths begin at the outside perimeter of a facility since it is the first line that must be crossed by an intruder to gain access to a protected element (Fischer and Green 2004). Each intrusion

path consists of a sequence of discrete *security zones*; a security zone is defined as a discrete region within the asset perimeter containing a distinct set of countermeasures and features. Security zones are generally separated by static detection measures. The *cross-section* of an intrusion path shows the sequence of security zones connecting the asset perimeter to the target element, such as is shown in Figure 3-4 (Dessent 1987). For a given threat type, compatible attack modes (e.g., ground vehicles for explosive threats) are identified for each intrusion path. The combination of attack mode and intrusion path defines an *attack profile*. The set of attack profiles partitions a given threat type into an exhaustive set of non-overlapping combinations of attack mode and intrusion path. Identification of the attack profiles can be achieved via an *attack profile compatibility matrix* such as that shown in Table 3-4.

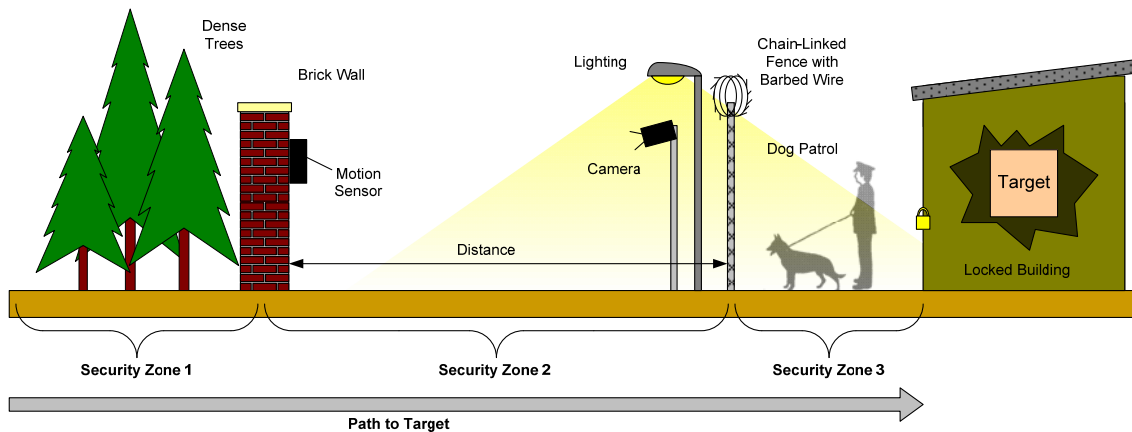


Figure 3-4. Cross-section of an intrusion path

Table 3-4. Attack profile compatibility matrix for an initiating event

Attack Mode	Intrusion Path				
	Via Back Road	Via Main Access Road	Via Forest	Via Water	Via Air
On Person	X	X	X	X	-
Ground Vehicle	X	X	-	-	-
Waterborne Vehicle	-	-	-	X	-
Aerial Vehicle	-	-	-	-	X

Detection requires capabilities to *sense* the environment, *recognize* whether an attack is taking place, and *annunciate* these observations to a responder (e.g., watch guard) for action. For example, a security system comprised of a closed-circuit television system (CCTV) system equipped with intrusion detection software, trained watch personnel, and effective alert policies possesses all the required elements of an effective detection capability. Similarly, a team of guards standing visual watch over a well lit, security-friendly environment (Crowe 1991) also possesses the ability to sense, assess, and annunciate, even if not supported by modern security technology.

Detection measures come in two types – static (demand-based) measures and active (time-dependent) measures. The performance of a static detection measure is specified as a *probability of detection* that is a function of attack mode and adversary capability. For example, the probability of detection for a trip wire depends on device placement, adversary awareness of this device, and ability of the adversary to overcome this measure, whether deliberately or by accident. In contrast, a key measure of effectiveness of active detection measures is the *mean time to detect* a given type of adversary and attack mode; the value of this parameter is affected by the choice of detection elements and degree of implementation, to include policies, procedures,

personnel training, and predictability. For example, the probability of detection for a naïve loiterer trespassing in a restricted area subject to random patrols of watch personnel increases for larger exposure times.

Engagement requires that the security system *delay* determined adversaries long enough for defenders to *respond to* and *engage* the adversary. Delay measures include the distance between the boundary of the protected perimeter of an asset and the target element, as well as any physical barriers along the way such as gates, fences, moats and bollards. A key measure of effectiveness for delay measures is *time to defeat*, which can be conservatively specified as a minimum value, characterized by the mean and coefficient of variation of a probability distribution, etc. For example, the effectiveness of security doors are specified in units of time to defeat under a set of standardized conditions (e.g., a 2-minute door). Measures to respond include suitable numbers and proper placement of guard forces or other response vehicles so as to minimize the *defender response time*. Engagement is achieved if the defender response time is less than the time remaining for the adversary to execute an attack once detected.

Neutralization requires that defenders possess the ability to defeat determined adversaries once engaged. When viewed from a stress-strength point of view (Kotz 2003), neutralization occurs when the “strength” of the defender force exceeds the “stress” imposed on it by the adversaries. The strength of a defender force largely depends on the capabilities of security guards, which considers the size of the security force, available weapons, quality of training, and complex social and organizational factors such as morale, team coherence, etc. (see Apostolakis 2004; Bunn 2004; Carroll 2004; Sagan 2004; Westrum, 2004). In principle, human reliability analysis (HRA)

techniques can be used to estimate the probability of neutralization, such as by establishing a baseline probability of neutralization that is then modified according to the states of various *adversary performance influencing factors* or *performance shaping factors* such as skill, number of adversaries, and determination (see Smidts et al. 1997; Chang and Mosleh 2007).

3.4.1.2. Target Accessibility

Given failure of the security system to successfully prevent the execution of an attack, adversary success still requires that the attacker successfully *accesses* and successfully *imparts its load* on the target. In many cases, access is assured given the opportunity to do so, thus leaving to chance whether the attack will go off as intended (e.g., a “dud” explosive). However, in some cases such as a physically enforced standoff attack, target access depends on the size of the target with respect to standoff distance. From a given distance, a small target is more difficult to hit than larger target. A cyber analog is access to an air-gapped SCADA system via the Internet: in this situation, access is *denied* since the chosen intrusion path cannot lead to the desired target.

3.4.1.3. Target Fragility

The *fragility* or *hardness* is a physical property of target elements that describes the degree of damage resulting from exposure to a hazard of specified intensity (Woo 1999; Filliben et al. 2003). The performance of target elements under the load imparted by a given hazard is typically expressed in terms of a *fragility curve* that specifies the probability of realizing a certain state of damage as a function of intensity of the damage-

inducing mechanisms of the hazard (e.g., Ellingwood 2001). For populations of humans exposed to biological or chemical hazards, the analog to fragility curves are dose-response curves (Kowalski 2002). An element is said to be “hard” with respect to a given threat type if the probability of damage is sufficiently low relative to the range of possible intensities. Conversely, an asset is said to be “soft” or “fragile” if small intensities lead to significant damage. (Admittedly, the descriptive phrases “hard,” “soft,” and “fragile” are quantitatively ambiguous despite clear intensions, a characteristic which begs for the use of fuzzy sets (Zadeh 1965)). In general, the hardness of an asset or system element can only be improved through reengineering (e.g., blast retrofitting, vaccination). For example, Newland and Cebon (2002) discuss ways in which the buildings could be retrofitted to prevent collapse in the event of deliberate aircraft impacts.

3.4.2. Response Vulnerability

Response vulnerability describes the probability distribution on loss associated with a given damage state considering the intrinsic susceptibility of the target system to loss in light of system interdependencies and the availability of response and recovery measures (McGill and Ayyub 2007b). This category of vulnerability consists of all contributors to vulnerability that influence the degree of loss that would be realized given that a specified initiating event e_i resulted in damage state d_k . That is, response vulnerability measures the probability of a specified consequence or outcome associated with a given damage state. If loss cannot be effectively controlled, then the asset is vulnerable unless this deficiency is compensated for by effective security countermeasures that minimize probability of adversary success. According to the event

tree in Figure 3-3, a simple mathematical expression for response vulnerability, $V_R(c_j, d_k)$, for a given degree of loss c_j resulting from damage state d_k can be expressed as:

$$V_R(c_j, d_k) = \sum_m \Pr(c_j | c_{P,m}) \Pr(c_{P,m} | d_k) \quad (3-3)$$

where $\Pr(c_{P,m} | d_k)$ is the probability that a loss $c_{P,m}$ could result from damage state d_k (which is a measure of the intrinsic resistance of the target systems to loss, or basis loss), $\Pr(c_j | c_{P,m})$ is the probability that the actual loss is c_j in light of the effectiveness of response and recovery capabilities given that the basis loss was $c_{P,m}$, and the summation is taken over all m states of potential loss. Equation 3-3 assumes that the response vulnerabilities are assessed independently of the scenario that initiated damage state, d_k , which may be true for the “crisp” consequence dimensions such as direct economic damage and number of fatalities, but less true for the “softer,” less ascertainable dimensions such as psychological impact where the nature of the attack itself prompts loss irrespective of the resulting damage (e.g., an unsuccessful bomb attack). Expressed in terms of favorable defender characteristics, Eq. 3-3 can be rewritten as:

$$V_R(c_j, d_k) = \sum_m (1 - I_R(c_j, c_{P,m})) (1 - I_I(c_{P,m}, d_k)) \quad (3-4)$$

where $I_R(c_j, c_{P,m}) = 1 - \Pr(c_j | c_{P,m})$ is the effectiveness of response and recovery capabilities and $I_I(c_{P,m}, d_k) = 1 - \Pr(c_{P,m} | d_k)$ is the intrinsic resistance to loss. Based on Eqs. 3-3 and 3-4, the two dimensions of response vulnerability are the *intrinsic susceptibility of a system to loss following damage* and the *weakness of (or lack of)*

response and recovery capabilities. A discussion of each dimension of response vulnerability is provided in the following sections.

3.4.2.1. Basis Loss

Given some level of damage associated with a target element, the ensuing loss depends on the system or asset's *intrinsic resistance* to loss that accounts for the value of the target, and the physical, geographical, cyber and logical connectedness (Rinaldi et al. 2001) of the target element with respect to a larger system defined by the needs and concerns of a specific decision maker, such as an asset owner, regulating agency, or regional policymaker. For example, damage to a redundant component of a power plant might be significant from an asset owner's perspective since the component must be repaired or replaced, but may be inconsequential from the perspective of those responsible for the regional energy grid so long as the total supply of power to the grid continues to meet or exceed consumer demands. Intrinsic resistance is expressed as a probability distribution (however imprecise) over loss in the absence of response and recovery measures (i.e., basis loss), and as such depends on the definition of the system and its interdependencies, the context in which it the system is viewed, and dimensions of consequence considered in the analysis.

3.4.2.2. Response and Recovery

The loss following the occurrence of an adverse event can be tempered with measures to *respond* and *recover* from an event. Response measures seek to quickly contain immediate loss, such as responding to a mass casualty or mass exposure incident

with effective triage and treatment capabilities. For example, measures to enhance community and regional disaster preparedness fall under this category (McGill 1957). Recovery measures seek to restore an affected asset or system to as close to its pre-incident condition as possible, such as by reducing the duration of accumulating losses. The effectiveness of response and recovery capabilities is assessed conditionally for each degree of basis loss.

3.4.3. Overall Vulnerability

Overall vulnerability is a multidimensional property of a system that describes the probability of realizing a specified degree of loss following the occurrence of an initiating event (McGill and Ayyub 2007b). Given the expressions for protection vulnerability, V_P , in Eq. 3-1 and response vulnerability, V_R , in Eq. 3-3, the overall vulnerability, V_T , of a target to a given consequence, c_j , resulting from initiating event e_i can be expressed as:

$$V_T(c_j, e_i) = \sum_k V_P(e_i, d_k) V_R(c_j, d_k) \quad (3-5)$$

Using the expressions for V_P in Eq. 3-2 and V_R in Eq. 3-4, the overall vulnerability can be expressed in expanded form in terms of interventions as:

$$V_T(c_j, e_i) = \sum_k \sum_m (1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, d_k))(1 - I_R(c_j, c_{P,m}))(1 - I_I(c_{P,m}, d_k)) \quad (3-6)$$

where the summations are taken over all m states of potential loss and all possible damage states k . Equation 3-6 permits statements about the vulnerability of a system to a specified degree of loss resulting from a specified initiating event.

For example, a team of analysts and engineers can employ Eq. 3-6 to assess the overall vulnerability of an enterprise to 100 or more fatalities following a truck bomb attack in the underground parking structure. To make statements about overall vulnerability of the company to 100 or more fatalities resulting from an explosive or malicious attack *in general* (considering all delivery modes, targets, and intrusion paths) requires an aggregation of the overall vulnerability for each individual attack profile and initiating event considered (see Section 3.5.3).

Implicit in the correct use of Eq. 3-6 is a complete *awareness of plausible initiating events* (Gibson 2003) and *awareness of potential outcomes* following an event. Arguably among the most significant of the security weaknesses, lack of awareness of plausible security events and attack profiles facilitates the potential to be surprised by potential adversaries who actively seek to exploit these unidentified weaknesses, or from unanticipated outcomes following the occurrence of an otherwise considered threat type (McGill and Ayyub 2007b). For example, insufficient awareness of plausible scenarios and outcomes may lead to a false impression of security, particularly if these errors of omission are significant. One useful indication of whether a decision maker is sufficiently aware of plausible scenarios and their effects is the degree to which a decision maker would feel *surprised* were they to occur (Shackle 1969). Though difficult to measure quantitatively, any significant feeling of surprise should be examined to determine whether it is justified: scenarios of maximum surprise should coincide with

impossible scenarios, whereas scenarios unaccompanied by any feelings of potential surprise should be considered perfectly possible. Scenarios in between these extremes of surprise should be considered regardless of whether they are considered likely, since anything considered possible carries with it some degree of likeliness, however small (Dubois et al. 2008).

3.5. Threat Probability Assessment

3.5.1. The Basic Model

Any statement of probability of occurrence for an initiating event must be in relation to number of times, whether “none,” “once,” “more than once,” etc., it is believed will occur in a specified time horizon. In general, an annual recurrence rate, λ (in number of events per year), for each initiating event or class of events can be estimated, whether based on historical data or expert judgment, so long as it is accompanied by appropriate confidence bounds that accounts for all relevant uncertainties (expressed as a possibility distribution (Karimi and Hüllermeier 2007), probability of frequency (Kaplan and Garrick 1981), etc.). This recurrence rate or frequency provides a basis for estimating the probability of N events in a given time period T based on a Poisson model as follows (Ang and Tang 1975):

$$\Pr(n = N) = \frac{(\lambda T)^N}{N!} \exp(-\lambda T) \quad (3-7)$$

The use of a Poisson model to estimate number of events in a given time period is justified on the basis of maximum entropy arguments in light of the available information

on mean annual recurrence rate (Kapur 1990). Alternatively, one could express the probability of an event occurring sometime over a given time span directly.

Of interest is the probability that some number of potentially adverse initiating events will occur over a specified time period. This probability can be determined from Eq. 3-7 given the total annual rate of initiating events, λ_A :

$$\lambda_A = \lambda_{A_1} + \lambda_{A_2} + \dots + \lambda_{A_k} \quad (3-8)$$

where λ_{A_k} is the annual rate of occurrence for each type or class of initiating events, where $A_1 \cup A_2 \cup \dots \cup A_k = A$ and $A_1 \cap A_2 \cap \dots \cap A_k = \emptyset$. The reciprocal of Eq. 3-8 gives the mean return period or mean time to event T_A :

$$T_A = \frac{1}{\lambda_A} \quad (3-9)$$

Equation 3-9 can also express the annual rate of occurrence for a given class of initiating events in terms of the total annual rate of initiating events and the conditional probability of realizing the particular class of initiating events given an adverse event, A , has occurred:

$$\lambda_{A_k} = \lambda_A \Pr(A_k | A) \quad (3-10)$$

where:

$$\Pr(A_k | A) = \frac{\lambda_{A_k}}{\lambda_{A_1} + \lambda_{A_2} + \dots + \lambda_{A_k}} \quad (3-11)$$

Any given class of initiating events can be further decomposed based on specific threat types, intensity of event or attack mode, and location of occurrence such as is shown in the possibility tree of Figure 3-5. Defining a scenario e_i as the occurrence of a specific type of initiating event type, E_A , of a characteristic intensity, I_E , affecting a given location, L , the annual rate of occurrence for this scenario can be determined as:

$$\lambda_{s_i} = \lambda_A \Pr(A_k | A) \Pr(E_A | A_k, A) \Pr(I_E | E_A, A_k, A) \Pr(L | I_E, E_A, A_k, A) \quad (3-12)$$

It is required that the set of all initiating event types E_A for a given threat class A_k , the set of all characteristic intensities I_E for a given initiating event type, and the set of affected locations L be disjoint and exhaustive with respect to a predefined scope to ensure an exhaustive set of scenarios; this is an essential requirement for probabilistic analysis. Note that L is a general event for an attack occurring at a given location, and may be designed so as to include multiple simultaneous attacks at different locations or targets. Depending on the scope of decision making, the location can be interpreted as a region (such as a city, state, or portion thereof), portfolio of assets (such as in a sector, owned by a single entity, or simultaneously affected), or a single asset or small area. Moreover, the events and probabilities in Eq. 3-12 can be further decomposed, but for present purposes the expression as presented has sufficient resolution when supported by a suitable

description of A . Comparing the expression in Eq. 3-12 with that of Eqs. 3-10 and 3-11, the probability of a given scenario, e_i , given the occurrence of A , can be determined as:

$$\Pr(e_i | A) = \Pr(A_k | A) \Pr(E_A | A_k, A) \Pr(I_E | E_A, A_k, A) \Pr(L | I_E, E_A, A_k, A) = \frac{\lambda_{e_i}}{\sum_j \lambda_{e_j}} \quad (3-13)$$

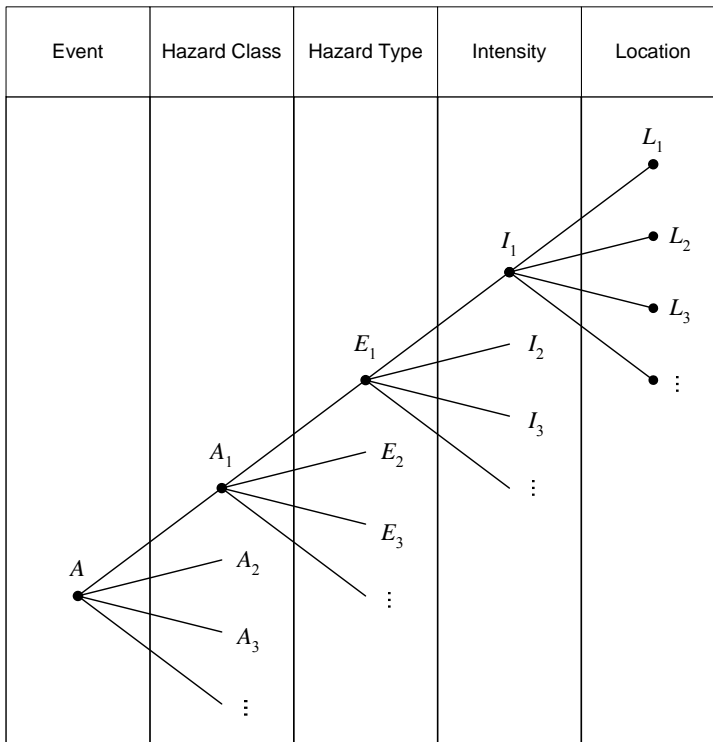


Figure 3-5. Possibility tree for threat probability assessment

3.5.2. Proportional Attractiveness Model

For malicious anthropic initiating events such as an explosive attack, the threat probability assessment phase estimates the annual rate of occurrence for each attack profile based on the perceived attractiveness of each asset, initiating event type, and

attack profile. More specifically, the annual rate of occurrence, λ_P , for an attack profile can be obtained as:

$$\lambda_P = \lambda_E A_A A_S A_P \quad (3-14)$$

where λ_E is a baseline annual rate of attack occurrence for a given threat type or class of threat types E , A_A is the probability of attack at a specific asset given the occurrence of an attack of specified type (i.e., asset attractiveness), A_S is the probability of occurrence for a specific threat scenario given the occurrence of an attack of specified type at a specified asset (i.e., scenario attractiveness), and A_P is the probability of occurrence for a specific attack profile given the occurrence of a specified threat scenario of a given type at a specified asset (i.e., profile attractiveness) (McGill et al. 2007). Comparing Eqs. 3-13 and 3-14 suggests that:

$$\Pr(e_i) = A_A A_S A_P \quad (3-15)$$

In contrast to tactical threat analysis that attempts to estimate the probability of attack based on available intelligence information to produce warnings and allocate tactical resources (McGill and Ayyub 2006; Pate-Cornell 1986), operational or strategic threat analysis, in general, seeks to estimate an representative annual rate of occurrence or probability for plausible security events and attack profiles in order to obtain quantitative expressions for total annual risk. For operational and strategic decision support, the probability of a given initiating event is a function of the annual rate of occurrence of the threat type affecting a portfolio of assets to which the asset belongs,

and the probability of realizing a specific attack profile given its occurrence. This latter parameter takes into account the relative attractiveness of all assets, their key elements, and potential attack profiles with respect to an adversary's perceptions of probability of success for attacking via the corresponding intrusion path and attack mode, gains from success, losses from failure, and costs to prepare for and execute an attack.

Attractiveness also depends on whether the adversary is aware of a particular intrusion path to the target or of the target itself; less visible intrusion paths and targets are less likely to be considered due to lack of information available to the adversary on their existence, and are therefore less attractive.

Considering the perceived probability of success, P_S^* , gain from success, G^* , loss from failure, L^* , cost to attack, C^* , associated with a given attack profile, the utility of the attack profile as perceived by the adversary, U_P , can be generically expressed as:

$$U_P = f(P_S^*, G^*, L^*, C^*) \quad (3-16)$$

In order to ascertain the form of the functional f in Eq. 3-16, it is important to first characterize the beliefs and capabilities of a notional adversary and how these translate into values for the parameters (Drake 1998; Bier et al. 2007). Such a characterization can be generic or specific to a given adversary or group of adversaries. For example, alternative adversary types such as a success oriented adversary (e.g., proportional to perceived probability of success, or $U_P = kP_S^*$), gain seeking adversary (e.g., proportional to perceived gain, or $U_P = kG^*$), or one seeking to maximize the benefit-to-cost ratio or expected utility can be considered as suggested by Yager (2006). Moreover, adversaries

may focus on losses of a specific type, systems of a certain type, or assets situated in a given location.

Assuming a rational adversary, attack profiles perceived to have a higher expected utility are more attractive than attack profiles with lower utilities. Considering the four variables comprising the adversary utility function shown in Eq. 3-16, the expected utility of an attack profile can be expressed as:

$$U_P = P_S^* G^* - (1 - P_S^*) L^* - C^* \quad (3-17)$$

If one assumes that the potential adversary (1) seeks to maximize total expected loss, (2) has perfect knowledge (i.e., the same as the defender's knowledge) of loss given success and probability of success for each visible attack profile and element, (3) has no expectations of survival after the attack regardless of whether the attack was successful, and (4) the relative cost to attack is negligible with respect to the expected gain from success, Eq. 3-20 can be reduced to:

$$U_P = \sum_j c_j V_T(P, c_j) \quad (3-18)$$

where c_j is a quantitative expression for degree of loss, $V_T(P, c_j)$ is the overall vulnerability to realizing c_j given $e_i = P$ from Eq. 3-5, and the summation is taken over all states of loss j . Note that Eq. 3-18 can be generalized to integral form if the consequence is specified as a continuous probability distribution function. From the four assumptions proposed, Eq. 3-18 suggests that the expected utility of a given attack profile from the

adversary perspective is equal to the expected loss given the occurrence of the attack profile as assessed by the defender. Further assuming that probability of a specified attack profile is directly proportional to the relative expected utility with respect to all other attack profiles raised to some non-negative power, it seems to follow that the assumptions leading to Eq. 3-18 yield a conservative estimate of risk; any deviation in adversary perceptions or preferences under these assumptions will apportion a greater degree of attractiveness to less consequential scenarios from the defender's point of view, and thus results in a lower estimate of actual risk. Accordingly, one strategy to maximize risk reduction under this assumption might be to promote adversary indifference by implementing strategies to reduce the expected conditional risk of all attack profiles to the same level.

An alternative, yet similar formulation to the utility function in Eq. 3-17 is to replace the cost to implement the attack (assuming cost to be irrelevant since alternative investments are not within the scope of an adversary's desired options) with a probability of achieving the capability needed to implement the attack, or P_C . If the adversary can achieve the capability to attack, then the expected utility is taken as before in Eq. 3-17 without the cost term; otherwise, there is no net gain or loss. This revised model expresses the expected utility from the adversary perspective as:

$$U_P = P_C^* (P_S^* G^* - (1 - P_S^*) L^*) \quad (3-19)$$

Making all the same assumptions as before, Eq. 3-19 can be reduced to:

$$U_P = P_C \sum_j c_j V_T(P, c_j) \quad (3-20)$$

Note that the form of Eq. 3-20 is the same as Eq. 3-17 with the exception of an added probability term P_C .

Similar to the attractiveness model described by Pate-Cornell and Guikema (2002) and touched on by Martz and Johnson (1987), the relative attractiveness of the i -th attack profile, A_{P_i} , can be defined as the ratio of the adversary perceived expected utility for a single profitable attack profile (i.e., $U_P > 0$) raised to some non-negative power to the sum of all profitable attack profile utilities for a given initiating event:

$$A_{P_i} = \frac{(U'_{P_i})^b}{\sum_j (U'_{P_j})^b} \quad (3-21)$$

where b is a bias parameter and U'_P is the perceived expected utility of the attack profile obtained as:

$$U'_{P_i} = \delta_{P_i} \max(U_P, 0) \quad (3-22)$$

where δ_{P_i} is a binary variable whose value is 1 if the attack profile is considered (i.e., is visible) and zero otherwise. By convention, $A_{P_i} = 0$ if the denominator of Eq. 3-21 is zero. The choice of b greatly influences how probability is apportioned; a value $b = 0$ defines a state of complete indifference in adversary preference where all attack profiles

are afforded equal probability, a value $b = \infty$ defines a state where all the probability is assigned to the attack profile with the largest utility, and increasing values of b toward infinity from zero specify increasing degrees of bias toward higher attractiveness attack profiles. A value in the neighborhood of $b = 2$ has been suggested by some researchers (Powers 2008).

The relative attractiveness of the i -th threat scenario, A_{S_i} , can be defined as the ratio of the perceived expected utility for a single threat scenario to the sum of all threat scenario utilities of the corresponding threat type as:

$$A_{S_i} = \frac{(U'_{S_i})^b}{\sum_j (U'_{S_j})^b} \quad (3-23)$$

where U'_{S_i} is taken as the maximum perceived expected utility among all attack profiles associated with scenario S_i or:

$$U'_{S_i} = \delta_{S_i} \max_j (U_{P_j}) \quad (3-24)$$

and δ_{S_i} is a binary variable whose value is 1 if the threat scenario is considered and zero otherwise. By convention, $A_{S_i} = 0$ if the denominator of Eq. 3-23 is zero. Alternatively, one could assume the scenario attractiveness to be equal to the expected value of all associated attack profiles, the minimum values among associated attack profiles, etc., the choice being at the reasonable discretion of the analyst.

The relative attractiveness of the i -th asset, A_{A_i} , can be defined as the ratio of the perceived expected utility for attacking the asset with a given threat type to the sum of all perceived expected utilities for all assets in a portfolio:

$$A_{A_i} = \frac{(U'_{A_i})^b}{\sum_j (U'_{A_j})^b} \quad (3-25)$$

where U'_{A_i} is taken as the maximum perceived expected utility among all threat scenarios associated with asset A_i or:

$$U'_{A_i} = \delta_{A_i} \max_j (U_{S_j}) \quad (3-26)$$

and δ_{A_i} is a binary variable whose value is 1 if the asset is considered and zero otherwise.

By convention, $A_{A_i} = 0$ if the denominator of Eq. 3-25 is zero. As with scenario attractiveness, Eq. 3-26 can assume alternative forms (e.g., expected value among all attack profiles, minimum value among all attack profiles, etc.) depending on the needs of the analyst.

Assuming that all assets, scenarios, and attack profiles are equally visible, the results from Eqs. 3-21, 3-23, and 3-25 can be integrated into Eq. 3-14 to estimate the annual rate of occurrence for each attack profile. However, treating asset, scenario, and profile visibility in a probabilistic manner insists that Eq. 3-15 be revised to account for all combinations of visibility situations. That is:

$$\Pr(e_i) = \sum_k \Pr(e_i | \nu_k) \Pr(\nu_k) \quad (3-27)$$

where $\Pr(\nu_k)$ is the probability corresponding to the state where only a given subset of assets, scenarios and attack profiles are visible and thus considered by the adversary, $\Pr(e_i | \nu_k)$ is the probability apportioned to e_i determined from the approach in Eqs. 3-21 through 3-26 considering only visible assets, scenarios, and attack profiles, and the summation is taken over all visibility combinations. More explicitly, Eq. 3-27 can be written in expanded form as:

$$\Pr(e_i) = \sum_j \sum_k \sum_l \Pr(\alpha_j) \Pr(\beta_k | \alpha_j) \Pr(\gamma_l | \beta_k, \alpha_j) A_{A|\alpha_j} A_{S|\beta_k, \alpha_j} A_{P|\gamma_l, \beta_k, \alpha_j} \quad (3-28)$$

where α_j defines a state where a subset of assets are visible (e.g., $\delta_{A_i} = 1$ for $i = 1, 2,$ and 5 ; $\delta_{A_i} = 0$ otherwise), β_k defines a state where a subset of threat scenarios associated with visible assets are themselves visible (e.g., $\delta_{S_i} = 1$ for $i = 1, 2,$ and 4 ; $\delta_{S_i} = 0$ otherwise), and γ_l defines a state where a subset of visible attack profiles associated with visible assets and threat scenarios (e.g., $\delta_{P_i} = 1$ for $i = 1, 2,$ and 3 ; $\delta_{P_i} = 0$ otherwise). The probabilities of these events are determined according to the assessed probabilities P_{VA} , P_{VE} , and P_{VP} that the assets, key elements, and intrusion paths are visible to the adversary, respectively, where for example the situation α_6 where assets 2 and 3 among a set of 4 assets are visible has a probability:

$$\Pr(\alpha_6) = \Pr(\delta_{A_1} = 0, \delta_{A_2} = 2, \delta_{A_3} = 1, \delta_{A_4} = 0) = (1 - P_{VA_1}) P_{VA_2} P_{VA_3} (1 - P_{VA_4})$$

Moreover, the attractiveness terms $A_{A|\alpha_j}$, $A_{S|\beta_k, \alpha_j}$, and $A_{P|\gamma_l, \beta_k, \alpha_j}$ in Eq. 3-28 are reassessed for all situations defined by α_j , β_k , and γ_l using appropriate values for δ_A , δ_S , and δ_P , in Eqs. 3-21, 3-23, and 3-25, respectively.

It should be noted, as was noted by Pate-Cornell and Guikema (2002), that there is currently no empirical justification for the use of the utility ratios as surrogates for probability, but is rather justified solely on the basis of the assumption that the probability of attack is proportional to the expected utility of alternative plausible attack profiles. However, Woo (2002) does make a good case for the use of such an exponential model based on order-of-magnitude comparisons of the utilities of alternative threat profiles and scenarios. Moreover, the appropriateness of using the maximum operator in lieu of, say, an averaging operator, minimum operator, etc., in Eqs. 3-22, 3-24, and 3-26 warrants further attention. For example, it may be sensible to specify lower-threshold values on expected utility for which only those scenarios that exceed this threshold will be considered in the analysis, just as it may be sensible to specify minimum values for one or more model parameters (e.g., $P_S^* \geq 0.75$, as described by Nerud 2008, or a minimum utility threshold as suggested by Bier 2007).

3.5.3. Aggregate Vulnerability

Given a set of initiating events e_i belonging to a class of threat types E ($e_i \in E$) (such as explosive attacks, malicious attacks, or natural hazards), the aggregate vulnerability, V_A , of the system to a degree of loss c_j can be obtained as:

$$V_A(c_j | E) = \sum_i V_T(c_j, e_i) \Pr(e_i | E) \quad (3-29)$$

where $\Pr(e_i | E)$ is the conditional probability of e_i given the occurrence of E , and the summation is taken overall all initiating events i belonging to E . In the case of malicious attacks, the probability of an initiating event depends on the attractiveness of the scenario relative to other options considered by the adversary. In general, malicious threats are intelligent and adaptive, and to assess the probability of a malicious initiating event thus requires consideration of intents, motivations, capabilities, and overall awareness of potential targets, threat types, and attack profiles.

According to the form of Eqs. 3-19, 3-21, 3-23, and 3-25, the conditional probability of an initiating event depends on an adversary's awareness of potential targets and perceptions of gain, loss, probability of success, and cost. In light of the expression for aggregate vulnerability in Eq. 3-29, the aggregate vulnerability for malicious attacks depends on adversary awareness and perceptions, which can be influenced by interventions that limit visibility and enhance deterrence. These considerations in the context of aggregate vulnerability are described in the following sections.

3.5.3.1. Visibility

As can be seen from the development of expressions in section 3.5.2, the *visibility* of an asset or system's elements and intrusion paths has a significant effect on aggregate vulnerability. If an element or intrusion path is not visible to an adversary, then the associated initiating events would not be considered. Visibility depends on the amount of information available to the adversary to assist in attack planning, such as through information gained through surveillance and reconnaissance or from open sources (Baker et al. 2004; Pluchinsky 2002). Strategies to minimize visibility serve to decrease aggregate vulnerability; however, difficulties in assessing what is truly visible to a potential adversary make this contributor hard to measure. A conservative approach to vulnerability assessment is to assume all assets, elements, and intrusion paths are visible to the adversary (i.e., probability of adversary awareness is one); any additional measures to limit visibility provide a bonus, though largely unassessed, improvement to aggregate vulnerability.

3.5.3.2. Perceived Attractiveness

As noted by Fuqua and Wilson (1977), *deterrence* affects the psyche of the adversary, and thus has influence over the choice of whether to attack and which attack profile to choose. In general, all visible and stated interventions and countermeasures have some deterrence value. The addition of deterrence measures designed solely for influencing adversary perceptions has the positive effect of moving adversary attention away from less protected elements and intrusion paths, and thus decreases aggregate vulnerability. While having no bearing on the actual performance of an asset under the

stress imposed by an adversary, measures such as fake cameras, decoy guards, signage, and mock targets serve to decrease vulnerability by creating the appearance of tight security or by creating irrelevant attack options. As with visibility, however, the assessing the perceptions of potential adversaries is difficult at best, and thus aggregate vulnerability should be conservatively assessed under the assumption of perfect adversary knowledge of all key elements, their loss potential, and the existence and effectiveness of interventions (i.e., the “mirror-imaging” assumption per McGill et al. (2007)).

3.5.3.3 Observations on Aggregate Vulnerability

According to the proportional attractiveness model for assessing the probability of a deliberate human-caused initiating event, the total mass of probability is biased toward those initiating events and attack profiles that are more attractive to the adversary from the standpoint of perceived expected utility. Under the conservative “mirror-imaging” assumption that assumes the adversary has perfect knowledge of system vulnerabilities, there exists a direct relationship between overall vulnerability and relative probability of occurrence for a given initiating event. That is, the more vulnerable a system is to a given initiating threat, the more likely the initiating event is to occur. Though in most circumstances this assumption is conservative, the fact that knowledge of adversary perceptions, motivations, capabilities, etc. is inherently limited justifies its use from a risk practitioner’s point of view. Unfortunately, the implications of this assumption is that a high overall vulnerability to loss from just one initiating event among a class of events dominates the aggregate vulnerability, whereas for naturally occurring events this would not necessarily be the case.

3.6. Actionable Risk Assessment

3.6.1. Expressing Risk

An expression for total risk conditioned on the occurrence of an event among class E of initiating events e_i in terms of a probability distribution on loss can be determined from Eqs. 2-3 and 3-5 as:

$$\Pr(c_j | E) = \sum_i V_T(c_j, e_i) \Pr(e_i | E) \quad (3-30)$$

where the summation is taken over the set of all initiating events $e_i \in E$. In expanded form for human-cause hazards, Eq. 3-33 can be expressed as:

$$\Pr(c_j | E) = \sum_j \sum_k \sum_l \sum_m \sum_n \frac{(1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, d_m)) \times \dots}{\Pr(\alpha_j) \Pr(\beta_k | \alpha_j) \Pr(\gamma_l | \beta_k, \alpha_j) A_{A|\alpha_j} A_{S|\beta_k, \alpha_j} A_{P|\gamma_l, \beta_k, \alpha_j}} (1 - I_R(c_j, c_{P,n})) (1 - I_I(c_{P,n}, d_m)) \times \dots \quad (3-31)$$

Note that c_j can be defined as the probability that the loss C exceeds some value c , which in turn causes Eqs. 3-30 and 3-31 to produce exceedance probabilities.

3.6.2. Loss Accumulation

Accepting the possibility that one or more events may occur within a given period of time, the total accumulated loss over a given time period t must consider the possibility of n event occurrences. In general, the loss given the occurrence of an event is dependent

on the loss from previous events, the elapsed time since the previous event, and how a decision maker decided to reconstitute his lost assets. For example, if an attack led to total loss, the asset owner may decide to not rebuild at all, thus making it pointless for the adversary to attack again. A general expression for loss accumulation can be expressed as:

$$F(t;l) = \sum_{n=0}^{\infty} \Pr(n,t) F_L^{(n)}(l) \quad (3-32)$$

where $F_L^{(n)}(l)$ is the general n-fold convolution as follows:

$$F_L^{(n)}(l) = P(\overbrace{L + L + \dots + L}^{n \text{ times}} < l) \quad (3-33)$$

In general, Eq. 3-33 must consider the fact that the probability of a given level of loss l occurring in the $(n+1)^{\text{th}}$ event is dependent on the level of loss realized in the n^{th} event. If it can be assumed that the distribution of loss given an event is independent of the spacing and number of events that have already occurred and that the rate of attack occurrence afflicting an asset or portfolio of assets is practically constant, the cumulative distribution on total accumulated loss in a time period t can be obtained assuming a Poisson model with rate of occurrence, λ_E , as follows (Ayyub 2003):

$$F(t;l) = \sum_{n=0}^{\infty} e^{-\lambda_E t} \frac{(\lambda_E t)^n}{n!} F_L^{(n)}(l) \quad (3-34)$$

It must be noted that the assumption of a constant rate of occurrence for attacks is highly contentious, particularly if the attack is of sufficient magnitude to prompt a significant defender response on the attacker's resources. Manunta (1999a) argues that probabilities cannot be justifiably assigned to intelligent adversaries that possess the power to decide where and when to attack, yet some empirical research has shown that, in some contexts, the overall frequency of attacks may remain constant in a given context despite a shift in tactics toward the less logistically complex (Enders and Sandler 2005). However, it may be reasonable to treat a recurrence rate not a statistically derived parameter, but as a subjective judgment that facilitates comparison with other rates for which statistics are available. For example, if one judges that the probability of occurrence of a terrorist attack within a given time span is less than that of earthquakes by some subjective order of magnitude, one could then apply this same order of magnitude reduction in the estimated annual recurrence rate for earthquakes to obtain a representative value for the terrorism hazard.

Often, of interest are the consequences following a single rare, catastrophic event. In this case, it may be sufficient to focus strictly on the losses of this single event. Accordingly, the analyst would leverage only the probability that an event will occur within a specified time frame in order to discount the conditional loss-exceedance curve given attack occurrence as the probability of a second event will often be much smaller than that of the first attack, if a second event is possible at all.

3.6.3. Sensitivity Analysis

A simple expression for determining the sensitivity, S , of some representative measure of risk, R , (e.g., mean, median, 99th percentile) with respect to a favorable improvement in the value of each risk variable (parameter) is given by:

$$S_i = \frac{1}{p} \frac{\Delta_p R_i}{R} \quad (3-35)$$

where $\Delta_p R_i$ is the change in the representative value of risk due to a favorable percentage change p in the value of the i -th risk contributor (in units of percentage change in risk per unit percentage change in the risk contributor) (Ayyub et al. 2007). If the upper limit of a parameter is fixed, p describes the degree of improvement of the variable as the fraction of distance between the current state and the ideal state. For example, assuming two parameters x and y bounded by the range [0 (bad), 10 (good)], if p is set to 10%, a fractional favorable change for $x = 2$ evaluates risk at $x = 2 + 10\%(10 - 2) = 2.8$, whereas a fractional favorable change for $y = 9.5$ evaluated risk at $y = 9.5 + 10\%(10 - 9.5) = 9.55$. Alternatively, if the favorable direction of a variable is theoretically unbounded but is bounded in the unfavorable direction (e.g., adversary delay time), the fractional change p is applied to the inverse of the variable. For example, if the delay time t is 20 seconds, the fractional favorable change for $p = 10\%$ would reassess risk at $t = 1/((100\% - 10\%)/(20 \text{ seconds})) = 22.2$ seconds. Equation 3-35 yields the ratio of fractional reduction in risk due to a fixed percentage change in the value of each risk contributor, which is a generalization of the risk reduction worth importance measure described by Modarres et al. (1999) (which can be achieved by setting $p = 100\%$ or 1.0).

3.7. Benefit-Cost Analysis

Benefit-cost analysis provides information that is useful to support strategic resource allocation decision making among alternative countermeasures and consequence mitigation strategies. In the context of malicious anthropic initiating events, countermeasures aim to reduce the probability of attack or probability of adversary success and consequence mitigation strategies aim to reduce the potential consequences following an attack, both of which serve to mitigate overall vulnerability to different degrees of loss. The benefit of a risk mitigation action is the difference between the values of loss, conditional risk, percentiles of risk, or total annual risk (collectively referred to as “state”) before and after its implementation (Ayyub 2003). The *benefit-to-cost ratio* is given by:

$$\frac{\textit{Benefit}}{\textit{Cost}} = \frac{\textit{Unmitigated State} - \textit{Mitigated State}}{\textit{Cost}} \quad (3-36)$$

where higher-valued ratios indicate better risk mitigation actions from a cost-effectiveness standpoint. The probability that a favorable benefit-to-cost ratio will be realized can be represented as:

$$\Pr\left(\frac{\textit{Benefit}}{\textit{Cost}} \geq \alpha\right) = 1 - \Pr(\textit{Benefit} - \alpha \textit{Cost} \leq 0) \quad (3-37)$$

where α is an acceptability criterion specified according to the dimensions of benefit and cost. In addition to the results of Eqs. 3-36 and 3-37, selection of a suitable risk mitigation action must also consider the affordability of each alternative and whether it achieves risk reduction objectives (McGill et al. 2007).

Chapter 4. Case Study – Asset Analysis

4.1. Problem Description

This chapter applies the CAPRA framework developed in Chapter 3 to the problem of allocating financial resources to protect a single infrastructure facility or asset (e.g., a chemical facility) against the threat posed by malicious attacks. The point of view of this analysis is the facility security manager, and by extension the asset owner, responsible for ensuring continuity of business and the safety of his employees and visitors. The decision *variables* in this study include all aspects of facility security, to include detection, delay, response, and defeat measures. The *effects* or *outcomes* of concern to the decision maker following an attack include service disruption, property damage, environmental damage, and loss of life. The *sources* of risk in this case study are limited to the phenomenologies associated with an improvised explosive device (IED) attack via a variety of different attack modes, including hand-emplaced, ground vehicle delivered, and aerial delivered explosives. The set of *targets* of the risk is defined by seven operational elements shown in Figure 4-1, namely tank 1 (“small tank”), tank 2 (“large tank”), underground pipeline, loading dock, 80-ton rail cars, railroad track, and a main building. (Note that collectively tank 1 and tank 2 comprise the “tank farm”). Supporting elements whose compromise would increase the probability of success for attacks (e.g., guard posts, fences, trees) and elements external to the facility whose compromise would negatively impact operations (e.g., the rail system, highway infrastructure, electric power, end-users) are outside the scope of this analysis. Note that

all aspects of this analysis, to include the facility, its elements, and its characterization, are purely notional and are only for the purpose of illustrating the CAPRA methodology.

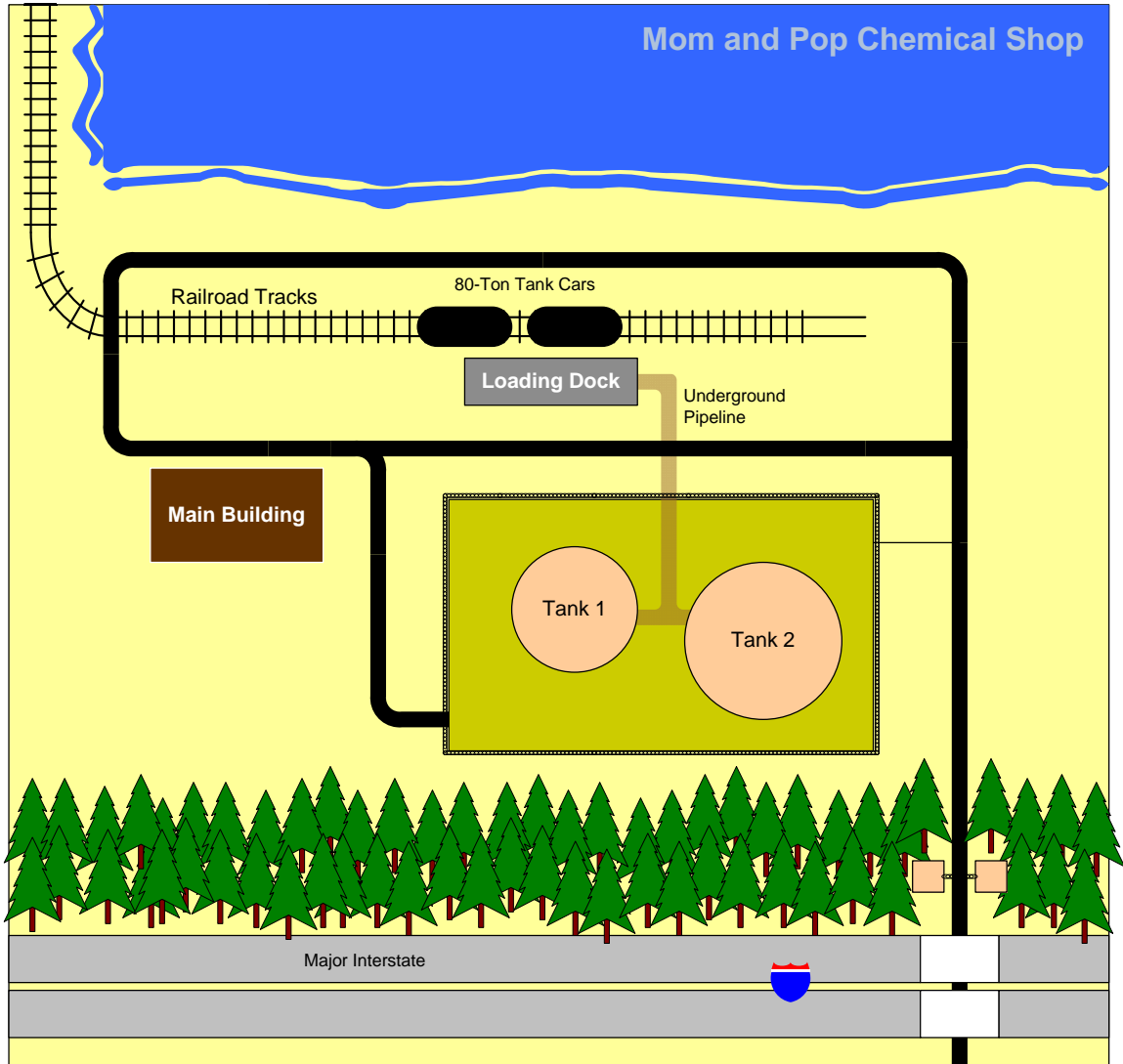


Figure 4-1. Site plan for the notional chemical facility

4.2. Scenario Identification

The scope of this analysis centers on the risk resulting from an explosive attack against elements of the notional chemical facility shown in Figure 4-1. A set of five

attack modes relevant to IED events were considered as described in Table 4-1. The explosive intensity associated with these attack modes is characterized by a simple discrete probability distribution constructed over a finite set of charge weight bins (i.e., “small,” “medium,” and “large”) where each bin represents a stratification of an otherwise continuous probability distribution (Figure 4-2). The probabilities in Table 4-1 were informally elicited from an explosives expert (Neale 2008). Each attack mode accesses a target in a specific way. In particular:

- Hand emplaced (HE) explosive attacks are characterized by explosives delivered by a human directly to the target, and includes satchel charges, backpack bombs, and suicide attacks. Hand emplaced explosive attacks are compatible with any target accessible to humans on foot and susceptible to the effects of explosives.
- Ground vehicle (GV) explosive attacks are characterized by explosives delivered by ground-transiting vehicles, ranging from small compact cars to large trucks. Ground vehicle explosive attacks are compatible with any target accessible via roads and susceptible to the effects of explosives.
- Manned aerial vehicle (AVM) explosive attacks are characterized by explosives delivered by any type of human-operated air vehicle capable of carrying explosives, including motorized gliders and small airplanes. Manned aerial vehicle explosive attacks are compatible with any target accessible by air and susceptible to the effects of explosives.
- Unmanned aerial vehicle (AVU) explosive attacks are characterized by explosives delivered by any type of unmanned or autonomous aerial vehicle capable of

carrying explosives, including radio-controlled aircraft and motorized balloons.

Unmanned aerial vehicle explosive attacks are compatible with any target accessible by air and susceptible to the effects of explosives.

- Waterborne (WB) vehicle explosive attacks are characterized by explosives delivered by any type of water-transiting vehicle, including small boats such as canoes and kayaks to large vessels such as sailboats, yachts, and barges.

Waterborne vehicle explosive attacks are compatible with any target directly adjacent to a body of water (e.g., river, lake) and susceptible to the effects of explosives.

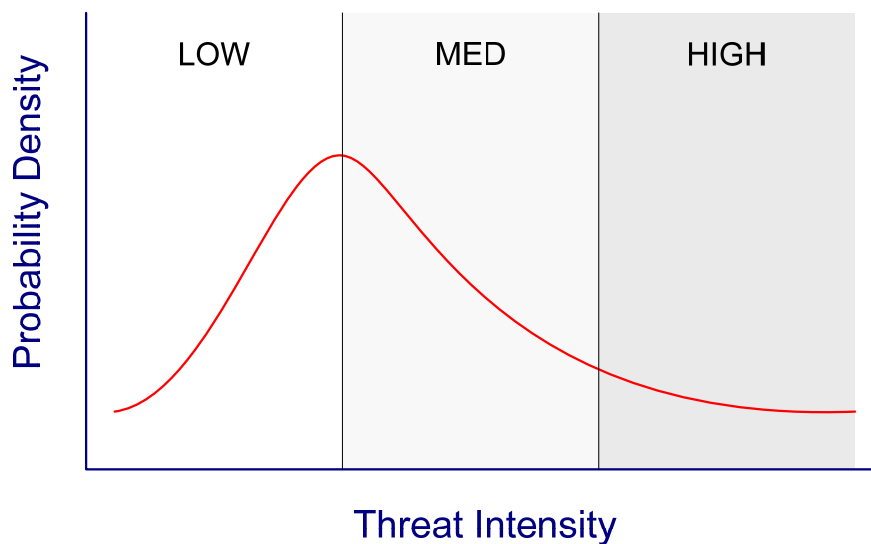


Figure 4-2. Threat intensity distribution for a given attack mode

Table 4-1. Explosive attack modes and expected loss given success.

Delivery System	Probability of Intensity, p		
	Low	Med	High
Hand Emplaced	0.9	0.1	0.0
Ground Vehicle	0.0	0.1	0.9
Manned Aerial Vehicle	0.8	0.2	0.0
Unmanned Aerial Vehicle	1.0	0.0	0.0
Waterborne Vehicle	0.0	0.5	0.5

To identify and screen initiating events on the basis of their relevance and first order assessment of risk, the hybrid FMECA/CARVER technique briefly mentioned in section 3.2 was employed to identify and screen in initiating events for more detailed analysis. In particular, this qualitative risk analysis method examines the inherent susceptibilities of all identified elements to a wide array of plausible malicious attack types, describes the manner in which the elements fail in response to an attack, and speculates on a worst reasonable case outcome given attack. In light of these narratives, this technique scores each of the seven attributes of the CARVER + Shock methodology (US Food and Drug Administration 2007) described in Table 4-2. Accepting the logic described in the simple possibility tree in Figure 4-3, an expression for the risk score, RS, for each initiating event can be obtained as:

$$RS = \log_{10}RAV + \log_{10}[w_{\text{H}}(10^{\text{H}}) + w_{\text{P}}(10^{\text{P}}) + w_{\text{E}}T(10^{\text{E}}) + w_{\text{S}}(10^{\text{S}})] \quad (4-1)$$

where R is the *recognizability* of the target element, A is the *accessibility* of the target, V is the *vulnerability* as the likeliness of damage given attempt (i.e., protection vulnerability per section 3.4), the *criticality* is the sum of human harm (H) and property damage (P), E is the economic effect of disruption per unit duration and T is the duration for complete

recoverability, and S is the impacts resulting from the shock of the attack to include psychological damage and other game changers. The expression for RS in Eq. 4-1 gives an order of magnitude expression of risk, and in linear space corresponds to a simple probabilistic risk analysis model (Cox 2005). Base-10 logarithms are used in Eq. 4-1 to accommodate estimates of loss as orders of magnitude, where the scoring schemes for the bracketed loss parameters are described in Tables 4-3 (probability terms), 4-4 (consequence terms), and 4-5 (recoverability). Given a minimum risk score threshold value M , a relative risk priority number, RRPN, can be determined as:

$$RRPN = 10^{(RS - M)} \quad (4-2)$$

For convenience and to enhance communication with senior leadership without loss of usefulness of the process, values for RS and RRPN are rounded to the nearest $1/10^{\text{th}}$ for display in the hybrid FMECA/CARVER table.

A complete set of relevant initiating events was obtained using the hybrid CARVER/FMECA method as shown in Table 4-6, where an event was deemed relevant if its RRPN was 6 or more (i.e., $M = 6$). According to Table 4-6, the following initiating events are screened-in for full analysis:

- Explosive attack against chemical tank 1 (small)
- Explosive attack against chemical tank 2 (large)
- Explosive attack against main building

For the purposes of illustration, the remainder of this chapter example focuses only on the disjunctive event “explosive attack against tank farm,” which corresponds to an attack occurring at tank 1, tank 2, or both. It is reasonable to consolidate these two scenarios into one since it is assumed to be a relatively trivial to attack both simultaneously given their close proximity to one another, or at the very least an attack on one has a significant potential to incite common cause failures in the other.

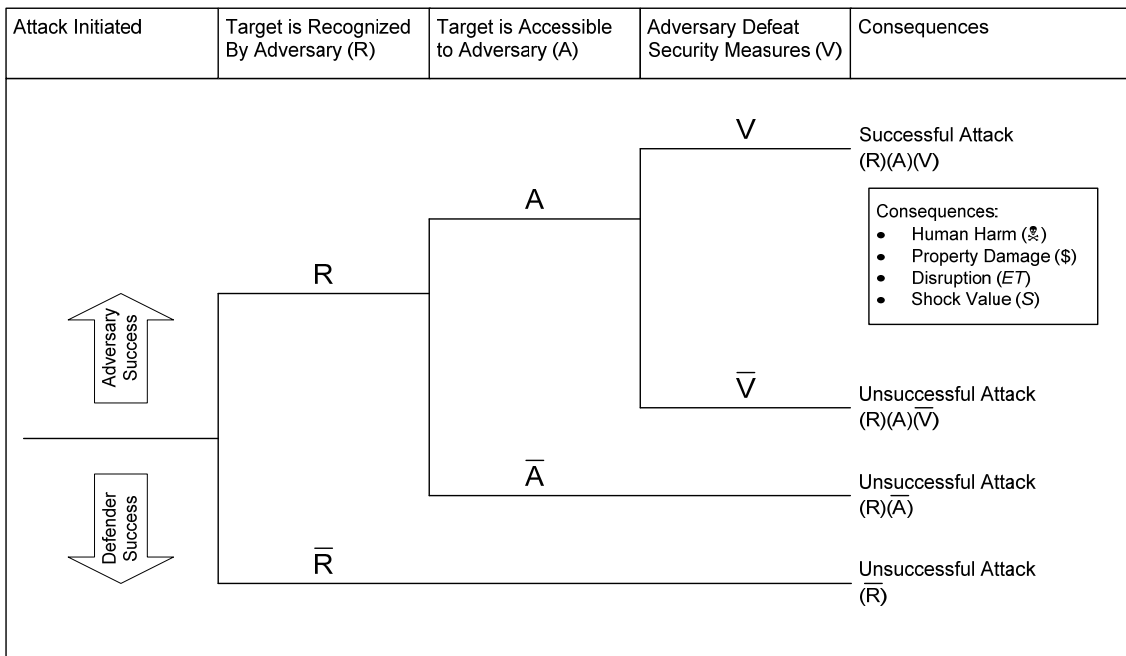


Figure 4-3. Possibility tree for the hybrid FMECA/CARVER method

Table 4-2. Hybrid FMECA/CARVER model parameters and interpretation

Parameter		Definition (FDA 2007)	Interpretation
Probability Parameters	Recognizability (<i>R</i>)	Ease of identifying target	Likelihood that a determined adversary would recognize the value of the target in question, measured as a probability
	Accessibility (<i>A</i>)	Ability to physically access and egress from target	Likelihood that the adversary could access the target in the absence of security measures, measured as a probability
	Vulnerability (<i>V</i>)	Ease of accomplishing attack	Likelihood of adversary success at damaging the target considering security measures and target fragility, measured as a probability
Severity Parameters	Criticality: Human Harm (☠)	Measure of public health and economic impacts of an attack	Order of magnitude of the seriousness of human health effects considering injuries and fatalities, measured on a bounded constructed scale
	Criticality: Property Damage (\$)		Order of magnitude of the seriousness of property damages and asset loss, measured on a bounded constructed scale
	Effect (<i>E</i>)	Amount of direct loss from an attack as measured by loss in production	Order of magnitude of the value of lost production through dissolution of the facility
	Shock (<i>S</i>)	Shock value of an attack in terms of psychological and other impacts	Order of magnitude of the game changing consequences, or seriousness of the shock to the system
Recoverability (<i>T</i>)		Ability of the system to recover from an attack	Time to reconstitute production as a fraction of time to dissolution

Table 4-3. Scoring scheme for each probability parameters of the hybrid approach

Score	Interpretation of Parameter at Each Score Level		
	Recognizability (<i>R</i>)	Accessibility (<i>A</i>)	Vulnerability (<i>V</i>)
0	It is near impossible that the adversary will recognize the element	The target is completely inaccessible to an adversary in light of plausible adversary capabilities	The security measures make it nearly impossible for an adversary to achieve success in light of plausible adversary capabilities
5	There is an even chance that the adversary will recognize the element	There is an even chance that a determined adversary can access the target in light of plausible adversary capabilities	There is an even chance that a determined adversary will successfully defeat security measures in light of plausible adversary capabilities
10	It is near certain that the adversary will recognize the element	It is near certain that a determined adversary can access the target in light of plausible adversary capabilities	It is near certain that a determined adversary will successfully defeat security measures in light of plausible adversary capabilities

Table 4-4. Scoring scheme for each consequence parameter of the hybrid approach

Score	Interpretation of Parameter at Each Score Level			
	Criticality: Human Harm (♣)	Criticality: Property Damage (\$)	Effect (E)	Shock (S)
0	Zero Lives	\$0-\$10	\$0-\$10	No Shock
1	<i>Not Used</i>	\$10-\$100	\$10-\$100	<i>Not Used</i>
2		\$100-\$1,000	\$100-\$1,000	
3		\$1,000-\$10,000	\$1,000-\$10,000	
4	Minor Injuries Only	\$10,000-\$100,000	\$10,000-\$100,000	Minor Psychological Response
5	Major Injuries Only	\$100,000-\$1M	\$100,000-\$1M	
6	1-10 Lives	\$1M-\$10M	\$1M-\$10M	Major Psychological Response
7	10-100 Lives	\$10M-\$100M	\$10M-\$100M	
8	100-1,000 Lives	\$100M-\$1B	\$100M-\$1B	Severe Psychological Response
9	1,000-10,000 Lives	\$1B-\$10B	\$1B-\$10B	
10	>10,000 Lives	>\$10B	>\$10B	Shutdown
w	5	1	1	1

Table 4-5. Scoring scheme for the recoverability parameter

Score	0	2	4	6	8	10
Percentage Time	0%	20%	40%	60%	80%	100%

Table 4-6. Hybrid FMECA/CARVER assessment for the notional chemical facility

Key Element	Failure Mode	Outcomes of Failure	Severity					Protection Vulnerability	Probability			Risk Score	Relative Risk Priority Number
			Criticality		Effect	Recoverability	Shock		Recognizability	Accessibility	Vulnerability		
			%	\$									
Tank 1 (Small)	Failure to contain hazardous materials	Release of hazardous materials followed by exposure of employees to lethal chemicals; damage to storage tank; disruption of mission	7	6	7	2	6	Tank is very visible but with few indications of current volume; Additional guard fence protection beyond baseline security	8	8	7	7.4	24
Tank 2 (Large)	Failure to contain hazardous materials	Release of hazardous materials followed by exposure of employees to lethal chemicals; damage to storage tank; disruption of mission	7	6	7	3	6	Tank is very visible but with few indications of current volume; Additional guard fence protection beyond baseline security; tank structure is vulnerable to damage from	8	8	7	7.4	24
Pipeline	Failure to transit products from storage tanks to rail cars	Minor release of hazardous materials followed by quick containment to minimize employee exposure; damage to pipeline; minor business disruption	5	5	7	1	4	No subsurface access without digging; main access control point and distance are the only barriers; highly ambiguous where the pipeline runs	2	3	6	4.8	(15)
Loading Dock	Failure of structure	Loss of use of loading dock; requires ad hoc substitute	5	3	0	2	4	Highly recognizable asset; only baseline security measures apply with main access control point and distance being the only barriers; structure highly vulnerability to damage from explosion	9	9	8	5.5	(3)
Rail Cars	Failure to provide means for shipping chemicals to customers	Loss of rail cars for shipping; replacement available within days	5	4	2	0	5	Rail cars are very visible to a facility insider; only baseline security measures apply	9	10	7	5.6	(3)
Railroad Track	Failure to allow passage of transiting rail cars	Loss of ability to transit rail cars for shipping product; fix can be achieved very quickly	0	3	2	0	4	Difficult to damage in any significant way using explosives; only baseline security measures apply; track is very visible	10	10	5	3.7	(182)
Main Building	Failure to house personnel and administrative functions	Exposure of personnel to effects of blast to include; with the exception of lost people, no major disruption to operations due to quick reconstitution of administrative support functions at a remote facility	6	5	2	3	6	Main building is less visible than all other elements except for the pipeline, but recognizable once on the facility; baseline security measures apply	10	10	8	6.7	5
Criticality: Measure of public health and economic impacts of an attack Recognizability: Ease of identifying target			Accessibility: Ability to physically access and egress from target Vulnerability: Ease of accomplishing attack			Effect: Amount of direct loss from an attack as measured by loss in production Recoverability: Ability to recover from an attack			Shock: Shock value of the attack				

4.3. Consequence and Severity Assessment

As stated in the problem description in Section 4.1, this analysis considers four consequence dimensions assessed from the point of view of the facility owner as follows:

- Repair and replacement costs (measured in dollars)
- Fatalities and injuries (measured in equivalent fatalities)
- Recuperation time at full disruption (measured in days)
- Environmental damage (measured in units for land area)

Table 4-7 describes the maximum potential loss for each consequence dimension.

Constant consequence conversion factors are used to convert all non-monetary consequences into an equivalent economic value. The consequence conversion factors used in this analysis are shown in the third column of Table 4-7. Since this analysis is looking at the risk situation exclusively from the point of view of a facility owner, external consequences such as downstream cascading effects and decreased public confidence are not considered. Moreover, while it can be expected that an attack of any type will result in “shock” effects (e.g., vicarious liability (Douglas 1929)) directly felt by the asset owner, such impacts are outside the scope of this analysis.

Table 4-7. Maximum potential loss and loss conversion factors

Consequence Dimension	Maximum Potential Loss	Consequence Conversion Factor
Fatalities	50 persons	\$6.0-M
Repair Costs	\$20.0M	N/A
Recuperation Time	90 days	\$100K/day
Environmental Damage: Chemical Release	10 acres	\$300K/acre

4.4. Overall Vulnerability Assessment

As described in Chapter 3, Section 3.4, overall vulnerability assessment examines both protection and response vulnerabilities. This study employs probabilistic event tree modeling and systems reliability engineering concepts to assess security system effectiveness, target accessibility, and fragility of key elements to arrive at a discrete probabilistic representation of protection vulnerability. However, because this particular facility lacks indigenous emergency response capabilities, the assessment of response vulnerability is simplified to focus exclusively on basis loss.

4.4.1. Security System Effectiveness

In order for a security system at any level to defeat an adversary, the adversary must be detected, engaged by response forces, and neutralized; failure to succeed at any one of these steps results in an overall failure to defeat a determined adversary (Hicks et al. 1999). Figure 4-4 illustrates an example event tree for an intrusion path at a facility consisting of three security zones, where the overall facility security system consists of hardware, human, and software elements (Smidts et al. 1997; Modarres et al. 1999; Mosleh and Chang 2004; Li et al. 2005; Li et al. 2006). Defining *interruption* as the combined event that the adversary has been detected *and* engaged by response forces, a

simple equation giving the probability of interruption, P_I , for an intrusion path consisting of n security zones considering only passive security measures can be expressed as (Dessent 1987):

$$P_I = P_{DP_1} P_{E|D_1} + \sum_{j=2}^n P_{DP_j} P_{E|D_j} \prod_{m=1}^{m=j-1} \{1 - P_{DP_m}\} \quad (4-3)$$

where P_{PD_j} is the probability that the adversary is detected with the passive detection measures present in security zone j and $P_{E|D_j}$ is the probability that the defender force engages the adversary given detection in security zone j .

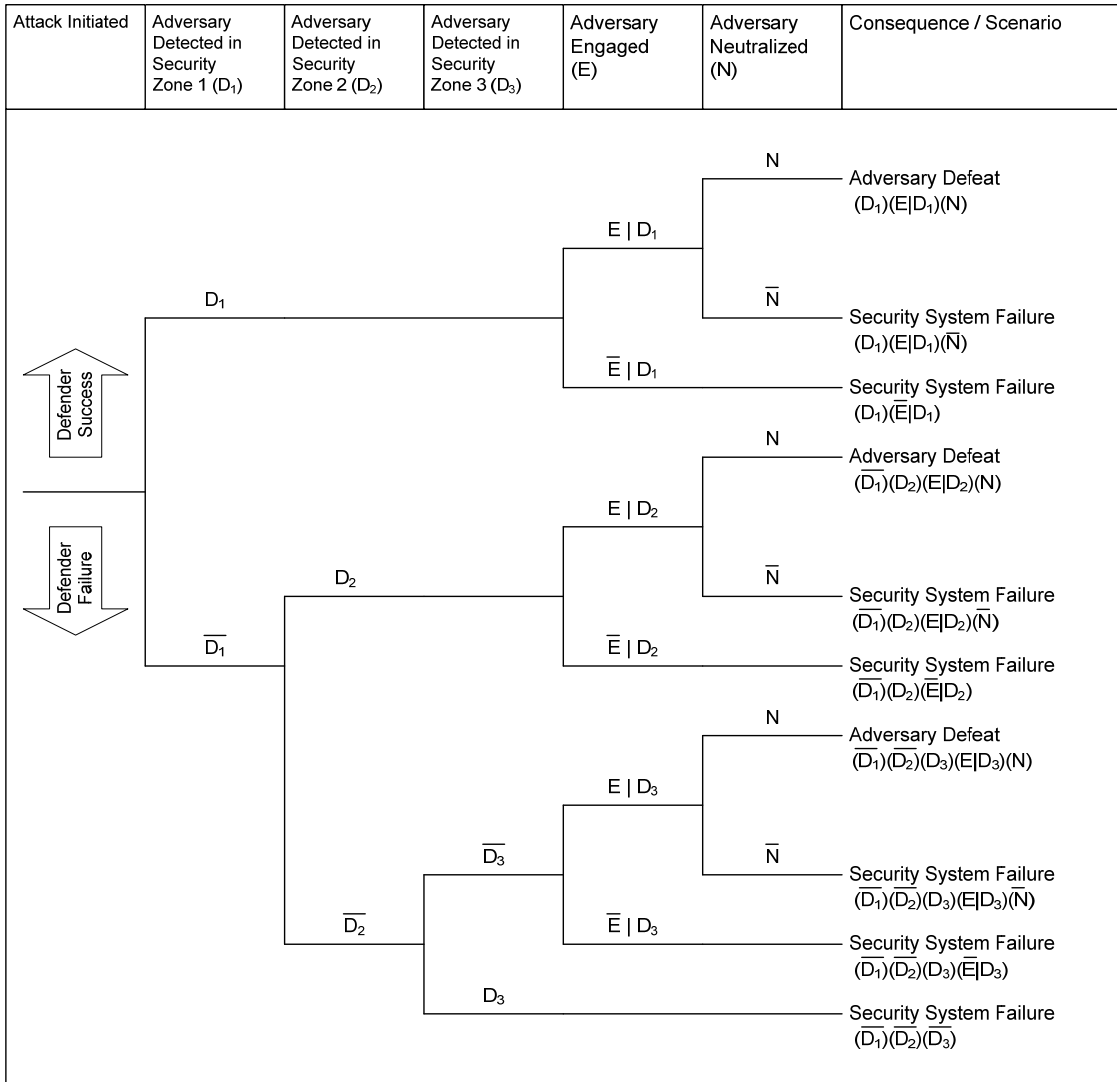


Figure 4-4. Event tree for assessing security system effectiveness

In general, the probabilities in Eq. 4-3 are a function of both time and adversary capability, and their assessment can be obtained with knowledge of the mean time to detect for active (i.e., time-dependent) detection measures and probability of detection for static (i.e., demand-based) detection measures (Doyon 1981; Kobza and Jacobson 1997), the adversary delay time associated with each barrier along an intrusion path, and

response times of the defender forces. The probability of engaging the adversary given detection, $P_{E|D}$ can be expressed as:

$$P_{E|D} = \Pr(t_R \leq t_D) \quad (4-4)$$

where t_D is a random variable describing the total adversary transiting delay time between the point of detection and the target (plus time for egress if egress is part of the scenario) and t_R is a random variable describing the time for the defender to respond to and engage the adversary. Using the stress-strength reliability model (Ayyub and McCuen 2002; Kotz 2003), the probability of engagement can be computed as:

$$\begin{aligned} \Pr(t_R \leq t_D) &= \int_0^\infty F_{T_R}(\tau) f_{T_D}(\tau) d\tau \\ &= \int_0^\infty (1 - F_{T_D}(\tau)) f_{T_R}(\tau) d\tau \end{aligned} \quad (4-5)$$

where the capital F and lower-case f denote the cumulative distribution and probability density functions, respectively, for the event in the subscript.

More significant is the probability of detection for active-detection measures, where the probability of detection is a function of duration of an adversary exposure in a security zone. This probability can be characterized by the exponential cumulative distribution function, F_{DA} , as follows:

$$F_{DA}(t) = 1 - \exp\left(-\frac{t}{MTTD}\right) \quad (4-6)$$

where $MTTD$ is the mean time to detect which is a function the defender capabilities to sense, recognize, and annunciate the presence of an adversary. Equation 4-6 assumes a constant rate of detection given the presence of an adversary in a security zone. The probability density function, f_{DA} , for this model can be expressed as:

$$f_{DA}(t) = \frac{1}{MTTD} \exp\left(-\frac{t}{MTTD}\right) \quad (4-7)$$

For active detection measures, detection can occur at any time while an adversary is present in a security zone. Accordingly, Eq. 4-3 must be revised to accommodate active measures by incorporating the following expression for probability of intervention given detection in a security zone:

$$P_D = \int_0^{\infty} \Pr(t_D > \tau) f_{DA}(\tau) d\tau \quad (4-8)$$

and

$$P_I = \int_0^{\infty} \Pr(t_R \leq t_D | t_D > \tau) \Pr(t_D > \tau) f_{DA}(\tau) d\tau \quad (4-9)$$

For security zones containing both active and passive detection measures, the probability of intervention is:

$$P_I = \Pr(t_R \leq t_D)P_{DP} + (1 - P_{DP}) \int_0^{\infty} \Pr(t_R \leq t_D | t_D > \tau) \Pr(t_D > \tau) f_{DA}(\tau) d\tau \quad (4-10)$$

For a security system composed of a sequence of n security zones with arbitrary composition of passive and active detection measures, Eq. 4-3 can be generalized as:

$$P_I = P_{I_1} + \sum_{j=2}^n P_{I_j} \prod_{m=1}^{m=j-1} \{1 - P_{D_m}\} \quad (4-11)$$

where the probability of intervention is determined from Eq. 4-10. Using the model for security effectiveness assessment described in Hicks et al. (1999), the probability that the defender interrupts and defeats the adversary (i.e., the security system effectiveness), I_S , can be expressed as:

$$I_S = P_I P_{N|I} \quad (4-12)$$

where $P_{N|I}$ is the probability that the defender neutralizes and defeats the adversary given interruption by the defender. The results from Eq. 4-12 can be interpreted as the *reliability* of the security system with respect to a given challenge defined by the attack profile (McGill et al. 2007).

As shown in Figure 4-5, four representative intrusion paths that define relevant plausible security events afflicting the tank farm. Figure 4-6 illustrates these intrusion paths in relation to tank farm attacks, each divided into a sequence of one or two security zones. For the event “explosive attack against the tank farm,” the attack profile

compatibility matrix shown in Table 4-8 defines all relevant combinations of delivery system and intrusion path, where an “X” denotes a relative pairing between intrusion path and attack mode. Table 4-9 summarizes notional values for security system performance variables in relation to security zones and applicable attack profiles. Since delay and response are non-negative values with an unbounded upper limit, maximum entropy arguments insist that these parameters be characterized by lognormal distributions when only a mean and coefficient of variation was provided (Kapur 1990). The summary results for probability of intervention, probability of neutralization (as an input) and security system effectiveness for each delivery system (attack mode) type is given in Table 4-10.

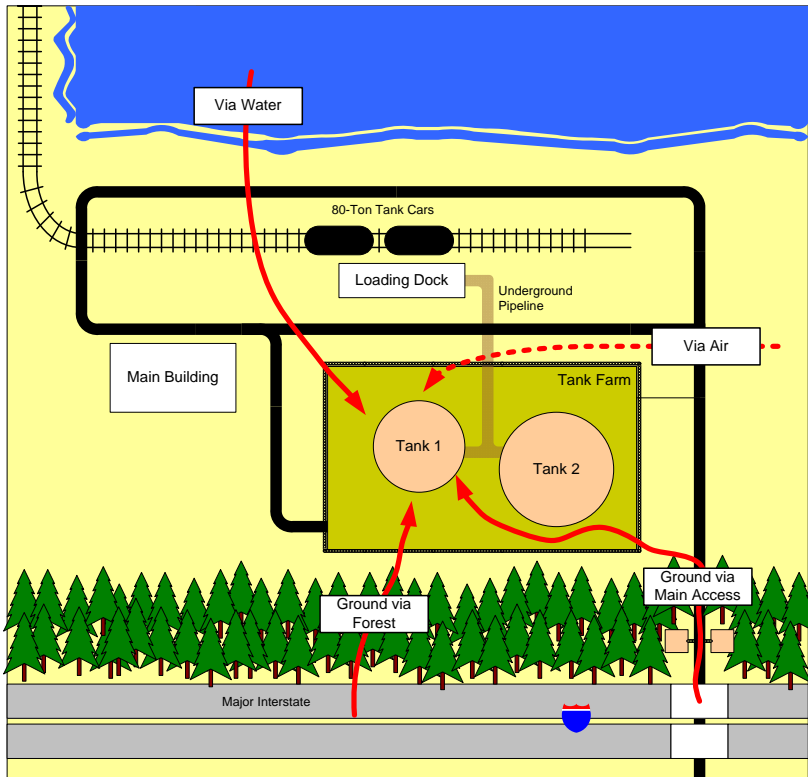


Figure 4-5. Representative intrusion paths into the chemical facility

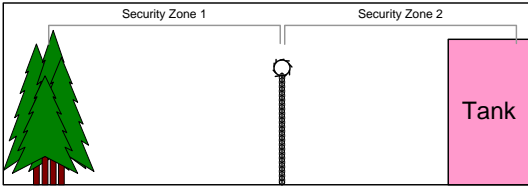
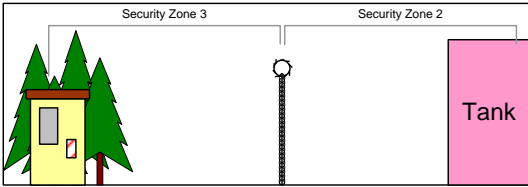
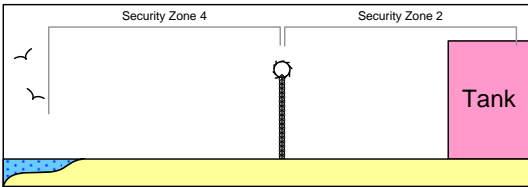
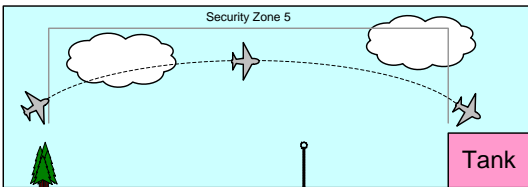
INTRUSION PATH CROSS-SECTION	COUNTERMEASURES
<p>Ground (via Forest)</p> 	<p><i>Security Zone 1:</i> Barriers: Forest, Distance Sensors: Concealed Trip Wire (silent alarm) Visual (Human)</p> <p><i>Security Zone 2:</i> Barriers: Chain-Linked Fence w/ Barbed Wire, Distance Sensors: Camera Motion Detector</p>
<p>Ground (via Main Access)</p> 	<p><i>Security Zone 3:</i> Barriers: Main Gate, Distance Sensors: Visual (Human) Camera</p> <p><i>Security Zone 2:</i> Barriers: Chain-Linked Fence w/ Barbed Wire, Distance Sensors: Camera Motion Detector</p>
<p>Ground (via Water)</p> 	<p><i>Security Zone 4:</i> Barriers: Distance Sensors: Visual (Human)</p> <p><i>Security Zone 2:</i> Barriers: Chain-Linked Fence w/ Barbed Wire, Distance Sensors: Camera Motion Detector</p>
<p>Air</p> 	<p><i>Security Zone 5:</i> Barriers: Distance Sensors: Visual (Human)</p>

Figure 4-6. Intrusion paths to a chemical tank

Table 4-8. Attack profile compatibility matrix for explosive attack against the tank farm

Delivery System	Intrusion Path			
	Via Main Access Road	Via Forest	Via Water	Via Air
On Person	X	X	X	-
Ground Vehicle	X	-	-	-
Waterborne Vehicle	-	-	-	-
Aerial Vehicle	-	-	-	X

Table 4-9. Security system performance attributes for each security zone

Delivery System	Security Zone	Delay Time*		Response Time*		Probability of Detection with Passive Detection Measures	Mean Time to Detect for Active Detection Measures (sec)
		Mean (sec)	COV	Mean (sec)	COV		
Hand Emplaced	1	150	0.15	60	0.20	0.0	300
	2	30	0.20			0.5	60
	3	150	0.20			0.5	1,200
	4	180	0.25			0.0	450
Ground Vehicle	2	10	0.20			0.7	30
	3	40	0.10			0.2	150
Aerial Vehicle (Manned and Unmanned)	5	60	0.20	120	0.10	0.0	300

*Note: Delay time and response time distributions are assumed to be lognormally distributed

Table 4-10. Summary of results for the explosive attack against tank farm event

Attack Profile	Probability of Intervention	Probability of Neutralization	Security System Effectiveness
Hand emplaced via forest	0.3292	0.70	0.2305
Hand emplaced via main access road	0.5490	0.70	0.3843
Hand emplaced via water	0.2820	0.70	0.1974
Ground vehicle via main access road	0.0486	0.20	0.0097
Manned aerial vehicle via air	0.0000	0.20	0.0000
Unmanned aerial vehicle via air	0.0000	0.10	0.0000

4.4.2. Target Accessibility

If the security system fails to defeat the adversary, the adversary must then successfully impart a load to the target in order to cause damage. For each of the five attack modes considered, Table 4-11 gives a notional probability of successful attack execution that applies equally to all target elements. This value accounts for both uncertainty in weapon performance and the accessibility of the target. Note that because the probability of successful execution is zero for both the tank farm and main building scenarios since none of the screened-in assets considered are sufficiently close to a body water.

Table 4-11. Probability of successful execution for each of the five delivery systems

Attack Mode	Probability of Successful Execution
Hand Emplaced	0.98
Ground Vehicle	0.95
Manned Aerial Vehicle	0.90
Unmanned Aerial Vehicle	0.75
Waterborne Vehicle	0.00

4.4.3. Target Hardness and System Response

Given that the adversary successfully imparts a load onto its target, the target must be unable to resist the load if damage, and consequently, loss or harm is to be achieved. In this study, the “fragility” of system response is expressed in terms of a series probability distributions constructed over each consequence dimension as a function of threat intensity. Table 4-12 describes system response fragility with respect to an explosive attack against the tank farm for a variety of explosive intensities. This approach is in contrast to a more detailed analysis that would first assess the probability of alternative damage states followed by an assessment of probability for different degrees of basis loss (i.e., system response) for each damage state (see, for example, the second case study in Chapter 5). However, since this study is designed to inform decisions to invest in improved security, the added resolution for accommodating both target fragility and system response as separate variables is unnecessary. The fragilities are given in Table 4-12.

Table 4-12. Fragility of system response to different attack intensities

Consequence Dimension	Conditional Loss Distribution*					
	Low		Med		High	
	Mean	Standard Deviation	Mean	Standard Deviation	Mean	Standard Deviation
Fatalities	0.20	0.05	0.30	0.05	0.35	0.10
Repair Costs	0.60	0.10	0.70	0.15	0.80	0.10
Recuperation Time	0.25	0.05	0.50	0.10	0.75	0.15
Environmental Damage	0.10	0.02	0.30	0.10	0.50	0.10

*Note: Conditional loss distributions are assumed to follow a beta distribution

Assuming non-negative dependence (i.e., positive quadrant dependence) among the loss distributions for each consequence dimension, the probability density and cumulative distribution functions on loss for each relevant attack profile for the tank farm events is shown in Figure 4-7 for the bounding cases of independence and perfect positive dependence. According to Figure 4-7, loss is expressed as a fraction of the maximum potential loss for each consequence dimension, and as such is expressed over the unit interval. Given fixed upper and lower bounds on loss in conjunction with a mean and coefficient of variation, maximum entropy arguments insists on expressing the uncertainty in loss in terms of beta distributions (Kapur 1990). Together, the cumulative distribution functions assuming independence and perfectly dependent random variables represents the lower and upper bounds, respectively, on the cumulative distribution of the actual loss distribution (Ferson et al. 2004). Table 4-13 summarizes the moments of the resulting distribution on aggregate loss (or aggregate fragility) expressed as a fraction of the maximum potential aggregate loss valued in dollars. In this example, the aggregate maximum potential loss is \$332-million, which is obtained by summing the product of maximum potential loss and consequence conversion factor for each consequence dimension. From Figure 4-7 and Table 4-13, it is observed that there is no practical

difference between the aggregate loss distributions assuming independence and assuming perfect dependence, where at its worst the deviation between the mean of the expected conditional loss distribution for the “low” case is less than one percent. According to this observation, it is justifiable to assume one or the other dependency case, this choice being what is most computationally efficient. The remainder of the example, however, considers both dependency cases.

Table 4-13. Aggregate fragility of system response to different attack intensities

Dependence Assumption	Conditional Loss Distribution*					
	Low		Med		High	
	Mean	Standard Deviation	Mean	Standard Deviation	Mean	Standard Deviation
Independent	0.2260	0.0596	0.3291	0.0462	0.3891	0.0915
Perfectly Dependent	0.2246	0.0528	0.3295	0.0578	0.3893	0.1009

*Note: Conditional loss distributions are assumed to follow a beta distribution

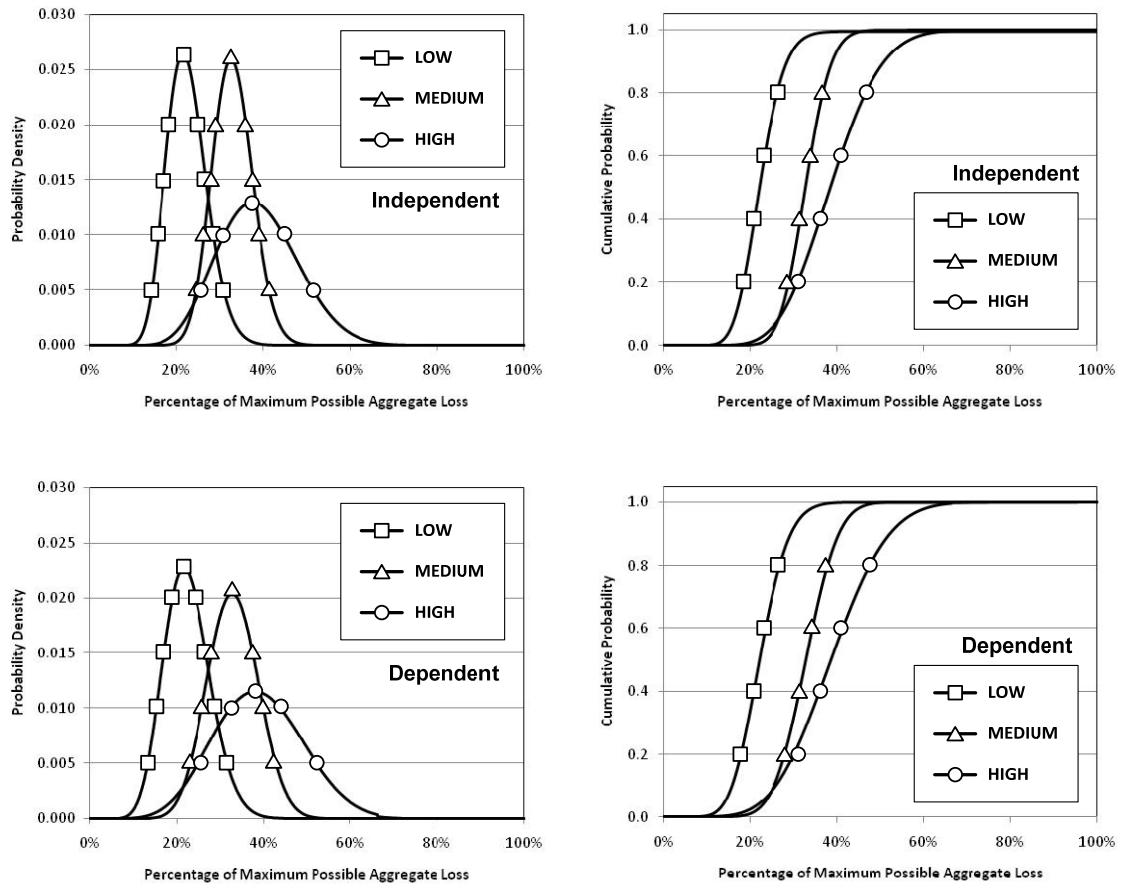


Figure 4-7. Probability density and cumulative distribution functions for loss

4.4.4. Response and Recovery

In this example, it is assumed that the facility does not possess indigenous response and recovery capabilities, and thus relies on external support to mitigate loss in the event of a successful attack. However, because the facility owner is unable to directly influence response and recovery capabilities controlled by external agencies, the worst case of no response and recovery capabilities is assumed. Expressed mathematically, the probability of actual loss given damage is taken as equal to the basis loss given damage, or:

$$\Pr(c | c_{P,m}) = 1 - I_R(c, c_{P,m}) = 1$$

This gives the expected loss given a successful attack (i.e., the so-called conditional risk) for each attack profile as described in Table 4-14.

Table 4-14. Expected aggregate loss give successful attack against the tank farm for both the independent and dependent case

Attack Profile	Conditional Risk (\$Million)	
	Independent	Dependent
Hand emplaced via forest	59.2	58.9
Hand emplaced via main access road	47.3	47.1
Hand emplaced via water	61.7	61.4
Ground vehicle via main access road	119.7	119.7
Manned aerial vehicle via air	73.7	73.4
Unmanned aerial vehicle via air	56.3	55.9

4.5. Threat Probability Assessment

It is assumed in this study that neither the facility owner nor security manager has any information that is useful for establishing actual adversary intent on the basis of actual motivations and capabilities, nor for identifying who the actual adversaries are that threaten the facility. To compensate for this missing threat information and to fulfill the requirements for analysis, this study assumes that, for each visible element, the adversary has perfect knowledge of facility loss potential and the effectiveness of protective security countermeasures. As described in Chapter 3, Section 3.5, these assumptions permit the use of the proportional attractiveness model under the mirror imaging case, where the adversary’s perceived probability of success is equal to the probability of the complement to security system effectiveness and the perceived gain from success is directly proportional to the defender’s assessed loss from failure. Under these

assumptions and further assuming perfect visibility of key elements and attack profiles and a perceived probability of capability acquisition for each attack mode as described in Table 4-15, a series of probability distributions describing the relative likeliness of alternative tank farm attack profiles can be constructed according to Eqs. 3-21 and 3-22 as shown in Figure 4-8 for bounding values of the bias parameter b (i.e., $b = 0$ and $b = \infty$) and one intermediate value (e.g., $b = 2$).

Despite missing information on actual adversary motivations and capability, this analysis assumes there is sufficient information to assess a probability of attack profile visibility (shown in Table 4-16) that accounts for adversary awareness or familiarity of alternative attack modes and facility intrusion paths. A comparison of the assessed probabilities of attack for each tank farm attack profile with and without considering visibility is shown in Figure 4-9 assuming a bias parameter of 2.

Table 4-15. Notional perceived probability of successful capability acquisition

Mode of Attack	Probability of Successful Capability Acquisition, P_C
Hand Emplaced	0.95
Ground Vehicle	0.85
Manned Aerial Vehicle	0.70
Unmanned Aerial Vehicle	0.50
Waterborne Vehicle	0.85

Table 4-16. Assessed visibility of tank farm attack profiles

Attack Profile	Profile Visibility
Hand emplaced via forest	1.0
Hand emplaced via main access road	0.8
Hand emplaced via water	0.7
Ground vehicle via main access road	1.0
Manned aerial vehicle via air	0.4
Unmanned aerial vehicle via air	0.6

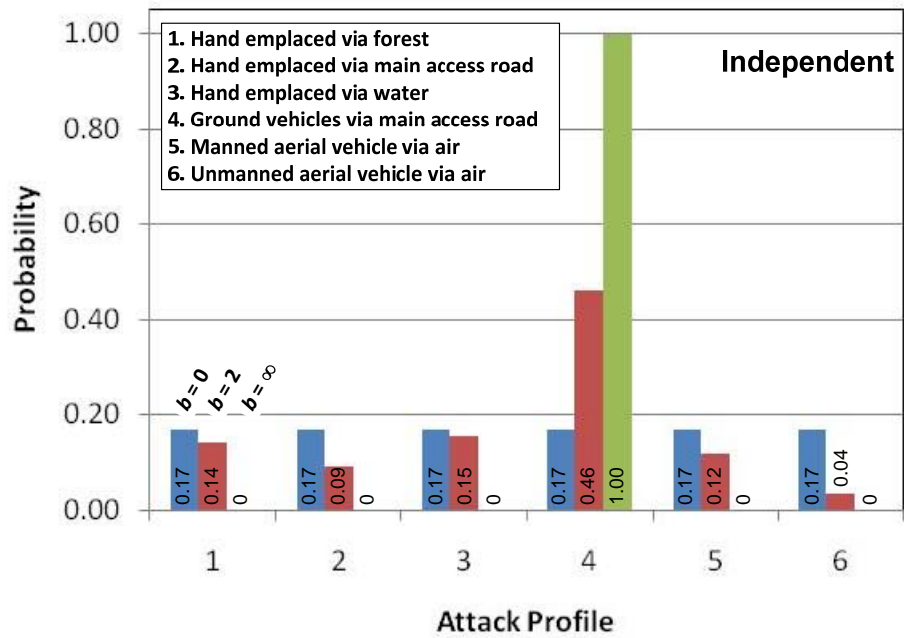


Figure 4-8. Threat probabilities without visibility for different values of b (for the independent and perfectly dependent cases)

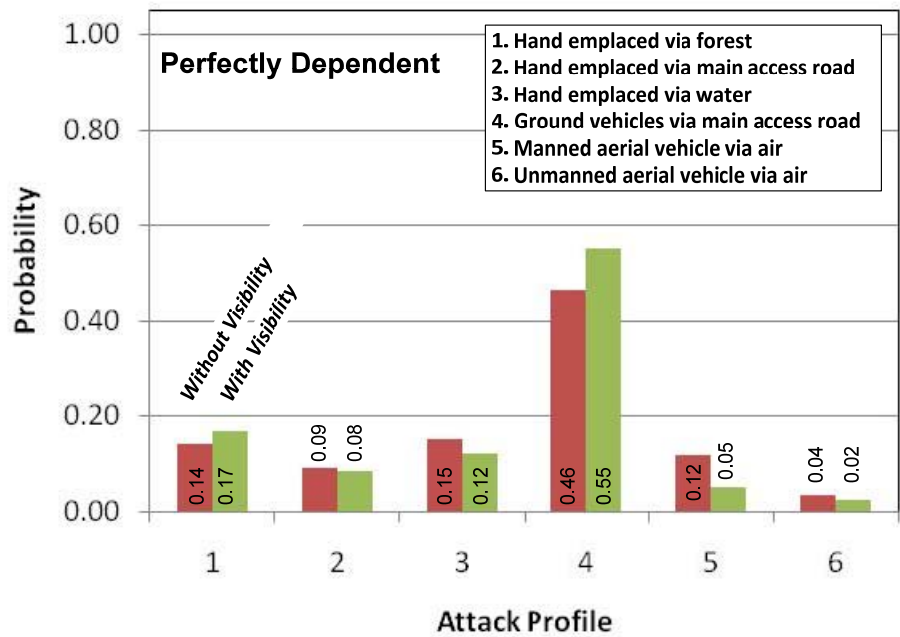
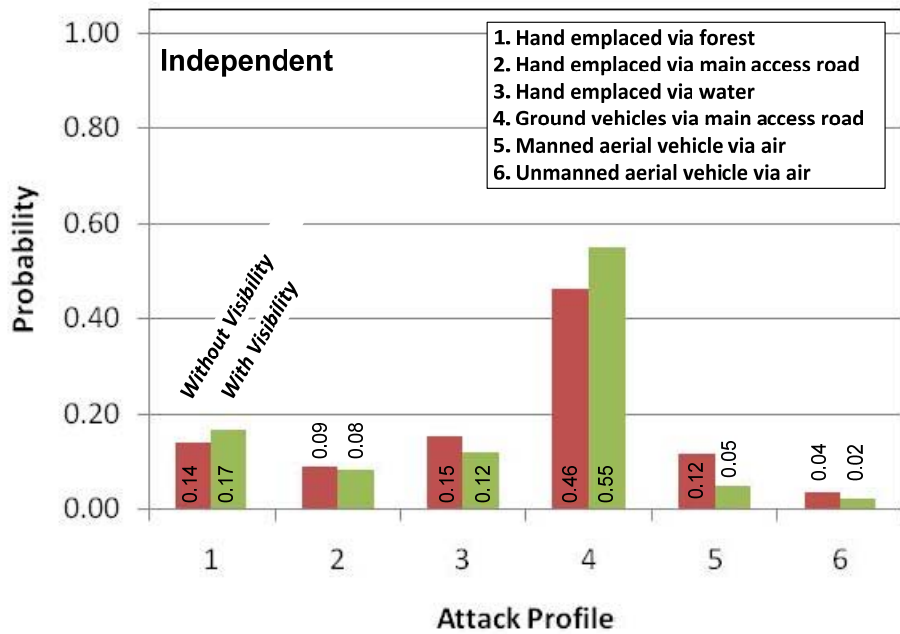


Figure 4-9. Probability distribution over attack profiles with and without considering visibility ($b=2$) (for the independent and perfectly dependent cases)

Accepting a bias parameter of 2 and the assessed visibilities of attack profiles, the aggregate conditional loss distribution given an attack against the tank farm considering all tank farm attack profiles, their overall vulnerability, and relative probabilities assessed according to the proportional attractiveness model is shown in Figure 4-10. The expected aggregate loss (fraction of aggregate maximum potential loss) given the occurrence of an attack against the tank farm is \$92.4-million (0.2783) and \$92.5-million (0.2787) for the independent and dependent case, respectively, which amounts to a discrepancy of less than two-tenths of one percent between the bounding dependency cases.

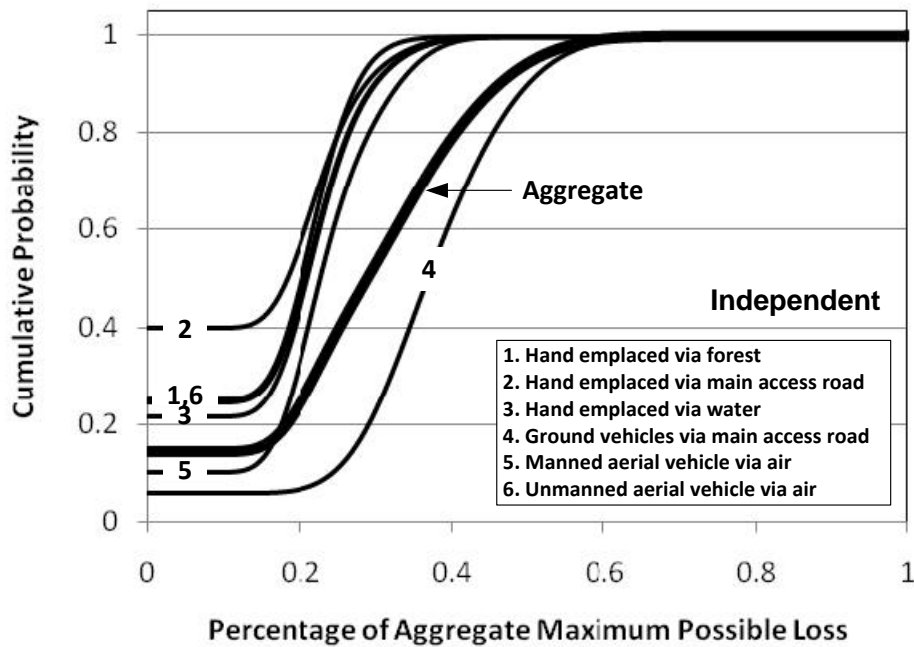


Figure 4-10. Individual and aggregate loss distributions for tank farm attack profiles (shown only for the independent case)

To obtain an estimate of overall facility risk with respect to explosive attacks, attack profiles centered on the main building must also be considered. Assuming perfect visibility of the tank farm and a visibility of 0.6 for the main building, the relative conditional probability of attack at an element and the probability density and cumulative distribution on aggregate loss given an attack at the facility can be obtained as shown in Figure 4-11 for both the independent and perfectly dependent cases. The resulting expected loss given attack is \$87.9-million and \$88.0-million per event for the independent and perfectly dependent cases, respectively.

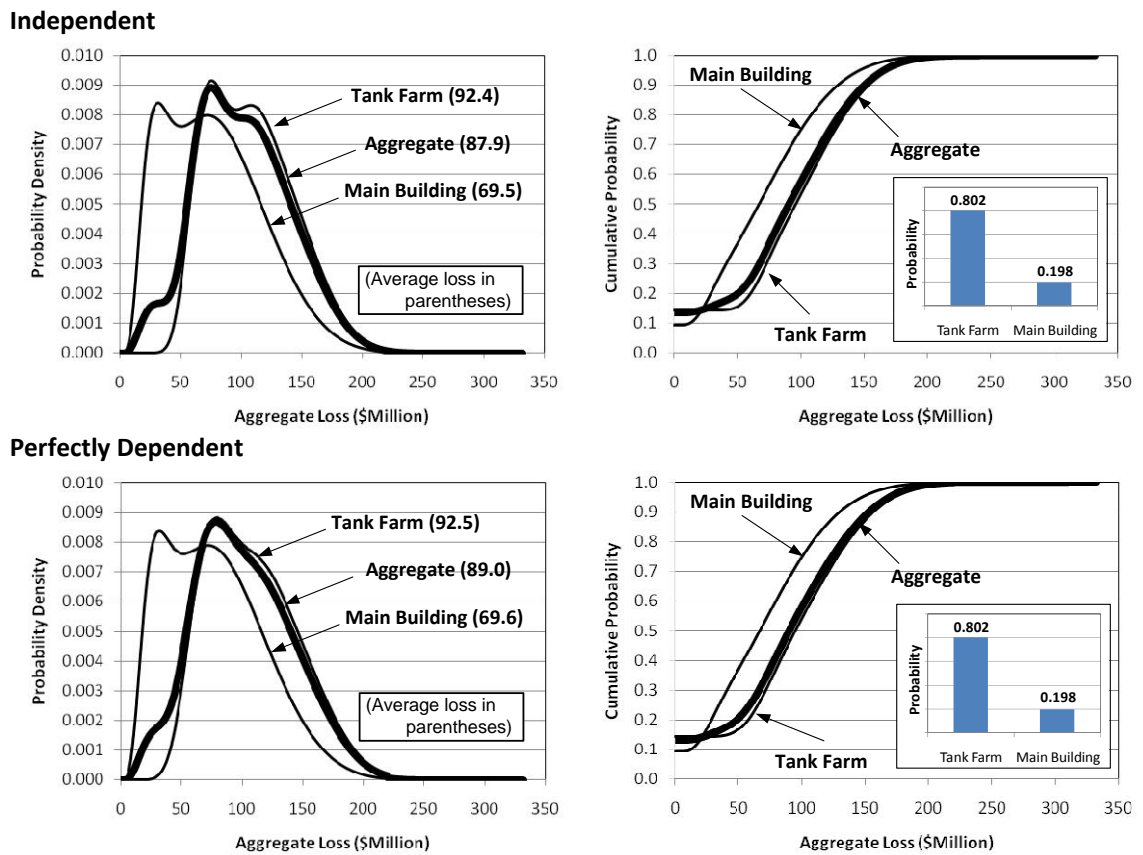


Figure 4-11. Individual and aggregate probability density and cumulative distribution functions considering tank farm and main building attack profiles

4.6. Actionable Risk Assessment

Assuming a subjectively assessed return period on attacks at the facility under study of once every twenty-five years with a coefficient of variation of 0.5 and that the loss between events is independent, a family of loss exceedance curves spanning a ten year planning horizon can be constructed as shown in Figure 4-12 using the techniques for loss accumulation described in Eqs. 3-32 and 3-33. In this figure, the 1st, 50th, and 99th percentiles are shown for only the independent case. Also shown in Figure 4-12 is the expected loss and coefficient of variation as a function of percentile distribution.

For the purposes of sensitivity analysis, the expected 10-year accumulated loss of the 99th percentile distribution will be considered (\$65.5-million). Since this analysis was designed to inform investment decisions to improve facility security, a sensitivity analysis was conducted on all controllable security variables (e.g., mean time to detect, probability of static detection, delay and response times, etc.) to produce actionable risk information that suggests where the decision maker should focus attention for decreasing risk. The scope of this sensitivity analysis considers only the impacts on risk internal to the facility due to changes in the performance variables, and does not account for corresponding redistribution of attack probabilities across a portfolio of assets. Table 4-17 summarizes the results of this sensitivity analysis using the fractional favorable change approach described in Eq. 3-34 with a fixed p value of 10%. According to this table, the initial focus for risk reduction should be on measures that improve security with respect to ground vehicle attacks since the assessed risk is most sensitive to these variables.

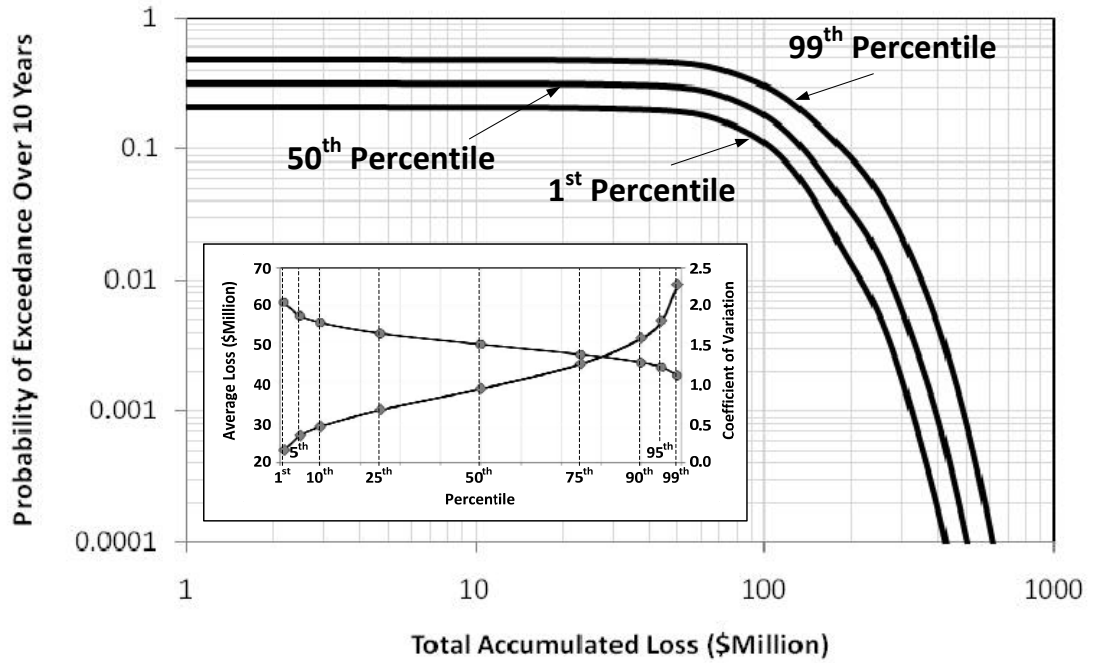


Figure 4-12. Percentile loss-exceedance curves for explosive attacks afflicting the chemical facility (shown only for the independent case)

Table 4-17. Summary of results from the sensitivity analysis

Parameter	Sensitivity (%)
Mean Time to Detect Zone 1 – HE	– 0.75
Mean Time to Detect Zone 2 – HE	0.00
Mean Time to Detect Zone 3 – HE	– 0.22
Mean Time to Detect Zone 4 – HE	– 0.16
Mean Time to Detect Zone 5 – AV	0.00
Mean Time to Detect Zone 1 – GV	+ 0.16
Mean Time to Detect Zone 2 – GV	+ 0.01
Probability of Neutralization – Hand Emplaced	– 1.51
Probability of Neutralization – Ground Vehicle	+ 3.78
Probability of Neutralization – Aerial Vehicle	0.00
Response Time – Mean	+ 8.51
Response Time – COV	– 1.11
Delay Time in Zone 1 – HE, Mean	– 0.96
Delay Time in Zone 2 – HE, Mean	– 0.12
Delay Time in Zone 3 – HE, Mean	– 0.16
Delay Time in Zone 4 – HE, Mean	– 0.12
Delay Time in Zone 1 – GV, Mean	+ 6.57
Delay Time in Zone 2 – GV, Mean	+ 1.53
Delay Time in Zone 5 – AV, Mean	+ 0.13
Delay Time in Zone 1 – HE, COV	+ 0.14
Delay Time in Zone 2 – HE, COV	+ 0.10
Delay Time in Zone 3 – HE, COV	+ 0.14
Delay Time in Zone 4 – HE, COV	+ 0.14
Delay Time in Zone 1 – GV, COV	+ 0.30
Delay Time in Zone 2 – GV, COV	+ 0.17
Delay Time in Zone 5 – AV, COV	+ 0.13
Probability of Passive Detection in Zone 1 – HE	– 2.12
Probability of Passive Detection in Zone 2 – HE	+ 0.12
Probability of Passive Detection in Zone 3 – HE	– 2.06
Probability of Passive Detection in Zone 4 – HE	– 0.68
Probability of Passive Detection in Zone 1 – GV	+ 3.25
Probability of Passive Detection in Zone 2 – GV	+ 0.13
Probability of Passive Detection in Zone 5 – AV	+ 0.13

4.7. Benefit-Cost Analysis

Assuming that the total risk exposure for this facility exceeds the risk tolerance of the facility owner or security manager, several options may be considered for risk

reduction such as those described in Table 4-18, where the cost is characterized by a lognormal distribution with the actual mean and coefficient of variation shown.

Leveraging the CAPRA approach used for baseline assessment as implemented in the previous sections, a cumulative probability distribution on benefit for each option can be constructed such as is shown in Figure 4-13. As a conservative assumption, the annual rate of occurrence is assumed to be constant before and after implementation of the risk mitigation measures, though in practice the risk reduction may be augmented by a decrease in the annual recurrence rate. According to the table in Figure 4-13, strategy S2 has the largest expected benefit-cost ratio at 1.24, followed by strategy S1 with an expected ratio of 1.07 and strategy S3 with an expected ratio of 1.01. However, according to Figure 4-14 which plots probability of exceeding a given benefit cost ratio as a function of this ratio, the probability of exceeding a benefit cost ratio between one and three is greatest for strategy S1 despite having a lower expected benefit cost ratio.

Additional information on whether the needed resources are available to implement strategy S1, whether this option meets risk reduction objectives, and the nature of impacts this option will have on future options is required prior to making a final decision. For example, though strategy S1 has the highest probability of exceeding a benefit-cost ratio of 1, an average price tag of \$4-million with significant uncertainty to implement this option may exceed the decision maker's budget for security improvements, which might force the decision maker to consider the next best option due to its lower cost. Moreover, a more complete risk picture considering a full-suite of anthropic and naturally occurring events is necessary to fully evaluate the benefits of

proposed security investments, though it can be reasoned that accounting for these other initiating events will only serve to improve the business case for any alternative.

Table 4-18. Alternative risk mitigation options

Risk Mitigation Option	Estimated Effect	10-Year Cost (COV)
S1: Improve passive detection capabilities of ground vehicle explosives in security zone 3 with increased ability to neutralize ground vehicle attacks	Increase passive probability of detection from 0.2 to 0.75 in security zone 3; probability of neutralization increased from 0.2 to 0.5	\$4-million (0.25)
S2: Decrease response time by hiring new guards and positioning them at strategic locations	Decrease response time from 60-seconds to 30-seconds, keeping COV constant	\$2-million (0.10)
S3: Increase delay time in security zone 2 for hand emplaced and ground vehicle attacks	Increase delay time by 100% in security zone 2 for hand emplaced (to 60-seconds) and by 200% for ground vehicle attacks (to 30 seconds)	\$1-million (0.15)

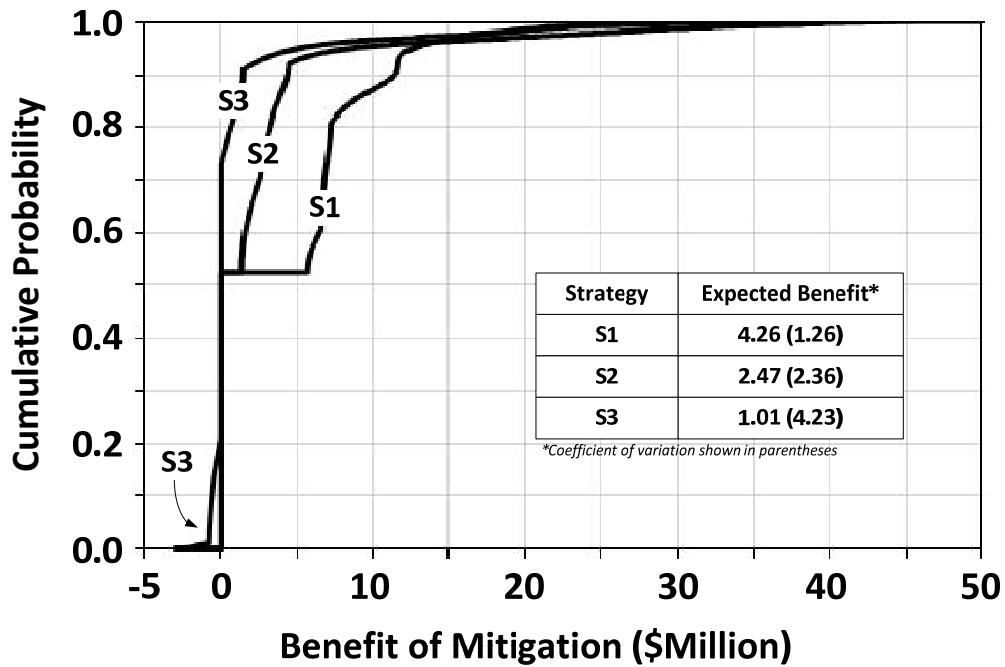


Figure 4-13. Cumulative probability distributions for accumulated benefit associated with each risk mitigation action tabulated expected benefits

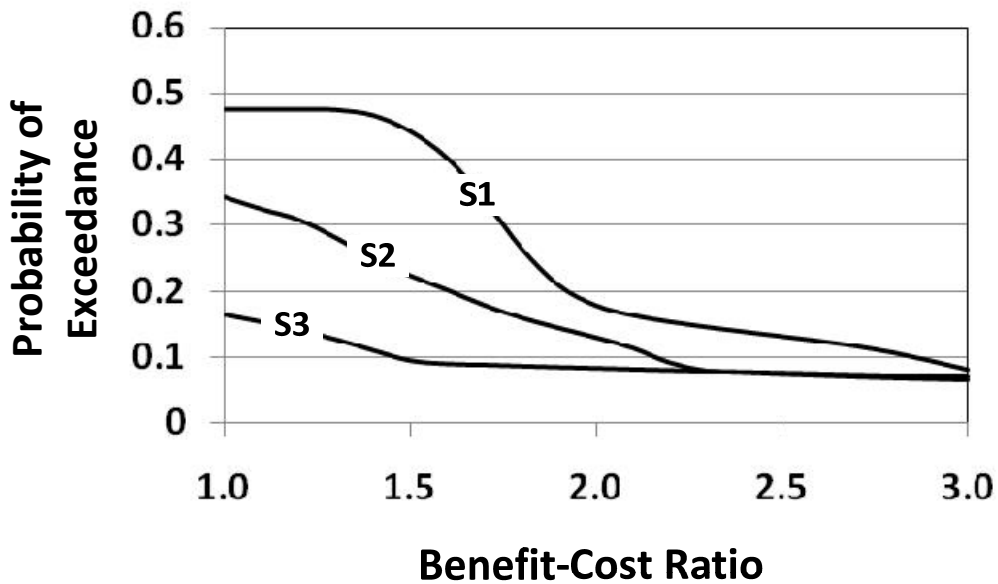


Figure 4-14. Probability of exceedance on benefit-cost ratios for each risk mitigation option

4.8. Discussion

This case study focused on applying the CAPRA methodology developed in Chapter 3 to produce actionable asset-level risk information for a notional chemical facility exposed to the threat of an explosive attack and to evaluate the cost-effectiveness of alternative options for mitigating risk through improved countermeasures. The inputs to the CAPRA methodology in this example were strictly probabilistic in nature, and consequently the outputs assumed the form of a standard family of loss-exceedance curves.

The scenario identification phase leveraged a new technique for scenario identification and screening based on the CARVER targeting (and vulnerability assessment) methodology and the FMECA approach. This approach identified initiating events based on the inherent susceptibility of key elements, and scored each initiating event according to the six CARVER criteria. These scores were then aggregated using a revised CARVER formula that expresses the aggregate score in terms of an order of magnitude estimate of risk. Given these order of magnitude estimates, only those initiating events for which the estimate exceeds some minimum threshold were screened-in for further analysis, i.e., those initiating events for which the relative risk priority number was one or greater.

The overall vulnerability assessment phase leveraged established techniques from systems reliability analysis to study the performance of security systems under the stress imposed on it by an adversary. While some of the tools used to make sense of security system effectiveness were leveraged from previous studies, this research extended these models to include consideration of active detection measures whose performance was

measured in terms of a mean time to detect. However, this analysis implicitly assumes that there is no capability beyond what the facility possesses to defeat the adversary once an attack is commenced. That is, this analysis does not consider the contribution to overall security from external countermeasures, to include local police and other security resources. The inclusion of these factors in terms of a *probability of interdiction* prior to an adversary's arrival at the facility fence line insists on analytic collaboration between the asset owner, local response forces, and so on. Absent this level of collaboration and information sharing insists that conservative assumptions be made, which though not necessarily bad, may result in an overstatement of the actual risk reduction achieved from different risk mitigation proposals.

In the absence of statistical information to construct empirical distributions for the loss parameters or infer a probability of adversary success, this case study leveraged knowledge of distribution parameters (e.g., mean, coefficient of variation, bounds) obtained, for instance, from expert elicitation (though no source was specified in this example) to support expression of uncertainty by maximum entropy distributions. In other cases for which no information was available to render a judgment of likeliness, such as for the effectiveness of external response and recovery measures, conservative values (i.e., a value of one for vulnerability parameters or zero for effectiveness parameters) were employed to arrive at conservative estimates of risk. Again, to arrive at such estimates of response and recovery capabilities insists on dialogue between the asset owner and local response and recovery forces. Moreover, this analysis demonstrated that no significant assumptions on the dependency are necessary for different consequence

dimensions save for omitting negative dependencies; it was shown that the results varied little depending on whether independence or perfect dependence was assumed.

Overall, while this analysis focused on informing decisions to improve security to reduce risk, the study acknowledged all contributors to vulnerability. However, this analysis was rightfully tailored to meet the specific decision requirements of the decision maker, which in this study centered on evaluating security system performance and assessing the cost-effectiveness of alternative strategies for decreasing probability of success. Accordingly, while it was acknowledged that the fragility of target elements and the intrinsic susceptibility of the asset to different levels of target damage are separate parameters that contribute to overall vulnerability, it was appropriate to combine the two to arrive at an expression of “system fragility,” or the probability of different degrees of loss given that the adversary successfully imparts its load on the target. Though not explicitly described in the discussion of overall vulnerability in Chapter 3, Section 3.5, system fragility is an element of overall vulnerability that crosses the largely artificial boundary between protection and response vulnerabilities.

The threat probability assessment phase demonstrated that meaningful attack probabilities can be obtained by assuming rational adversaries with perceptions of opportunity that mirror defender assessments of risk. As demonstrated in the analysis of mitigation strategies, the CAPRA methodology is sensitive to changes in adversary perceptions of risk and reward due to changes in the facility security posture. However, since this analysis focused on a single asset in isolation, it could not account for a shift in perceived attractiveness away from the facility itself and toward other facilities. Had some of the probability of attack at the asset been allowed to move away toward other

assets, the assessed reduction in risk would be greater was assessed without considering this behavior. Consequently, all else being equal, the assessed benefit of a consequence mitigation action might, in actuality, be less than would actually be realized when implemented. Again, with improved collaboration with other assets and higher-level decision makers, this model could easily accommodate this level of analysis.

The threat probability assessment also demonstrated how the visibility of key elements and intrusion paths can be integrated to analysis to arrive at threat probabilities that are considerate of the fact that not all assets are necessarily visible. It is a fairly straightforward task to extend this model to consider uncertainties in other adversary dimensions; for example, variations in adversary behavior and attractiveness attitudes can be accommodated through a probability distribution constructed over a finite (or perhaps infinite) set of representative attractiveness attitudes and preferences. Similarly, for a given adversary with defined attitude, a probability distribution can be constructed over the bias parameter b . In the end, the resulting probability of attack for each asset, initiating event type, and attack profile obtained in this manner could more effectively leverage intelligence resources to estimate threat probabilities for operational and strategic resource allocation decisions not in terms of actual adversary activities, but in terms of assessed adversary preferences, knowledge, and attitudes.

In terms of providing actionable risk information for decision makers, this case study also demonstrated how to produce actionable risk information via sensitivity analysis using a new approach to sensitivity analysis based that examines how a fractional favorable change in model parameters reduces risk, which as a special case reduces to the risk reduction worth importance factor described by Modarres et al. 1999.

The results from a sensitivity analysis combined with a baseline expression of risk communicates not only the magnitude of the risks afflicting decision makers, but also offers insight on where to focus attention to achieve cost-effective risk reduction. Given a set of risk mitigation options, this case study also demonstrated that while the expected benefit-cost ratio for a given risk mitigation strategy may appear superior, the probability of exceeding a given benefit-cost ratio may not be superior relative to other strategies with lower expected benefit-cost ratios. It is thus important to take into account the variability in benefit and cost when selecting one or more investments options from among a set of alternatives.

Future lines of research that would augment the analysis described in this Chapter include leverage human-reliability based models of guard performance in relation to detection, response, and neutralization (e.g., force on force models) capabilities. For example, the recent work in the area of human reliability analysis described by Chang and Mosleh (2007) can be explored, in addition to work in the area of agent based simulation of adversary behavior. Moreover, this analysis could readily consider multiple simultaneous attacks against different elements, but the assessment would then have to consider the synergies and inefficiencies of multiple coordinated attacks. Also, since this analysis was asset centric, it does not consider the contribution to overall risk stemming from incidents afflicting external assets for which the current asset is dependent. Finally, more analysis is needed to select an appropriate value for the bias parameter to capture the true preferences of adversaries, which combined with the need to understand adversary attitudes (and utility functions) embodies the need to better understand attacker behaviors.

Chapter 5. Case study – Regional Risk Analysis

5.1. Problem Description

This chapter applies the CAPRA framework developed in Chapter 3 to the problem of allocating financial resources to improve one or more capabilities possessed by a region to prevent, respond to, and recover from adverse initiating events. The point of view of this analysis is regional leadership responsible for maintaining critical services and protecting the health and safety of its citizens. The decision *variables* in this study are the 37 target capabilities defined by DHS and as shown in Table 5-1 (DHS 2006c; DHS 2007) plus additional variables that characterize regional security capabilities. The *effects* or *outcomes* of concern to the decision makers include service disruption and loss of life. The *sources* of risk in this case study are limited to the phenomenologies associated with an improvised explosive device (IED) attack against selected infrastructure targets; the IED scenario is number 12 (i.e., NPS-12) among the 15 *National Planning Scenarios* shown in Figure 2-2 (US Department of Homeland Security 2006b). The *targets* of the risk in this case study are five infrastructure assets situated in the region as illustrated in Figure 5-1. The relevance of each target capability to one or more variables of the CAPRA risk model are denoted by an “X” in Table 5-2. Note that some of the capabilities, while important in the general case, are not applicable to the given problem due to its focus being limited to IED attacks (e.g., epidemiological surveillance and investigation).

The specific region under study is a large city with a population of 500,000 people and a gross regional product of \$100-billion. Of particular concern to regional

decision makers are the five infrastructure assets shown in Figure 5-1, all of which are owned by private (e.g., non-governmental) enterprises. As part of their annual grant application for federal resources to improve security and resilience, the task of the regional decision makers is to identify and evaluate alternative investment strategies for mitigating the risk associated with an adverse IED attack against one or more of these five infrastructure assets. The scope of this study focuses on two dimensions of loss: fatalities resulting from the aggregate effects of the attack and ensuing damage (measured in fatality equivalents) and disruption of essential services (measured in units of time-%). Note that since the scope of the analysis is on regional decision makers, property damage to privately-owned assets is assumed to be outside the scope of regional decision maker concerns.

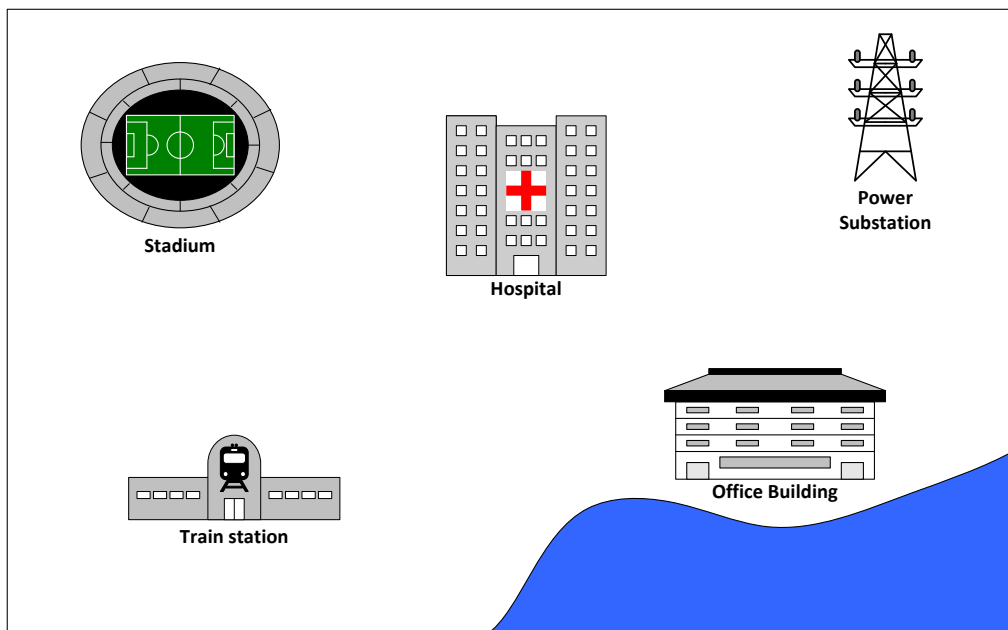


Figure 5-1. Five infrastructure assets in the study region

The goal of this case study is to produce actionable risk information that informs regional decision makers on where to focus their attention for cost-effective risk reduction. The main challenges in this case study are threefold: (1) mapping the performance of a subset of the 37 capabilities to one or more elements of the CAPRA risk equation developed in Section 3, where it is generally assumed that the relationship between these capabilities and risk is highly nonlinear and lacks explicit functional representation; (2) consideration of physical, geographical, cyber, and logical interdependencies among assets within the portfolio; and (3) producing risk results that are faithful to the limited available information and data collection resources.

The proposed implementation of the CAPRA framework for regional risk analysis in light of regional capabilities is illustrated in Figure 5-2. Section 5.2 describes the nature and the characteristics of the security hazards considered in this analysis. Section 5.3 describes the means with which each of the five infrastructures are characterized to support regional analysis, to include an assessment of maximum loss potential, basis loss for each damage state, fragility of the asset to different hazard intensities, and security system performance. Section 5.4 describes the means of characterizing regional capabilities, to include approximate reasoning models that link regional capability variables to ability to reduce basis loss and regional security performance. In addition, Section 5.4 describes a simple first-order interdependency analysis technique used for estimating the total impact due to service disruption in light of portfolio interdependencies. The remaining sections synthesize regional and asset information to produce risk profiles expressed as a family of pignistic probability distributions and sensitivities of key distribution parameters to guide resource allocation decisions.

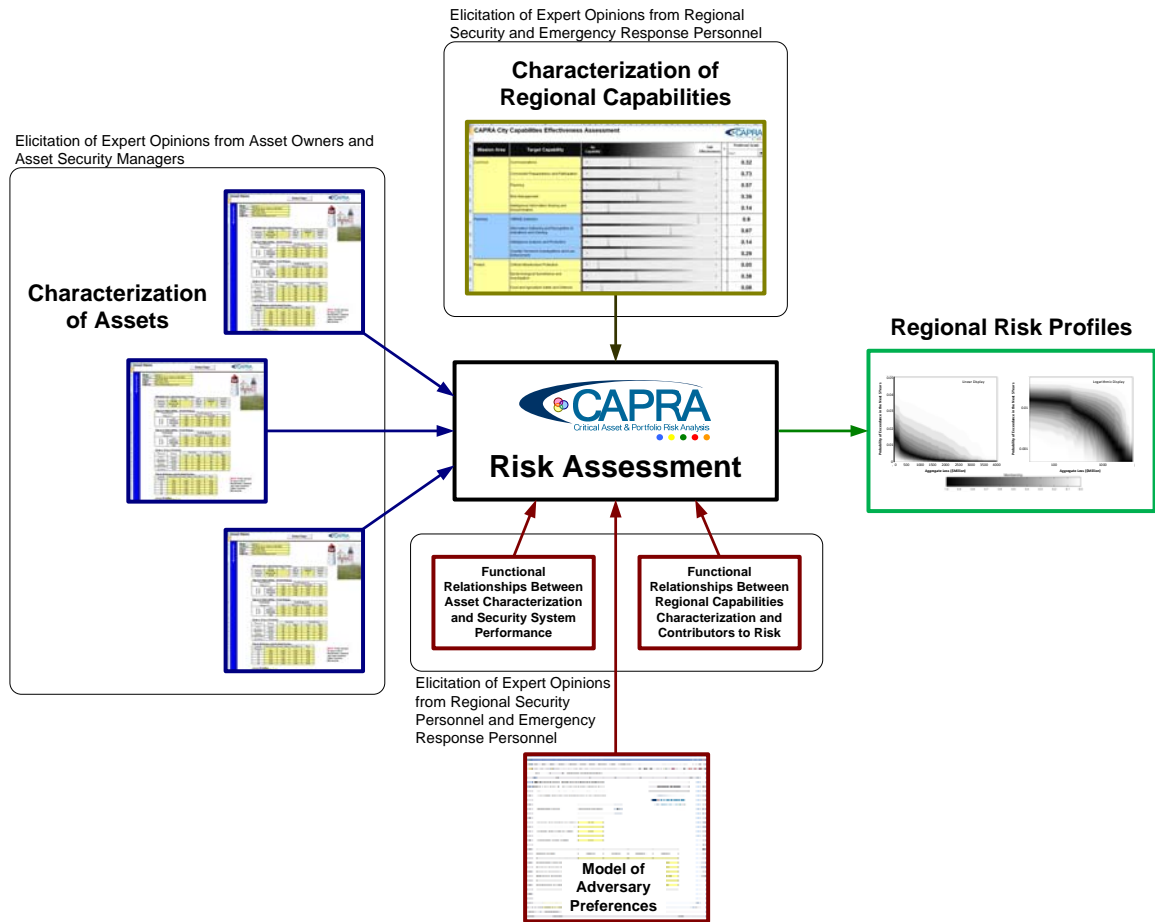


Figure 5-2. Implementation of CAPRA for regional risk analysis

Table 5-1. Target Capabilities List (DHS 2006c; DHS 2007)

Category	Label	Capability	Desired Outcome at Full Effectiveness
Common Mission Area	Y ₁	Communications	A continuous flow of communication is maintained as needed among multi-jurisdictional and multi-disciplinary emergency responders, command posts, agencies, and government officials for the duration of the emergency response operation in compliance with the National Incident Management System (NIMS). In order to accomplish that, the jurisdiction has a continuity of operations plan for public safety communications including the consideration of critical components, networks, support systems, personnel, and an appropriate level of redundant communications systems in the event of any emergency.
	Y ₂	Community Preparedness and Participation	There is a structure and a process for ongoing collaboration between government and nongovernmental organizations at all levels; volunteers and nongovernmental resources are incorporated in plans and exercises; the public is educated, trained, and aware; citizens participate in volunteer programs and provide surge capacity support; nongovernmental resources are managed effectively in disasters; and there is a process to evaluate progress.
	Y ₃	Planning	Plans incorporate an accurate threat analysis and risk assessment and ensure that capabilities required to prevent, protect against, respond to, and recover from all-hazards events are available when and where they are needed. Plans are vertically and horizontally integrated with appropriate departments, agencies, and jurisdictions. Where appropriate, emergency plans incorporate a mechanism for requesting State and Federal assistance and include an clearly delineated process for seeking and requesting assistance from appropriate agencies.
	Y ₄	Risk Management	Federal, state, local, tribal, territorial and private sector entities identify and assess risks, prioritize and select appropriate protection, prevention, and mitigation solutions based on reduction of risk, monitor the outcomes of allocation decisions, and undertake corrective actions. Additionally, Risk Management is integrated as a planning construct for effective prioritization and oversight of all homeland security investments.
	Y ₅	Intelligence/ Information Sharing and Dissemination	Effective and timely sharing of information and intelligence occurs across Federal, State, local, tribal, territorial, regional, and private sector entities to achieve a coordinated awareness of, prevention of, protection against, and response to threatened or actual domestic terrorist attack, major disaster, or other emergency.
Planning Mission Area	Y ₆	CBRNE Detection	Chemical, biological, radiological, nuclear, and/or explosive (CBRNE) materials are rapidly detected and characterized at borders and ports of entry, critical locations, events, and incidents.
	Y ₇	Information Gathering and Recognition of Indications and Warning	Locally generated threat and other criminal and/or terrorism-related information is identified, gathered, entered into appropriate data/retrieval system, and provided to appropriate analysis centers.

Table 5-1. (continued)

Category	Label	Capability	Desired Outcome at Full Effectiveness
Planning Mission Area (Continued)	Y ₈	Intelligence Analysis and Production	Timely, accurate, and actionable intelligence/information products are produced in support of prevention, awareness, deterrence, response, and continuity planning operations.
	Y ₉	Counter-Terror Investigations and Law Enforcement	Suspects involved in criminal activities related to homeland security are successfully deterred, detected, disrupted, investigated, and apprehended. All counterterrorism-related cases are aggressively prosecuted.
Protect Mission Area	Y ₁₀	Critical Infrastructure Protection	The risk of, vulnerability of, and consequence of an attack on critical infrastructure are reduced through the identification of critical infrastructure; conduct, documentation, and standardization of risk assessments; prioritization of assets; decisions regarding protective and preventative programs; and implementation of protective and preventative response plans.
	Y ₁₁	Epidemiological Surveillance and Investigation	Potential exposure to disease is identified rapidly by determining exposure and mode of transmission and agent; interrupting transmission to contain the spread of the event; and reducing number of cases. Confirmed cases are reported immediately to all relevant public health, food, regulatory, and law enforcement agencies. Suspected cases are investigated promptly, reported to relevant public health authorities, food regulatory, environmental regulatory, and law enforcement agencies. Suspected cases are investigated promptly, reported to relevant public health authorities, and accurately confirmed to ensure appropriate preventive or curative countermeasures are implemented. An outbreak is defined and characterized; new suspect cases are identified and characterized based on case definitions on an ongoing basis; relevant clinical specimens are obtained and transported for confirmatory lab testing; the source of exposure is tracked; methods of transmission identified; and effective mitigation measures are communicated to the public, providers, and relevant agencies, as appropriate.
	Y ₁₂	Food and Agriculture Safety and Defense	Threats to food and agriculture safety are prevented, mitigated, and eradicated; affected products are disposed of; affected facilities are decontaminated; public and plant health are protected; notification of the event and instructions of appropriate actions are effectively communicated with all stakeholders; trade in agricultural products is restored safely; and confidence in the U.S. food supply is maintained.
	Y ₁₃	Public Health Laboratory Testing	Chemical, radiological, and biological agents causing, or having the potential to cause, widespread illness or death are rapidly detected and accurately identified by the public health laboratory within the jurisdiction or through network collaboration with other appropriate Federal, State, and local laboratories. The public health laboratory, working in close partnership with public health epidemiology, environmental health, law enforcement, agriculture, and veterinary officials, hospitals, and other appropriate agencies, produces timely and accurate data to support ongoing public health investigations and the implementation of appropriate preventive or curative countermeasures.

Table 5-1. (continued)

Category	Label	Capability	Desired Outcome at Full Effectiveness
Respond Mission Area	Y ₁₄	Animal Disease Emergency Support	Foreign animal disease is prevented from entering the United States by protecting the related critical infrastructure and key assets. In the event of an incident, animal disease is detected as early as possible, exposure of livestock to foreign diseases is reduced, immediate and humane actions to eradicate the outbreak are implemented, public and animal health and the environment are protected, continuity of agriculture and related business is safely maintained and/or restored, and economic damage is minimized. Trade in agricultural products and domestic and international confidence in the U.S. food supply are safely maintained or restored.
	Y ₁₅	Citizen Evacuation and Shelter-In-Place	Affected and at-risk populations (and companion animals to the extent necessary to save human lives) are safely sheltered-in-place or evacuated to safe refuge areas.
	Y ₁₆	Critical Resource Logistics and Distribution	Critical resources are available to incident managers and emergency responders upon request for proper distribution and to aid disaster victims in a cost-effective and timely manner.
	Y ₁₇	Emergency Operations Center Management	The event is effectively managed through multi-agency coordination for a pre-planned or no-notice event.
	Y ₁₈	Emergency Public Information and Warning	Government agencies and public and private sector entities receive and transmit coordinated, prompt, useful, and reliable information regarding threats to their health, safety, and property through clear, consistent information delivery systems. This information is updated regularly and outlines protective measures that can be taken by individuals and their communities.
	Y ₁₉	Environmental Health	After the primary event, disease and injury are prevented through the quick identification of associated environmental hazards, including exposure to infectious diseases that are secondary to the primary event as well as secondary transmission modes. The at-risk population (i.e., exposed or potentially exposed) receives the appropriate countermeasures, including treatment or protection, in a timely manner. The rebuilding of the public health infrastructure, removal of environmental hazards, and appropriate decontamination of the environment enable the safe re-entry and re-occupancy of the impacted area. Continued monitoring occurs throughout the recovery process in order to identify hazards and reduce exposure.
	Y ₂₀	Explosive Device Response Operations	Threat assessments are conducted, the explosive and/or hazardous devices are rendered safe, and the area is cleared of hazards. Measures are implemented in the following priority order: ensure public safety; safeguard the officers on the scene (including the bomb technician); collect and preserve evidence; protect and preserve public and private property; and restore public services.

Table 5-1. (continued)

Category	Label	Capability	Desired Outcome at Full Effectiveness
Respond Mission Area (Continued)	Y ₂₁	Fatality Management	Complete documentation and recovery of human remains and items of evidence (except in cases where the health risks posed to personnel outweigh the benefits of recovery of remains). Remains receive surface decontamination (if indicated) and, unless catastrophic circumstances dictate otherwise, are examined, identified, and released to the next-of-kin's funeral home with a complete certified death certificate. Reports of missing persons and ante mortem data are efficiently collected. Victims' family members receive updated information prior to the media release. All hazardous material regulations are reviewed and any restrictions on the transportation and disposition of remains are made clear by those with the authority and responsibility to establish the standards. Law enforcement agencies are given all information needed to investigate and prosecute the case successfully. Families are provided incident-specific support services.
	Y ₂₂	Fire Incident Response Support	Dispatch and safe arrival of the initial fire suppression resources occur within jurisdictional response time objectives. The first unit to arrive initiated the Incident Command System (ICS), assesses the incident scene, communicates the situation, and requests appropriate resources including any necessary mutual aid or cross-discipline support. Firefighting activities are conducted safely and fire hazards are contained, controlled, extinguished, and investigated, and the incident is managed in accordance with emergency response plans and procedures.
	Y ₂₃	Isolation and Quarantine	Individuals who are ill, exposed, or likely to be exposed are separated, movement is restricted, basic necessities of life are available, and their health is monitored in order to limit the spread of a newly introduced contagious disease (e.g., pandemic influenza). Legal authority for those measures is clearly defined and communicated to all responding agencies and the public. Logistical support is provided to maintain measures until danger of contagion has elapsed.
	Y ₂₄	Mass Care (Sheltering, Feeding, and Related Services)	Mass care services, including sheltering, feeding, and bulk distribution, are rapidly provided for the population and companion animals within the affected area.
	Y ₂₅	Mass Prophylaxis	Appropriate drug prophylaxis and vaccination strategies are implemented in a timely manner upon the onset of an event to prevent the development of disease in exposed individuals. Public information strategies include recommendations on specific actions individuals can take to protect their family, friends, and themselves.
	Y ₂₆	Medical Supplies Management and Distribution	Critical medical supplies and equipment are appropriately secured, managed, distributed, and restocked in a timeframe appropriate to the incident.
	Y ₂₇	Medical Surge	Injured or ill from the event are rapidly and appropriately cared for. Continuity of care is maintained for non-incident related illness or injury.

Table 5-1. (continued)

Category	Label	Capability	Desired Outcome at Full Effectiveness
Respond Mission Area (continued)	Y ₂₈	Onsite Incident Management	The event is managed safely, effectively, and efficiently through the common framework of the ICS.
	Y ₂₉	Emergency Public Safety and Security Response	The incident scene is assessed and secured; access is controlled; security support is provided to other response operations (and related critical locations, facilities, and resources); emergency public information is provided while protecting first responders and mitigating any further public risks; and any crime/ incident scene preservation issues are addressed.
	Y ₃₀	Responder Safety and Health	No illness or injury to any first responder, first receiver, medical facility staff member, or other skilled support personnel as a result of preventable exposure to secondary trauma, chemical/radiological release, infectious disease, or physical and emotional stress after the initial incident or during decontamination and incident follow-up.
	Y ₃₁	Emergency Triage and Pre-Hospital Treatment	Emergency Medical Services (EMS) resources are effectively and appropriately dispatched and provide pre-hospital triage, treatment, transport, tracking of patients, and documentation of care appropriate for the incident, while maintaining the capabilities of the EMS system for continued operations.
	Y ₃₂	Search and Rescue (Land-Rescue)	The greatest number of victims (humans and, to the extent that no humans remained endangered, animals) are rescued and transferred to medical or mass care capabilities, in the shortest amount of time, while maintaining rescuer safety.
	Y ₃₃	Volunteer Management and Donations	The positive effect of using unaffiliated volunteers and unsolicited donations is maximized and does not hinder response and recovery activities.
	Y ₃₄	WMD/Hazardous Materials Response and Decontamination	Any hazardous materials release is rapidly identified and mitigated; victims exposed to the hazards are rescued, decontaminated, and treated; the impact of the release is limited; and responders and at-risk populations are effectively protected.
	Recover Mission Area	Y ₃₅	Economic and Community Recovery
Y ₃₆		Restoration of Lifelines	Lifelines to undertake sustainable emergency response and recovery activities are established.
Y ₃₇		Structural Damage Assessment	Accurate situation needs and damage assessments occur. The full range of engineering, building inspection, and enforcement services are implemented, managed, and coordinated in a way that maximizes the use of resources, aids emergency response, and implements recovery operations. Mitigation projects to lessen the impact of similar future events are identified and prioritized.

Table 5-2. Relevant of capabilities to CAPRA model variables

Category	Label	Capability	Fatalities	Threat Occurrence
Common Mission Area	Y ₁	Communications	X	-
	Y ₂	Community Preparedness and Participation	X	X
	Y ₃	Planning	X	-
	Y ₄	Risk Management	-	-
	Y ₅	Intelligence/ Information Sharing and Dissemination	-	X
Planning Mission Area	Y ₆	CBRNE Detection	-	X
	Y ₇	Information Gathering and Recognition of Indications and Warning	-	X
	Y ₈	Intelligence Analysis and Production	-	X
	Y ₉	Counter-Terror Investigations and Law Enforcement	-	X
Protect Mission Area	Y ₁₀	Critical Infrastructure Protection	-	-
	Y ₁₁	Epidemiological Surveillance and Investigation	-	-
	Y ₁₂	Food and Agriculture Safety and Defense	-	-
	Y ₁₃	Public Health Laboratory Testing	-	-
Respond Mission Area	Y ₁₄	Animal Disease Emergency Support	-	-
	Y ₁₅	Citizen Evacuation and Shelter-In-Place	X	-
	Y ₁₆	Critical Resource Logistics and Distribution	X	-
	Y ₁₇	Emergency Operations Center Management	X	-
	Y ₁₈	Emergency Public Information and Warning	X	-
	Y ₁₉	Environmental Health	-	-
	Y ₂₀	Explosive Device Response Operations	-	-
	Y ₂₁	Fatality Management	X	-
	Y ₂₂	Fire Incident Response Support	X	-
	Y ₂₃	Isolation and Quarantine	-	-
	Y ₂₄	Mass Care (Sheltering, Feeding, and Related Services)	X	-
	Y ₂₅	Mass Prophylaxis	-	-
	Y ₂₆	Medical Supplies Management and Distribution	X	-
	Y ₂₇	Medical Surge	X	-
	Y ₂₈	Onsite Incident Management	X	-
	Y ₂₉	Emergency Public Safety and Security Response	X	-
	Y ₃₀	Responder Safety and Health	X	-
Y ₃₁	Emergency Triage and Pre-Hospital Treatment	X	-	
Y ₃₂	Search and Rescue (Land-Rescue)	X	-	
Y ₃₃	Volunteer Management and Donations	-	-	
Y ₃₄	WMD/Hazardous Materials Response and Decontamination	-	-	
Recover Mission Area	Y ₃₅	Economic and Community Recovery	X	-
	Y ₃₆	Restoration of Lifelines	-	-
	Y ₃₇	Structural Damage Assessment	-	-

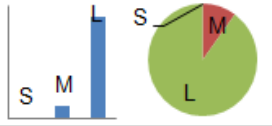
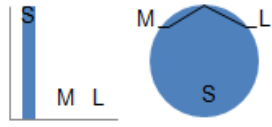
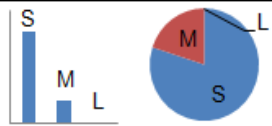

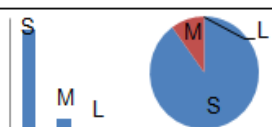
5.2. Threat Characterization

The scope of this analysis centers on the risk resulting from an IED attack against one or more of the five infrastructure assets identified in Figure 5-1. A set of five modes of attack for the IED events were considered as described in Table 5-3, where a simple probability distribution constructed over a discrete space of possible explosive weights (i.e., “small,” “medium,” and “large”) was constructed leveraging informal opinions from an explosives expert (Neale 2008). Each mode of attack accesses the target in a specific way. In particular:

- Hand emplaced (HE) explosive attacks are characterized by explosives delivered by a human directly to the target, and includes satchel charges, backpack bombs, and suicide attacks. Hand emplaced explosive attacks are compatible with any target accessible to humans on foot and susceptible to the effects of explosives.
- Ground vehicle (GV) explosive attacks are characterized by explosives delivered by ground-transiting vehicles, ranging from small compact cars to large trucks. Ground vehicle explosive attacks are compatible with any target accessible via roads and susceptible to the effects of explosives.
- Manned aerial vehicle (AVM) explosive attacks are characterized by explosives delivered by any type of human-operated air vehicle capable of carrying explosives, including motorized gliders and small airplanes. Manned aerial vehicle explosive attacks are compatible with any target accessible by air and susceptible to the effects of explosives.

- Unmanned aerial vehicle (AVU) explosive attacks are characterized by explosives delivered by any type of unmanned or autonomous aerial vehicle capable of carrying explosives, including radio-controlled aircraft and motorized balloons. Unmanned aerial vehicle explosive attacks are compatible with any target accessible by air and susceptible to the effects of explosives.
- Waterborne (WB) vehicle explosive attacks are characterized by explosives delivered by any type of water-transiting vehicle, including small boats such as canoes and kayaks to large vessels such as sailboats, yachts, and barges. Waterborne vehicle explosive attacks are compatible with any target directly adjacent to a body of water (e.g., river, lake) and susceptible to the effects of explosives.

Table 5-3. Delivery system types for IED events (Neale 2008)

Mode of Attack	Most Likely Weight (pounds TNT equivalent)	How Much More Likely Is It Relative to Alternative Weights?		Probability Distribution			Probability Distribution S=Small, M=Medium, L=Large
		Charge Weight	Relative Probability	Small	Medium	Large	
Ground Vehicle	Large	Small	1,000,000	0.00	0.10	0.90	
		Medium	9				
Unmanned Aerial Vehicle	Small	Medium	1,000,000	1.00	0.00	0.00	
		Large	1,000,000				
Manned Aerial Vehicle	Small	Medium	4	0.80	0.20	0.00	
		Large	1,000,000				
Waterborne Vehicle	Large	Small	1,000,000	0.00	0.50	0.50	
		Medium	1				
Hand-Emplaced	Small	Medium	9	0.90	0.10	0.00	
		Large	1,000,000				

The relative attractiveness of alternative modes of attack is a function of the perceived probability of success, P_S , gain from success, G , loss from failure, L , and cost to attack, C or probability of successful capability acquisition, P_C . A set of notional probabilities for this latter factor is given in Table 5-4. Assuming perfect adversary knowledge of regional and target defenses and loss potential for each target asset (per Chapter 3, Section 3.5), values for the remaining factors can be obtained directly from the assessment of the risk variables. For the gain parameter, the preferences of the adversary determine which risk variables to map to, whether to maximize fatalities, maximize disruption, maximize aggregate loss, satisfy a minimum requirement on probability of success (e.g., 0.75), etc. (Yager 2006; Nerud 2008). This analysis assumes an “optimistic, rational” adversary that seeks to maximize worst case aggregate loss, which for practical purposes can be taken as the 99% value on the 99% confidence level distribution for aggregate loss.

Table 5-4. Notional perceived probability of acquisition and capability

Mode of Attack	Probability of Successful Capability Acquisition, P_C
Hand Emplaced	0.95
Ground Vehicle	0.85
Manned Aerial Vehicle	0.70
Unmanned Aerial Vehicle	0.50
Waterborne Vehicle	0.85

For the purposes of this example, the probability of an attack in the region within a given time span is specified as single point working value. Assuming a planning horizon of 5 years between risk assessments, the assessed probability of one or more attacks in the region affecting one or more of the five assets is assessed to be “remote” with a representative probability of 0.05.

5.3. Asset Characterization

This section characterizes each of the five assets in the region under study in terms of relevant attack modes (section 5.3.1) maximum potential loss for the dimensions of disruption (units of time-%) and public health (units of fatality equivalents) (section 5.3.2), asset security system effectiveness in terms of probability of adversary success at the asset (section 5.3.3), target accessibility and attack mode success in terms of probability of kill (section 5.3.4), hardness of the target in terms of asset fragility matrices (section 5.3.5) and resistance to loss in terms of basis loss potential (section 5.3.6).

5.3.1. Relevant Attack Modes

All five infrastructure assets in this case study are susceptible to the effects of an explosive attack. However, due to the geographic constraints, not all attack modes are necessarily compatible with each asset. In particular for this example, the office building is the only asset adjacent to water, and as such is the only asset susceptible to a waterborne attack. Table 5-5 provides the attack profile compatibility matrix for the five regional assets, where an “X” denotes an attack mode that is compatible with an asset.

Table 5-5. Attack profile compatibility matrix for the five regional assets.

Asset	Compatibility Between Asset and Attack Mode				
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle	Waterborne Vehicle
Office Building	X	X	X	X	X
Hospital	X	X	X	X	
Train Station	X	X	X	X	
Stadium	X	X	X	X	
Power Substation	X	X	X	X	

5.3.2. Maximum Potential Loss and Value of Disruption

The maximum potential loss associated with each asset in terms of functional disruption and potential fatalities is given in Table 5-6. In practice, this data can be elicited as the maximum disruption time (e.g., time to completely reconstitute functionality in light of total loss) and maximum number of individuals that can possibly be exposed to the effects of an explosive attack against the asset. Since this analysis is examining each asset from the perspective of a regional decision maker, individuals within and adjacent to the asset are considered in addition to those within the scope of the asset owner's concern. The economic value to the region per day of disruption for each asset is given in Table 5-7.

Table 5-6. Maximum potential loss for each asset

Asset	Maximum Potential Loss	
	Disruption	Fatalities
Office Building	550 days (1.5 years)	500
Hospital	730 days (2 years)	2,000
Train Station	180 days (6 months)	3,500
Stadium	730 days (2 years)	75,000
Power Substation	90 days (3 months)	50

Table 5-7. Daily value of total disruption for each asset

Asset	Value of Disruption (\$/100%/day)*
Office Building	About \$50,000
Hospital	About \$100,000
Train Station	About \$25,000
Stadium	About \$75,000
Power Substation	About \$10,000

*Note: The word “about” implies $\pm 5\%$

5.3.3. Security System Effectiveness (Asset)

The following implements an approximate reasoning approach to assessing the effectiveness of each asset’s security system in terms of probability of adversary success in light of asset defenses using principles of fuzzy systems and fuzzy logic (McGill and Ayyub 2008b). Based on a discussion with a team of security experts and a review of current approaches to asset vulnerability assessment within the US Department of Defense, Morgenson et al. (2006) identified a set of six defensive criteria that are thought to characterize the effectiveness of a target’s (e.g., facility or asset) defenses as described in Table 5-8.

Table 5-8. Asset Defensive criteria for probability of adversary success assessment (Morgenson et al. 2006)

Variable	Defensive Criterion	Definition
X ₁	Perimeter Access Control	This attribute includes an access control system designed to preclude un-authorized entry. Effective access control systems prevent the introduction of harmful devices, materials and components. Access control systems include guarded entry and exit points, access control rosters, personal recognition, ID cards, badge exchange procedures and personnel escorts for visitors. Cyber access systems include firewall, passwords protection, antivirus software and are Tempest Secure as well as shielded from electromagnetic pulse or intrusion.
X ₂	Personnel Perimeter Barriers	Fencing is the primary personnel barrier. Standard fences are six foot tall, chain link fence topped with three strands of barbed wire with twisted and barbed selvages at the bottom. They are fastened to rigid metal or re-enforced concrete posts. In addition, these fences are typically inspected and maintained at least on a weekly basis. It should also be noted that the fence gates are designed to prevent personnel from crawling underneath. Sewer air and water intakes and exhausts and other utility openings that pass through perimeter barriers have security measures equivalent to those of the perimeter.
X ₃	Vehicle Perimeter Barriers	These barriers reinforce the fence and prevent vehicles from penetrating the perimeter. They keep VBIEDs at a safe standoff distance from the asset. Two types of barriers are used to protect the asset from vehicle bombs: perimeter and active barriers. Barriers differ for stationary and moving vehicle bombs. Barriers capable of stopping a moving vehicle include chain link fence reinforced with cable, reinforced concrete (jersey barriers), pipe bollards, planters, ditches, and berms. All these systems are anchored and spaces between barriers are no greater than four feet. Active barriers are required at entry and exit points; these barriers are substantial and must be strong enough to resist a 15000 pound vehicle moving at fifty miles per hour. Reinforced sliding gates, retractable bollards, and delta barriers are acceptable barriers. Other measures used to control the speed of vehicles moving up to the entrances or exits are anchored serpentines or permanent obstacles in the roadways, which force vehicles to slow down to get around them.
X ₄	Surveillance Systems	These systems are used to provide early warning of an intruder. Systems consist of hardware and software elements operated by trained security personnel. They are configured to provide two or more layers of detection around an asset. Each of these layers is made up of a series of interlocking detection zones. They isolate the asset and further control entry and exit of authorized personnel and equipment. Redundant power systems are utilized. These provide a separate emergency power source for surveillance and perimeter lights in case of a power failure or sabotage of the power main power systems. The term that is used to describe overall site surveillance is Electronic Security System (or ESS). An ESS consists of sensors interfaced with electronic entry controls, closed circuit television, alarm reporting displays, both visual and audible, and security lighting. Typically, a given security situation is assessed by re-positioning guards to the alarm site or using closed circuit television. The incident can be monitored from the security center, where the terminal for these devices is located. Depending on the severity of the incident, the guard force can be augmented. Other types of sensors are sometimes employed including boundary sensors that detect penetration (structural vibration sensors or passive ultrasonic sensors). The advantage to these sensors is the extra time they give the security force to react.

Table 5-8. (continued)

Variable	Defensive Criterion	Definition
X ₅	Guard Force	<p>The guard force or security force for a facility provides the enforcement element in the physical security program. The force consists of personnel specifically organized, trained, and equipped to protect the asset's physical security. It is considered the asset's most effective tool in a comprehensive, integrated, physical security program. This tool, however, requires vulnerability tests and advanced training to maintain effectiveness. For our purposes, the guard force will be considered adequately armed and trained. For example, there must be regular weapons qualification as well as practical drills to test reaction times and to correct weaknesses. Another consideration is that the guards are required to have prior military or law enforcement experience and be in relatively good physical condition. Training includes:</p> <ul style="list-style-type: none"> • Care and use of weapons • Areas of responsibility and authority of security personnel, including apprehension, search and seizure and the use of force • Location of first aid and fire control equipment as well as important electrical switches and circuit breaker boxes • Duties during emergencies, alerts, fires, explosions, and civil disturbances • Recognition of the common forms of sabotage and espionage activity • Knowing the location of vulnerable equipment and systems <p>New security force personnel are given instruction and are capable of assuming various different roles in the overall defense team. Rotating retraining schedules is a common practice, in order to cover adequately the entire security force.</p>
X ₆	Reaction Force with Heavy Weapons	<p>This is the asset's own reaction force and it should not to be confused with the reaction force provided by the local defense layer. It is normally a reserve from within the guard force on-site. They are uncommitted to security posts or check-points in order to be available for commitment at a decisive moment. Armament for the reaction force is heavier than the regular guard force and the level of training of the reaction force is equivalent to or better than the regular guard force. It includes an on-site HAZMAT response force based on the nature of work done at the site. For example, the chemical production facilities normally have some level of internal HAZMAT response capability within their workforce to respond to local emergencies. There are also memoranda of understanding (MOUs) with local law enforcement, fire departments, and other first responders that delineate the specific instances when they will respond to emergency situations at the asset.</p>

Applying the mathematics of fuzzy systems described Appendix A, a fuzzy system can be constructed (Figure 5-3) that approximates the functional relationship between the subjective assessment of each defensive criterion to an output probability of adversary success via an exhaustive set of linguistic rules of the form:

$$\text{If } X_1 \text{ and } X_2 \text{ and } X_3 \text{ and } X_4 \text{ and } X_5 \text{ and } X_6, \text{ then } \Pr(S_A | A, S_R) \quad (5-1)$$

where X_i are linguistic variables for the defensive criteria (i.e., premises) from Table 5-8 specified as membership functions spanning a constructed scale (Keeney 1981) on the bounded domain $[0, 10]$ (where 0 corresponds to no capability and 10 corresponds to full performance for the criteria in light of the mode of attack considered), and the consequent $\Pr(S_A|A,S_R)$ is the probability of adversary success at the asset given attack and adversary success against regional defenses specified over the domain $[0,1]$ as required by the axioms of probability theory (Ayyub and McCuen 2002). Within the context of this case study, the premises X_i may take on the fuzzy values “Low,” “Medium,” or “High” defined with membership functions shown in Figure 5-4, and the consequent $\Pr(S_A/A,S_R)$ may take on linguistic values such as “Likely,” “Certain,” or “Even Chance” with membership functions shown in Figure 5-5.

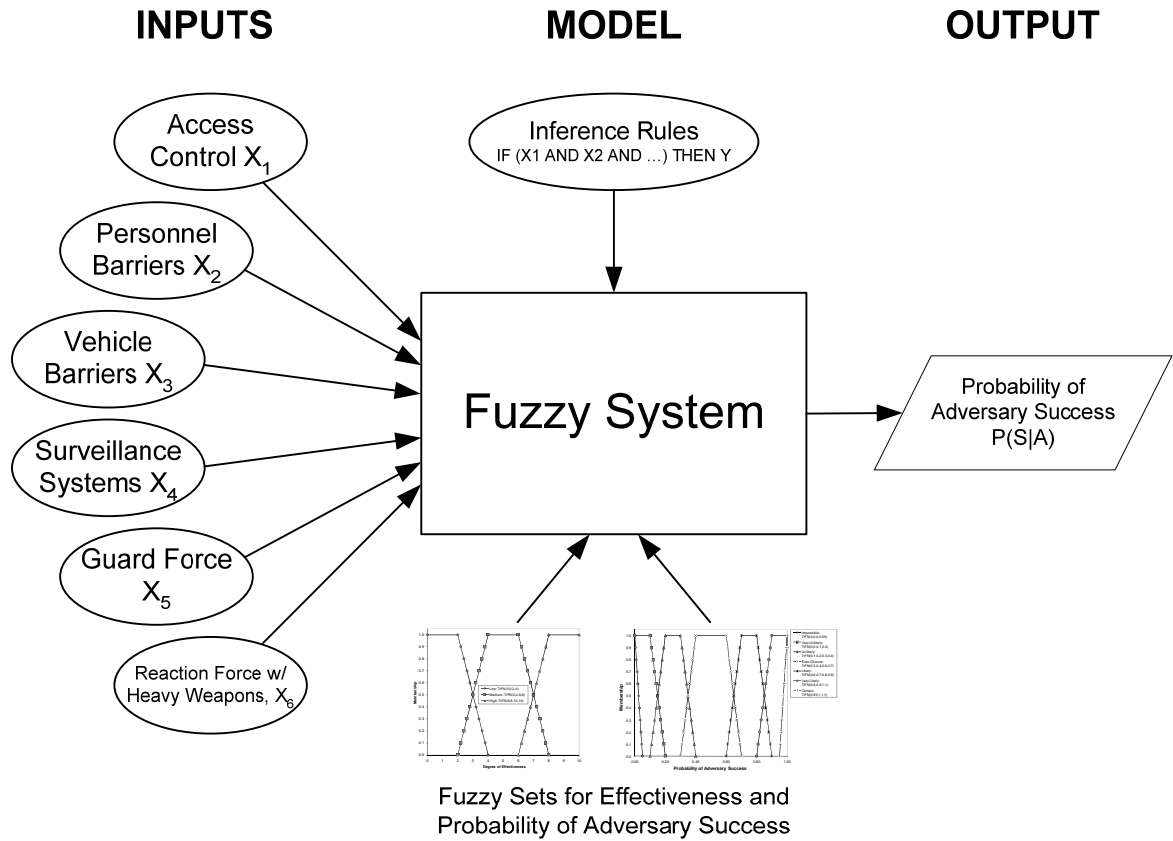


Figure 5-3. Schematic of the fuzzy system architecture for security system performance assessment

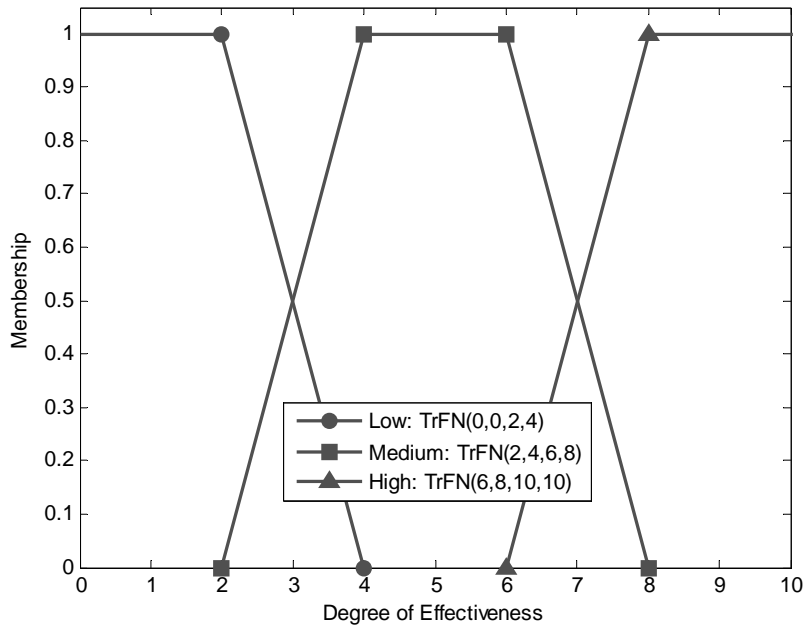


Figure 5-4. Membership functions for the fuzzy numbers representing degree of effectiveness on a constructed scale

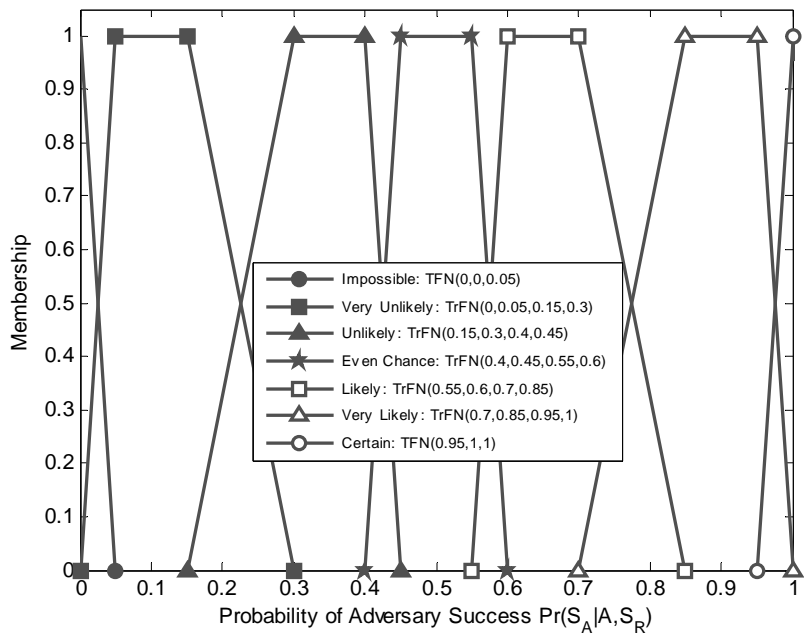


Figure 5-5. Membership functions for some fuzzy numbers representing probability of adversary success

Given a set of antecedents containing all possible linguistic state combinations of X_i , a corresponding consequent linguistic state $\Pr(S_A/A, S_R)$ can be specified for each by a panel of security experts. The set of all possible antecedents represents an exhaustive set of fuzzy rules, which would contain 729 rules according to Eq. A-9 using the three fuzzy numbers in Figure 5-4. For example, a panel of experts might decide that the following set of premises on the effectiveness of security measures corresponds to a probability of success equal to “Very Likely” (selected from the fuzzy numbers in Figure 5-5):

$$\begin{aligned}
 &\text{If } (X_1 \text{ is "Medium"}) \text{ and} \\
 &\quad (X_2 \text{ is "Low"}) \text{ and} \\
 &\quad (X_3 \text{ is "Low"}) \text{ and} \\
 &\quad (X_4 \text{ is "High"}) \text{ and} \\
 &\quad (X_5 \text{ is "Low"}) \text{ and} \\
 &\quad (X_6 \text{ is "Low"}) \\
 &\text{Then } (\Pr(S_A/A, S_R) \text{ is "Very Likely"})
 \end{aligned} \tag{5-2}$$

When combined, the complete set of fuzzy inference rules of this form approximate the true functional relationship between inputs and outputs, and thus provide a means for specifying the function:

$$\Pr(S_A | A, S_R) = \tilde{P}_A(X_1, X_2, X_3, X_4, X_5, X_6) \tag{5-3}$$

where the tilde “ \sim ” over the functional P_A denotes that it is a fuzzy system. An exhaustive set of notional, yet realistic fuzzy rules for assessing security system

effectiveness given the fuzzy sets for the defensive criteria and probability of adversary success is shown in Figure 5-6 for hand emplaced attacks, Figure 5-7 for ground vehicle and waterborne vehicle attacks, and Figure 5-8 for aerial vehicle (manned and unmanned) attacks. Given that each defensive criterion can assume one of three linguistic input states (i.e., 0 for “low,” 1 for “medium,” and 2 for “high”), a rule base is comprised of 729 rules, each represented as a cell in Figures 5-6 through 5-9 with unique number, Z , according to Eq. A-11 in Appendix A and background pattern denoting the corresponding probability of adversary success. For example, the rule described in Eq. 5-2 in the context of hand emplaced attacks according to Figure 5-6 is:

$$Z = (3^0)(1)+(3^1)(0)+(3^2)(0)+(3^3)(2)+(3^4)(0)+(3^5)(0) = 55$$

and is patterned with vertical dark grey and light grey stripes.

Once the fuzzy inference rules are defined, a user such as a security expert can subjectively assign a value to each premise or criterion on a scale of, say, 0 to 10 for a given facility or asset and threat type. According to the proposed model, the corresponding membership values for each relevant fuzzy set associated with the premises would be obtained, processed according to the set of fuzzy inference rules, and then the result would be translated back into a value for probability of adversary success represented as a random set which can be displayed in terms of the corresponding probability-boxes or p-boxes (Ferson et al. 2004). An equivalent probability distribution can be obtained from this random set via a suitable transformation, such as the pignistic transformation described by Smets (1994). Tables 5-9 through 5-13 describe the

subjective assessment of the six defensive criteria for each of the five infrastructure assets, and provide the corresponding probability of adversary success (at the asset) expressed as a p-box determined via the fuzzy system in Eq. 5-3 and mathematics described in Appendix A.

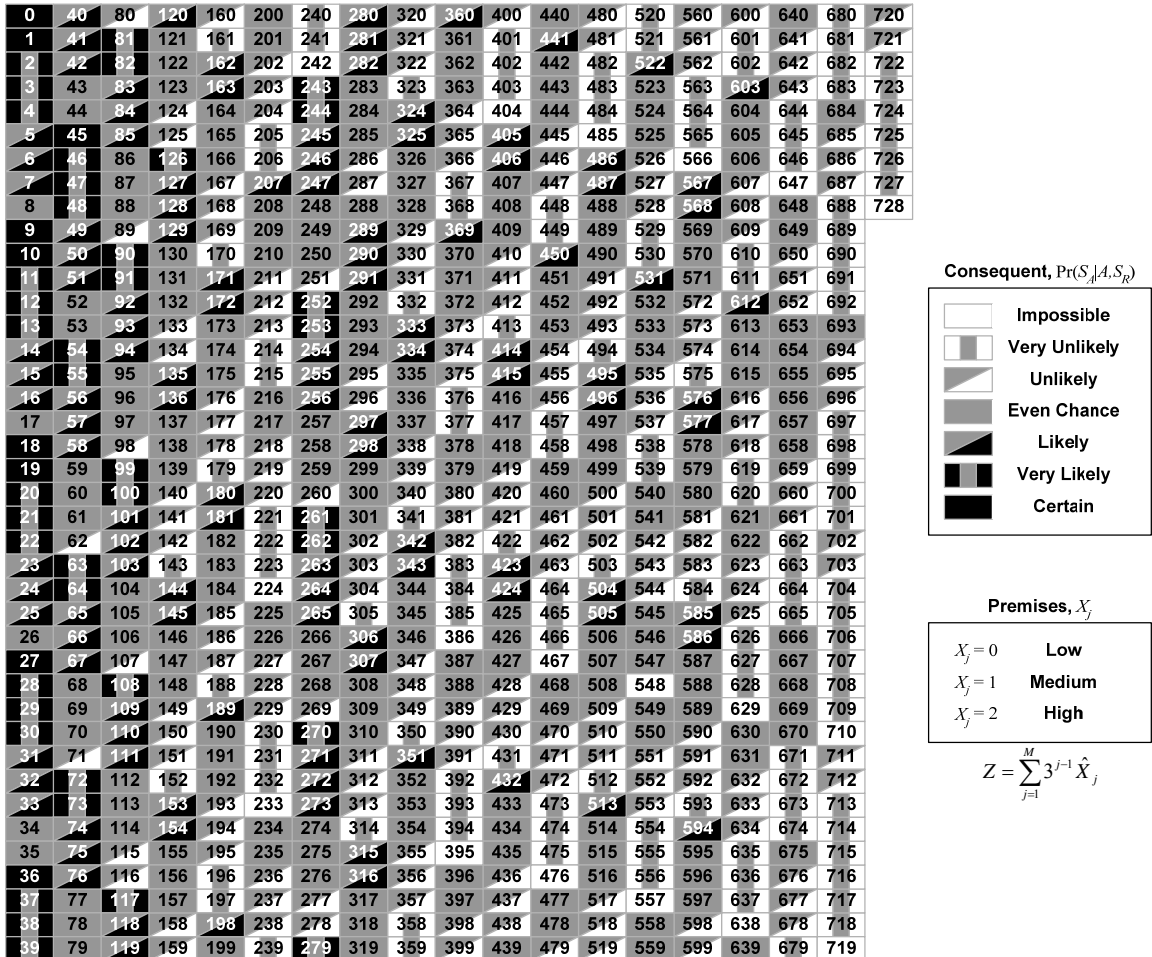


Figure 5-6. Exhaustive set of fuzzy inference rules for a hand emplaced explosive attack

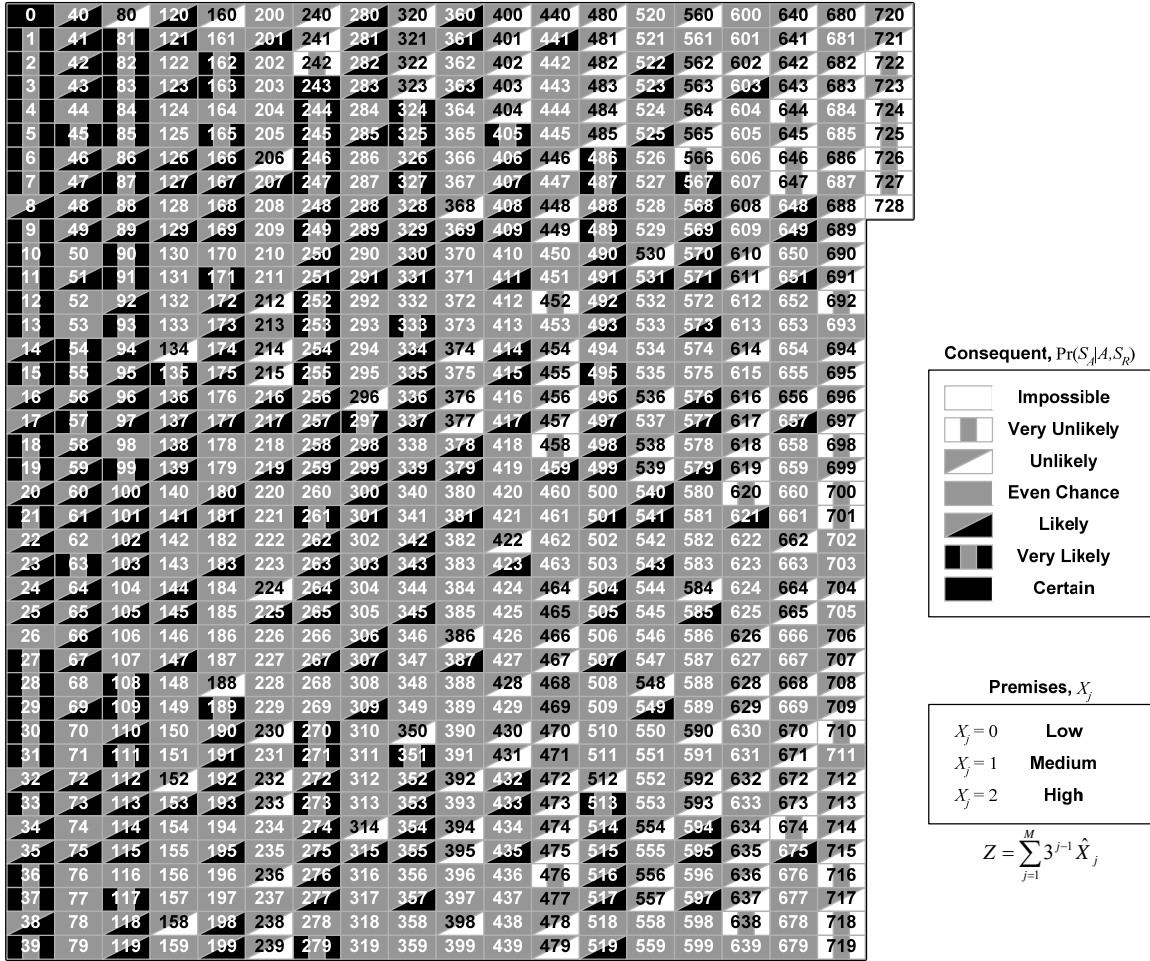


Figure 5-7. Exhaustive set of fuzzy inference rules for a ground vehicle and waterborne vehicle explosive attack

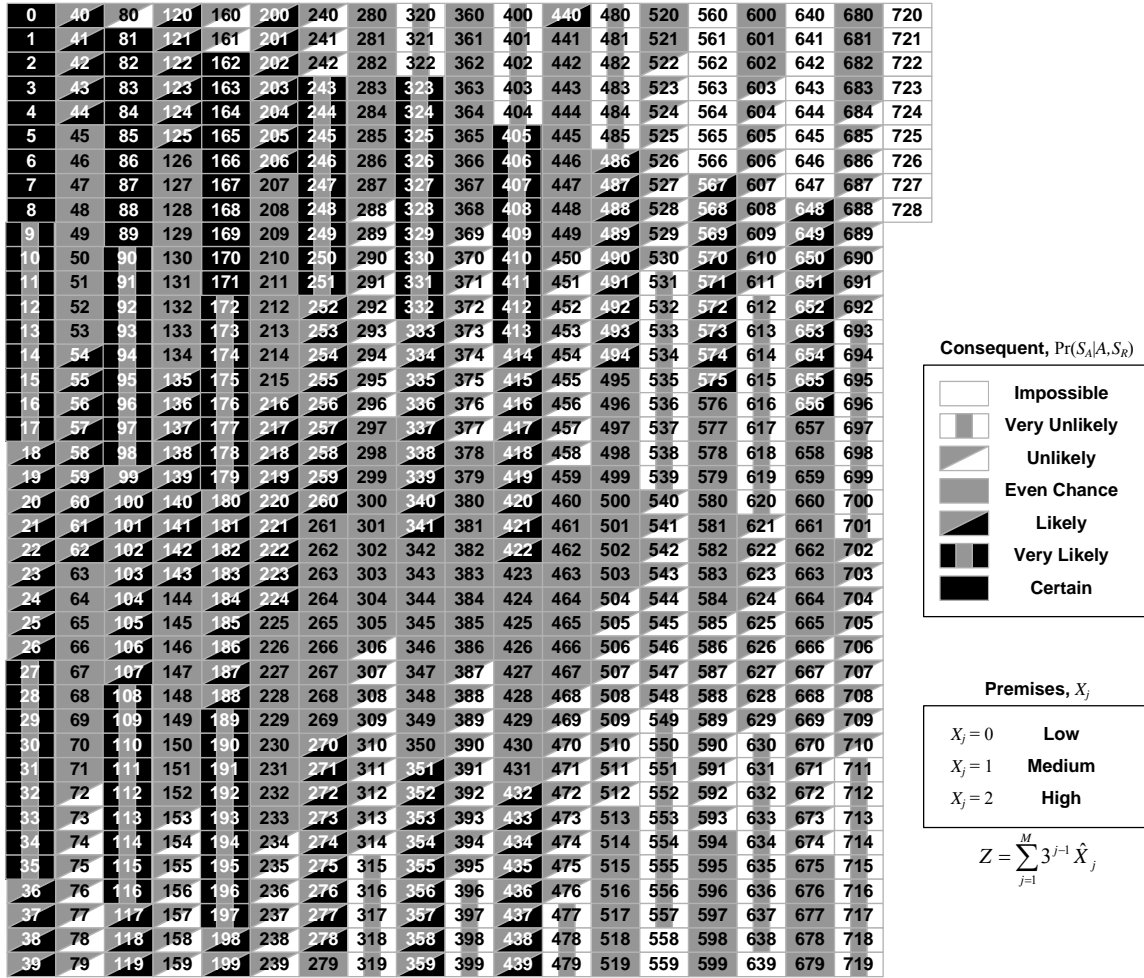


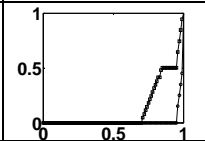
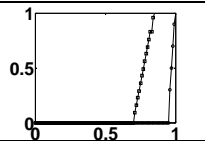
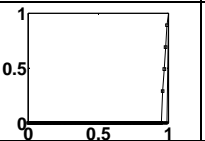
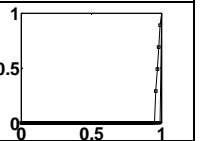
Figure 5-8. Exhaustive set of fuzzy inference rules for an aerial vehicle explosive attack

Table 5-9. Security system effectiveness assessment for the office building

Defensive Criterion	Assessed Value for Each Attack Mode (Office Building)				
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle	Waterborne Vehicle
X_1 : Perimeter Access Control	3	2	0	0	7
X_2 : Personnel Perimeter Barriers	1	NA	NA	NA	NA
X_3 : Vehicle Perimeter Barriers	NA	5	0	0	2
X_4 : Surveillance Systems	6	4	3	2	5
X_5 : Guard Force	6	4	0	0	6
X_6 : Reaction Force with Heavy Weapons	0	0	0	0	0
$\Pr(S_A A,S_R)^*$					

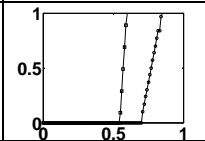
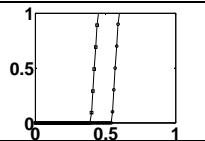
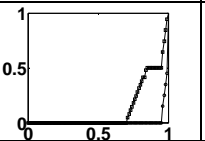
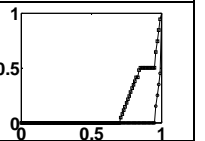
*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A,S_R)$ and the y-axis is the epistemic CDF on this probability.

Table 5-10. Security system effectiveness assessment for the hospital

Defensive Criterion	Assessed Value for Each Attack Mode (Hospital)			
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle
X_1 : Perimeter Access Control	2	0	0	0
X_2 : Personnel Perimeter Barriers	0	NA	NA	NA
X_3 : Vehicle Perimeter Barriers	NA	0	0	0
X_4 : Surveillance Systems	8	5	1	1
X_5 : Guard Force	3	1	2	2
X_6 : Reaction Force with Heavy Weapons	0	0	0	0
$\Pr(S_A A, S_R)^*$				

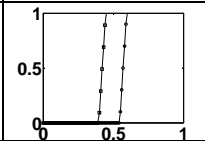
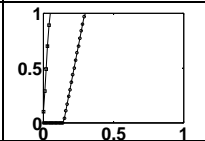
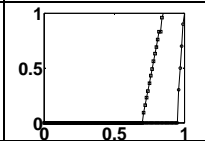
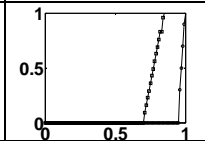
*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A, S_R)$ and the y-axis is the epistemic CDF on this probability.

Table 5-11. Security system effectiveness assessment for the train station

Defensive Criterion	Assessed Value for Each Attack Mode (Train Station)			
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle
X_1 : Perimeter Access Control	4	4	0	0
X_2 : Personnel Perimeter Barriers	0	NA	NA	NA
X_3 : Vehicle Perimeter Barriers	NA	6	0	0
X_4 : Surveillance Systems	8	8	3	3
X_5 : Guard Force	5	4	2	2
X_6 : Reaction Force with Heavy Weapons	2	2	1	1
$\Pr(S_A A, S_R)^*$				

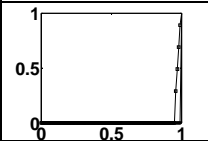
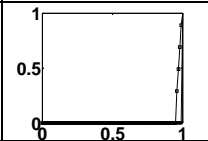
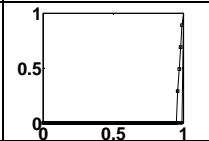
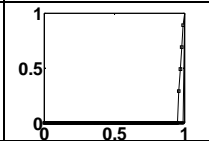
*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A, S_R)$ and the y-axis is the epistemic CDF on this probability.

Table 5-12. Security system effectiveness assessment for the stadium

Defensive Criterion	Assessed Value for Each Attack Mode (Stadium)			
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle
X_1 : Perimeter Access Control	6	8	0	0
X_2 : Personnel Perimeter Barriers	4	NA	NA	NA
X_3 : Vehicle Perimeter Barriers	NA	6	0	0
X_4 : Surveillance Systems	8	8	5	5
X_5 : Guard Force	6	6	4	2
X_6 : Reaction Force with Heavy Weapons	4	4	2	2
$\Pr(S_A A, S_R)^*$				

*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A, S_R)$ and the y-axis is the epistemic CDF on this probability.

Table 5-13. Security system effectiveness assessment for the electric power substation

Defensive Criterion	Assessed Value for Each Attack Mode (Electric Power Substation)			
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle
X_1 : Perimeter Access Control	0	0	0	0
X_2 : Personnel Perimeter Barriers	2	NA	NA	NA
X_3 : Vehicle Perimeter Barriers	NA	0	0	0
X_4 : Surveillance Systems	1	1	0	0
X_5 : Guard Force	0	0	0	0
X_6 : Reaction Force with Heavy Weapons	0	0	0	0
$\Pr(S_A A,S_R)^*$				

*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A,S_R)$ and the y-axis is the epistemic CDF on this probability.

5.3.4. Probability of Successful Attack Execution

Given adversary success at penetrating regional and target defenses, the probability that the attack will go off as intended and successfully impart the explosive energy to the target, $\Pr(K | S, A_i)$ (as in probability of kill per Washburn 2002) takes into account a variety of factors, including the construction of the device, the accessibility of the target to the delivery system, maneuverability of the delivery system, etc. A notional set of such probabilities is given in Table 5-14 for each of the five attack modes paired against the five regional assets.

Table 5-14. Probability of successful execution for each of the five delivery systems

Asset	Probability of Successful Execution for Each Attack Mode				
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle	Waterborne Vehicle
Office Building	0.98	0.95	0.90	0.75	0.95
Hospital	0.98	0.95	0.90	0.75	NA
Train Station	0.98	0.95	0.90	0.75	NA
Stadium	0.98	0.95	0.90	0.75	NA
Electric Power Substation	0.98	0.95	0.70	0.40	NA

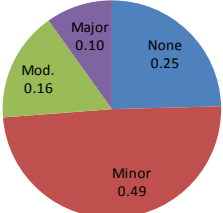
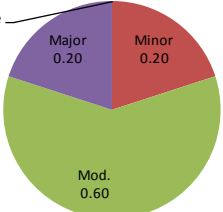
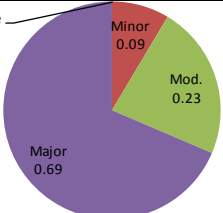
5.3.5. Asset Fragility Matrices

The probability $\Pr(D_k | A)$ that an asset will suffer a given damage state D_k subject to a given attack mode defined by the initiating event A can be obtained as:

$$\Pr(D_k | A) = \sum_j \Pr(D_k | I_j) \Pr(I_j | A) \quad (5-4)$$

where the probability of intensity given an attack of specified type, $\Pr(I_j | A)$ is given by the information in Table 5-3 and the probability of damage with respect to different size explosive attacks, $\Pr(D_k | I_j)$ is specified according to fragility matrices constructed over a finite space of four discrete damage states (i.e., “no damage,” “minor damage,” “moderate damage,” and “major damage”) shown in Tables 5-15 through 5-19 for the five regional assets. The resulting probability of damage over the finite space of damage states for each asset in light of the five attack modes is given in Table 5-20.

Table 5-15. Probability of damage subject to different size IED attacks for the office building.

Weight	Most Likely Damage State	Comparative Damage State	Relative Probability of Damage*	Probability Distribution (Only two decimal places shown)
Small	Minor	None	2	
		Moderate	3	
		Major	5	
Medium	Moderate	None	∞	
		Minor	3	
		Major	3	
Large	Major	None	∞	
		Minor	8	
		Moderate	3	

*Note: This column describes how many times more likely is the comparative damage state relative to the most likely damage state.

Table 5-16. Probability of damage subject to different size IED attacks for the hospital.

Weight	Most Likely Damage State	Comparative Damage State	Relative Probability of Damage*	Probability Distribution (Only two decimal places shown)
Small	Minor	None	10	
		Moderate	5	
		Major	20	
Medium	Moderate	None	50	
		Minor	5	
		Major	10	
Large	Major	None	∞	
		Minor	100	
		Moderate	20	

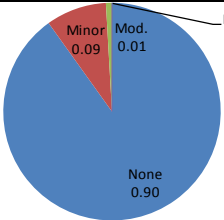
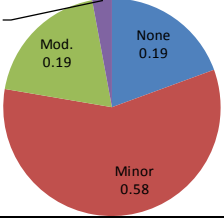
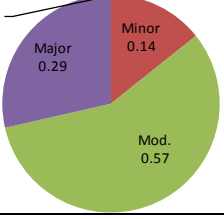
*Note: This column describes how many times more likely is the comparative damage state relative to the most likely damage state.

Table 5-17. Probability of damage subject to different size IED attacks for the train station.

Weight	Most Likely Damage State	Comparative Damage State	Relative Probability of Damage*	Probability Distribution (Only two decimal places shown)
Small	None	Minor	2	
		Moderate	10	
		Major	∞	
Medium	Minor	None	3	
		Moderate	3	
		Major	20	
Large	Moderate	None	∞	
		Minor	4	
		Major	2	

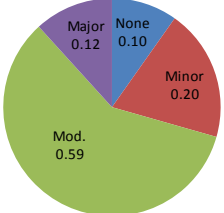
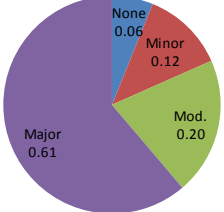
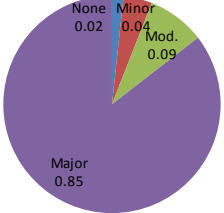
*Note: This column describes how many times more likely is the comparative damage state relative to the most likely damage state.

Table 5-18. Probability of damage subject to different size IED attacks for the stadium.

Weight	Most Likely Damage State	Comparative Damage State	Relative Probability of Damage*	Probability Distribution (Only two decimal places shown)
Small	None	Minor	10	
		Moderate	100	
		Major	∞	
Medium	Minor	None	4	
		Moderate	50	
		Major	∞	
Large	Moderate	None	10	
		Minor	2	
		Major	100	

*Note: This column describes how many times more likely is the comparative damage state relative to the most likely damage state.

Table 5-19. Probability of damage subject to different size IED attacks for the electric power substation.

Weight	Most Likely Damage State	Comparative Damage State	Relative Probability of Damage*	Probability Distribution (Only two decimal places shown)
Small	Moderate	None	6	
		Minor	3	
		Major	5	
Medium	Major	None	10	
		Minor	5	
		Moderate	3	
Large	Major	None	50	
		Minor	20	
		Moderate	10	

*Note: This column describes how many times more likely is the comparative damage state relative to the most likely damage state.

Table 5-20. Probability of damage states for each asset and attack mode combination

Asset	Attack Mode				
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle	Waterborne Vehicle
Office Building					
Hospital					
Train Station					
Stadium					
Power Substation					

5.3.6. Basis Loss

The basis loss for an asset describes the loss potential in the absence of regional response and recovery capabilities for a given state of damage following a successful attack. The basis loss considers the ability of the asset to resist, respond to, and recover from loss, which depends on such things as intrinsic system structure, the existence of redundant elements, and safety systems. To simplify the elicitation of the basis loss, the uncertainty in this loss is characterized by a triangular possibility distribution over the space of outcomes for each consequence dimension (see Appendix A.1). To simplify matters further, this possibility distribution can be constructed over the domain of percentage of maximum potential loss with three points as follows:

- Reasonable Best Case
- Most Likely Loss
- Reasonable Worst Case

The reasonable best case and reasonable worst case bound the scope of imagined outcomes in the absence of regional response and recovery capabilities; values of experienced loss beyond these limits are thus deemed to be practically impossible and carry maximum value of potential surprise (Shackle 1969). Tables 5-21 and 5-22 specify the basis loss corresponding to each damage state with respect to the five regional assets.

Table 5-21. Basis loss for each damage state (disruption)

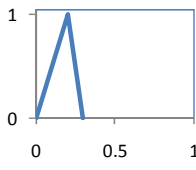
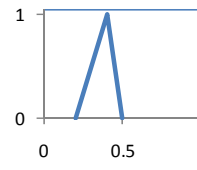
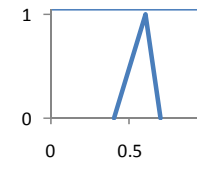
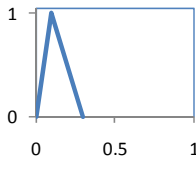
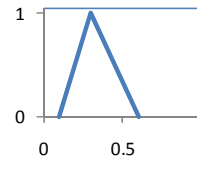
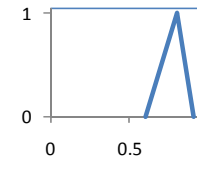
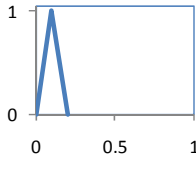
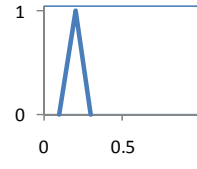
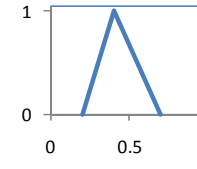
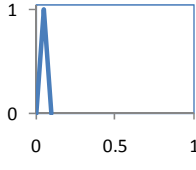
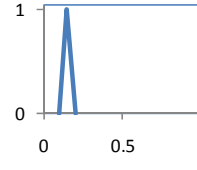
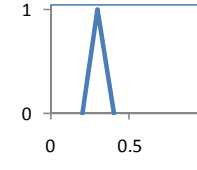
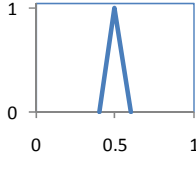
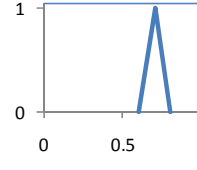
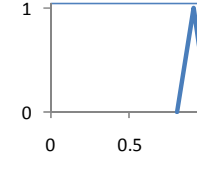
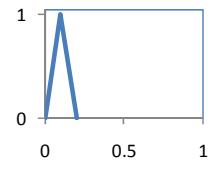
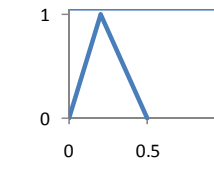
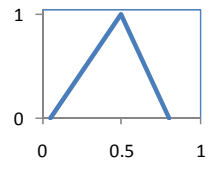
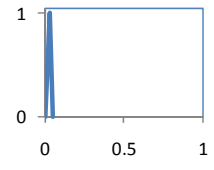
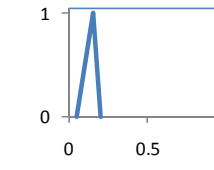
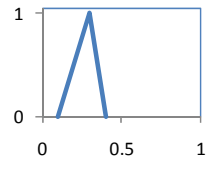
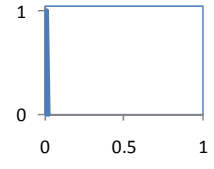
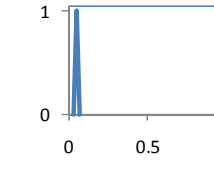
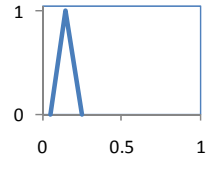
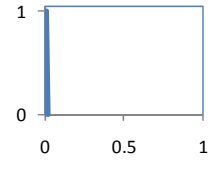
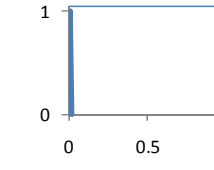
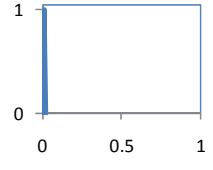
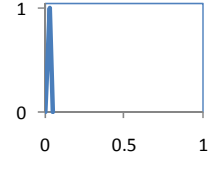
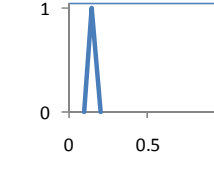
Asset	Basis Loss for Each Damage State (Disruption)		
	Minor	Moderate	Major
Office Building	 TFN(0.0,0.2,0.3)	 TFN(0.2,0.4,0.5)	 TFN(0.4,0.6,0.7)
Hospital	 TFN(0.0,0.1,0.3)	 TFN(0.1,0.3,0.6)	 TFN(0.6,0.8,0.9)
Train Station	 TFN(0.0,0.1,0.2)	 TFN(0.1,0.2,0.3)	 TFN(0.2,0.4,0.7)
Stadium	 TFN(0.0, 0.05, 0.1)	 TFN(0.1, 0.15, 0.2)	 TFN(0.2, 0.3, 0.4)
Power Substation	 TFN(0.4,0.5,0.6)	 TFN(0.6,0.7,0.8)	 TFN(0.8,0.9,1.0)

Table 5-22. Basis loss for each damage state (fatalities)

Asset	Basis Loss for Each Damage State (Fatalities)*		
	Minor	Moderate	Major
Office Building	 TFN(0.0, 0.1, 0.2)	 TFN(0.0, 0.2, 0.5)	 TFN(0.05, 0.5, 0.8)
Hospital	 TFN(0.0, 0.03, 0.05)	 TFN(0.05, 0.15, 0.2)	 TFN(0.1, 0.3, 0.4)
Train Station	 TFN(0.00, 0.01, 0.02)	 TFN(0.03, 0.05, 0.07)	 TFN(0.05, 0.15, 0.25)
Stadium	 TFN(0.001, 0.002, 0.003)	 TFN(0.002, 0.005, 0.007)	 TFN(0.01, 0.02, 0.025)
Power Substation	 TFN(0.0, 0.03, 0.05)	 TFN(0.1, 0.15, 0.2)	 TFN(0.15, 0.2, 0.25)

*Note: In the figures, the x -axis is percent maximum potential loss, and the y -axis is the corresponding membership value

5.3.7. Asset Visibility

In the context of this case study, it is assumed that the adversary has perfect knowledge of all five assets. Visibility of all attack profiles and asset is assured under this assumption, and thus the probability that the asset is visible to the adversary is set equal to one ($\Pr(V) = 1$) for all five regional assets.

5.4. Regional Characterization

This section characterizes the region under study in terms of performance of each of its capabilities to protect, prevent, respond to, recover from, and mitigate (section 5.4.1), first-order interdependencies among the identified assets in the region (section 5.4.2), and the effectiveness of regional security in terms of probability of adversary success in the region (section 5.4.3).

5.4.1. Response and Recovery Effectiveness - Fatalities

It is standard practice within most US regions and locales to mobilize publicly-funded resources to assist in responding to and recovering from the effects of adverse initiating events affecting its citizens. In the extreme situation where no such resources exist, the loss following an adverse initiating event affecting an asset can be characterized by uncertainty distributions, such as the possibility distributions constructed in section 5.3.5 (i.e., the basis loss), that only account for the inherent resistance of the asset to loss in light of its system characteristics and its indigenous response and recovery capabilities. It can be assumed that any additional capability brought to bear by the region to assist in response and recovery serves to reduce this basis loss potential. Stated another way, it

can be assumed that regional capabilities do not increase ensuing loss, but rather serve to discount it as a function of its unmitigated magnitude. This assumption further assumes a saturation point at which regional capabilities can no longer reduce loss in an efficient manner. That is, there exists some value or saturation point of loss L^* at which further loss cannot be mitigated by regional capabilities.

Given the basis loss potential information collected for the five regional assets in Section 5.3.6, an approximate model that relates a subset of the 37 capabilities to public health and safety loss can be constructed leveraging the approximate reasoning techniques already applied to the asset security system effectiveness problem in Section 5.3.3 and elaborated on in detail in Appendix A. Table 5-2 summarizes a mapping of capabilities to the loss variable “fatalities.” The approximate relationship, \tilde{C}_F , between relevant capabilities y_F , basis public health and safety loss, $l_{F,B}$, and percentage reduction in loss, ρ_F can be expressed as:

$$\rho_F = \tilde{C}_F(l_{F,B}, y_F) \quad (5-5)$$

In the context of this case study, the loss inputs to Eq. 5-5 are conditioned on a specific damage state. The epistemic uncertainty associated with the output of the fuzzy system \tilde{C}_F can be expressed as a probability box (Ferson et al. 2004) with lower and upper bounds characterized by the cumulative belief function $Cbel_L(l)$ (Eq. A-26) and cumulative plausibility function $Cpl_L(l)$ (Eq. A-27), respectively. That is, a crisp input for basis loss produces a less certain output that can be characterized by a family of loss-exceedance curves contained in the probability box bounded by the functions $1 - Cbel_L$

and $1 - Cpl_L$. Moreover, given that the input $l_{F,B}$ to Eq. 5-5 is characterized by a possibility distribution as described in Section 5.3.6, the corresponding outputs take the form of a nested set of conditional loss-exceedance curves (or probability boxes/hybrid numbers) with increasing degrees of membership such as is shown in Figure 5-9. This form of loss distribution can be referred to as possibilistic loss exceedance curves, which to the author's knowledge was first introduced in concept by Karimi (2006).

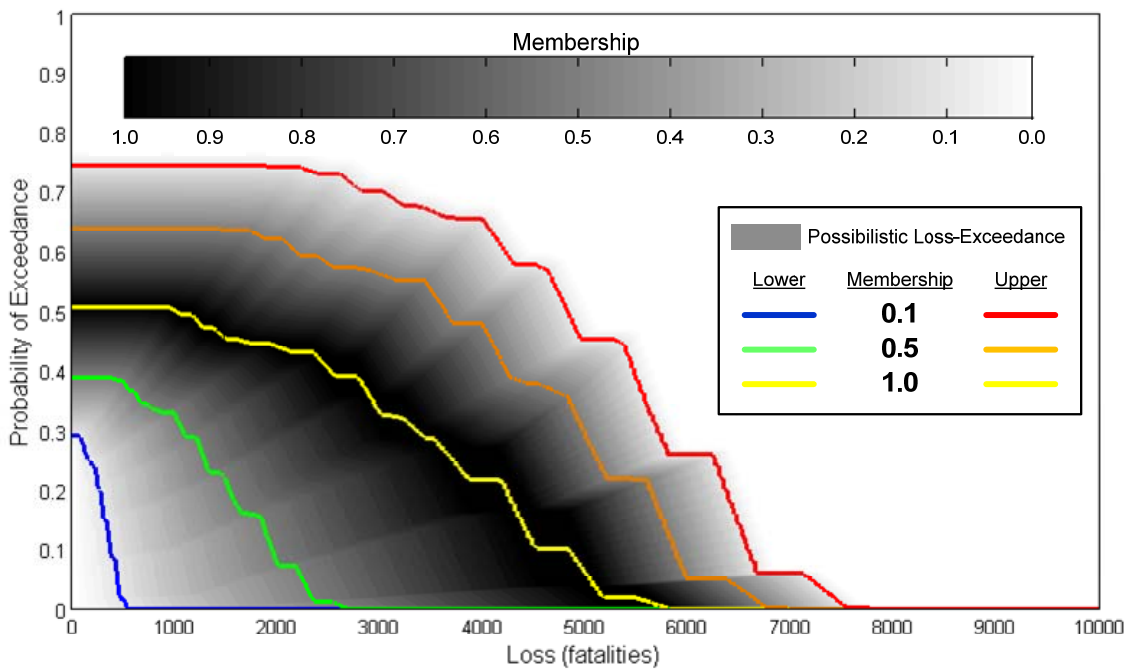


Figure 5-9. Notional conditional possibilistic loss exceedance curve given successful attack

The total rule base to implement the fuzzy systems of Eq. 5-6 consists of a set of M conditional rule bases for each possible state of loss, $L_{B,F}$. The fuzzy system for percentage reduction in fatality loss in Eq. 5-5 is comprised of a set of linguistic rules of the form:

$$\text{If } L_{F,B} \text{ and } Y_1 \text{ and } Y_2 \text{ and } \dots \text{ and } Y_{35}, \text{ then } \rho_F \quad (5-6)$$

According to Table 5-2, 18 regional capabilities are assumed to contribute and interact toward reducing the number of fatalities following an adverse initiating event. To simplify calculations in this model in light of the large number of capabilities relevant to public health and safety loss, each capability Y_j (see Table 5-2 for the list of Y_j relevant to fatalities loss) is allowed to assume one of two states – “effective” or “ineffective” – with membership functions shown in Figure 5-10 constructed over the bounded domain $[0, 10]$. This results in $2^{18} = 262,144$ rules according to Eq. A-9. Greater sensitivity is afforded to the loss variable, which is allowed to take on one of five states as described in Figure 5-11 constructed over the bounded domain $[0, L^*]$, where L^* is the saturation point of the response capabilities in the region. Any amount of basis loss that exceeds L^* is assumed to be unmitigable. The percentage reduction in loss, ρ_F , can assume one of ten output sets as shown in Figure 5-12 (without labels) constructed over the bounded domain $[0, 100\%]$.

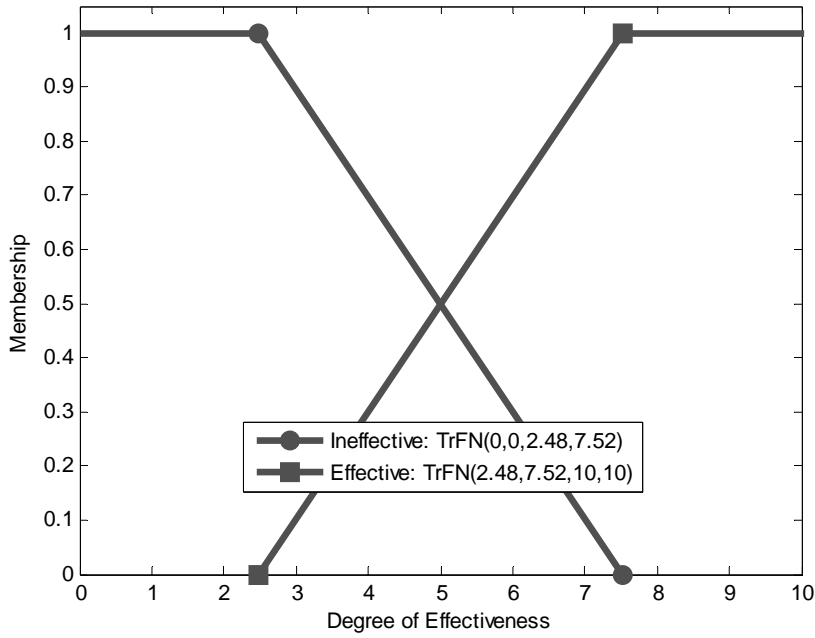


Figure 5-10. Membership functions for states of the input capability variables

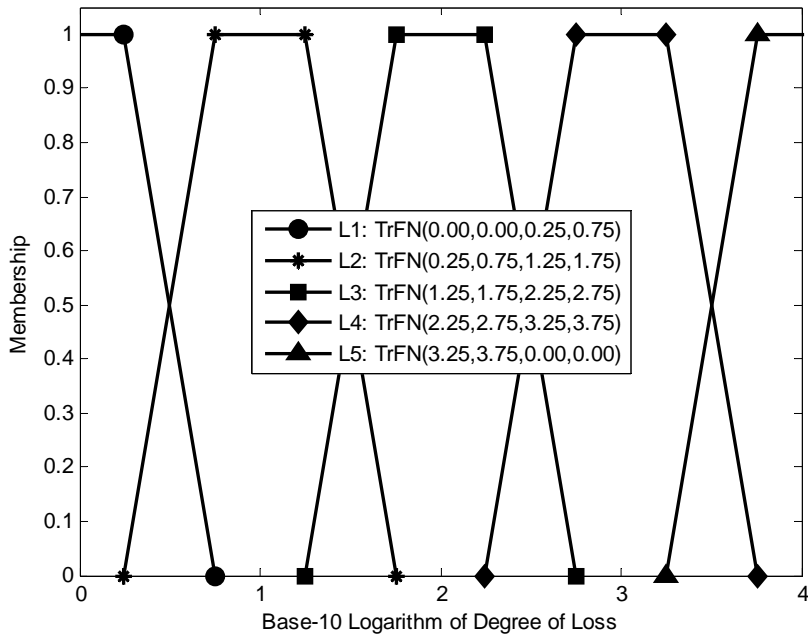


Figure 5-11. Membership functions for states of the input loss variable

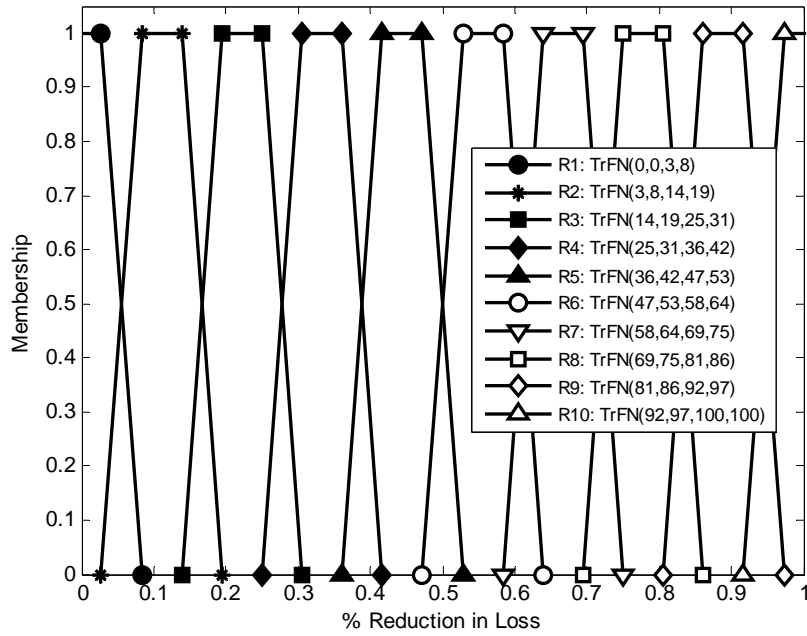


Figure 5-12. Membership functions for states of the output reduction variable

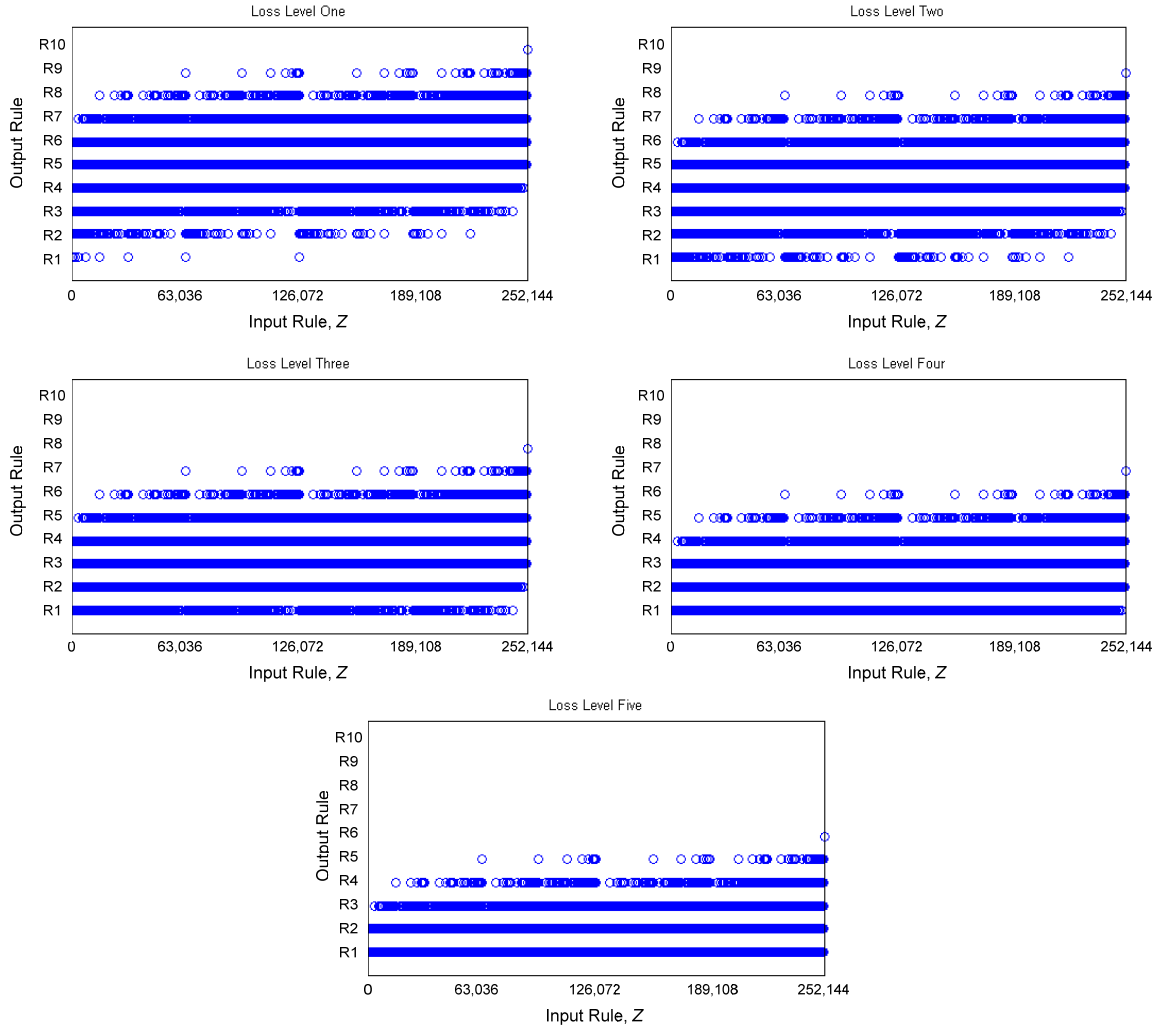


Figure 5-13. Conditional rules bases for fatality loss reduction. Each circle maps a rule number to an output state R_i .

A notional assessment of relevant regional capabilities is provided in Table 5-23, where a “-” means that the assessed value for the corresponding capability is not relevant to this analysis. According to the model in Eq. 5-5 and the basis public health and safety loss in Table 5-21, these capabilities produce a conditional cumulative distribution function on public health and safety loss such as that shown in Figure 5-14 for ground vehicle attack

against the office building. A summary of results for all five assets and corresponding attack profiles is provided in Appendix B, Section B.1.

Table 5-23. Notional regional Capability Assessment

Category	Label	Capability	Value*
Common Mission Area	Y ₁	Communications	5
	Y ₂	Community Preparedness and Participation	7
	Y ₃	Planning	8
	Y ₄	Risk Management	--
	Y ₅	Intelligence/ Information Sharing and Dissemination	6
Planning Mission Area	Y ₆	CBRNE Detection	4
	Y ₇	Information Gathering and Recognition of Indications and Warning	5
	Y ₈	Intelligence Analysis and Production	6
	Y ₉	Counter-Terror Investigations and Law Enforcement	8
Protect Mission Area	Y ₁₀	Critical Infrastructure Protection	--
	Y ₁₁	Epidemiological Surveillance and Investigation	--
	Y ₁₂	Food and Agriculture Safety and Defense	--
	Y ₁₃	Public Health Laboratory Testing	--
Respond Mission Area	Y ₁₄	Animal Disease Emergency Support	--
	Y ₁₅	Citizen Evacuation and Shelter-In-Place	8
	Y ₁₆	Critical Resource Logistics and Distribution	7
	Y ₁₇	Emergency Operations Center Management	8
	Y ₁₈	Emergency Public Information and Warning	5
	Y ₁₉	Environmental Health	--
	Y ₂₀	Explosive Device Response Operations	--
	Y ₂₁	Fatality Management	4
	Y ₂₂	Fire Incident Response Support	6
	Y ₂₃	Isolation and Quarantine	--
	Y ₂₄	Mass Care (Sheltering, Feeding, and Related Services)	7
	Y ₂₅	Mass Prophylaxis	--
	Y ₂₆	Medical Supplies Management and Distribution	8
	Y ₂₇	Medical Surge	4
	Y ₂₈	Onsite Incident Management	5
	Y ₂₉	Emergency Public Safety and Security Response	6
	Y ₃₀	Responder Safety and Health	5
	Y ₃₁	Emergency Triage and Pre-Hospital Treatment	8
	Y ₃₂	Search and Rescue (Land-Rescue)	9
	Y ₃₃	Volunteer Management and Donations	--
Y ₃₄	WMD/Hazardous Materials Response and Decontamination	--	
Recover Mission Area	Y ₃₅	Economic and Community Recovery	5
	Y ₃₆	Restoration of Lifelines	--
	Y ₃₇	Structural Damage Assessment	--

*Note: a '--' indicates a capability that does not bear on the assessment of response and recovery vulnerability

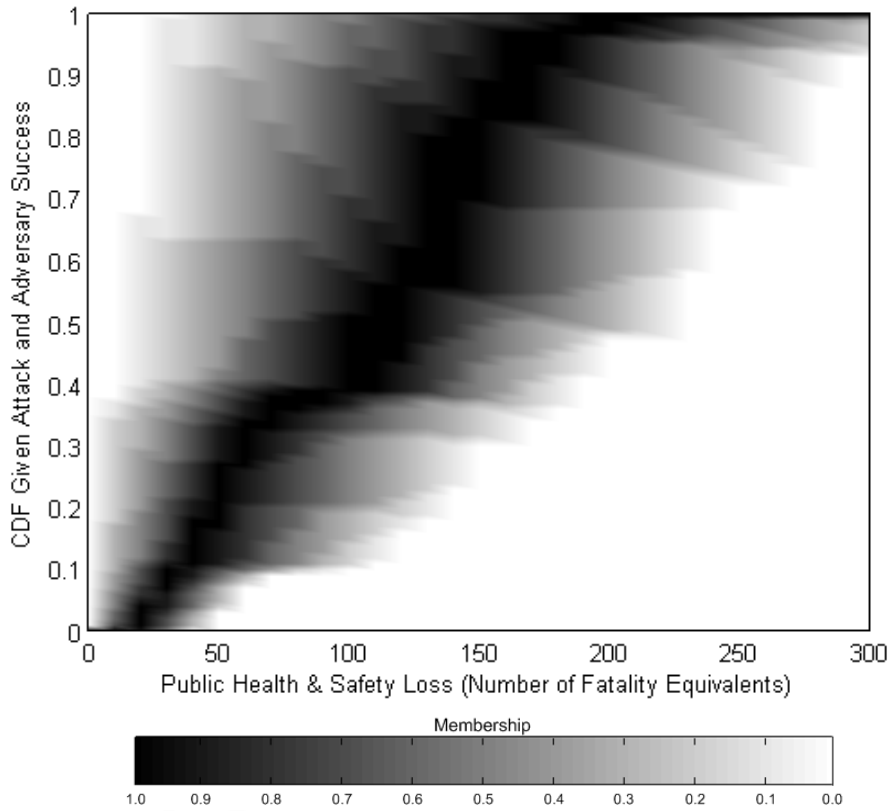


Figure 5-14. Conditional cumulative distribution on public health and safety loss for the office building subject to a ground vehicle attack

5.4.2. Interdependency Analysis

For disruption of service, a consequence conversion factor is developed uniquely for each asset according to the economic loss corresponding to service outage. Such values were assessed in Table 5-5 for each asset. The effects of dependencies among the portfolio of assets in the region (i.e., internal interdependencies) are captured in a first-order basis via a simple proportionality relationship between disruption and economic loss of the form (Ayyub et al. 2007):

$$L_I = (\mathbf{c}_A^T \mathbf{K}_A \mathbf{u}_b) \cdot L_{T,b} \quad (5-7)$$

where \mathbf{c}_A^T is a vector that assigns a cost per unit time of disruption for each asset in the portfolio, \mathbf{K}_A is the portfolio interdependency matrix where elements k_{ij} give the percentage degree of disruption to asset a_i due to complete loss of asset a_j ($a_i, a_j \in A$), \mathbf{u}_b is a disruption vector with elements u_i that take on the value of the percentage service disruption for i corresponding to asset b (zero otherwise), and $L_{T,b}$ is the time to recover lost functionality of asset b (i.e., disruption time determined for the asset). The following assumptions were made to justify the form of Eq. 5-7:

- Only first-order internal interdependencies are considered. Second-order and higher interdependencies are not considered, nor are interdependencies arising from interactions with assets and services external to the portfolio.
- Substitution of services is not considered. The model makes the conservative assumption that the interdependent assets will not make any non-immediate substitutions beyond what is nominally available in the market relating to the asset.
- The degree of degradation of the function of an asset is linearly proportional to the degree of degradation in its dependencies. This assumption justifies the use of the interdependency matrix \mathbf{K}_A with elements k_{ij} that linearly map disruption of the initiating asset to percentage disruption of interdependent assets.
- The loss attributed to disruption of an asset is proportional to the degree of disruption and the time to reconstitute its function. This assumption justifies the

use of a cost vector \mathbf{c}_A^T to map percent damage to economic loss, and use of the recuperation time L_{T0} of the initiating asset to scale it according to time. This assumption is conservative in the sense that with increasing time, portfolios such as a region or infrastructure sector will tend to compensate for the loss via substitution.

Referring to the list of 37 target capabilities shown in Table 5-2, any improvements in lessening the interdependency values \mathbf{K}_A , lessening the cost per unit disruption \mathbf{c}_A^T , or decreasing the amount of time for disruption following an adverse incident (such through a purchase of spare transformers for an electric power substation) addresses capability Y_{36} , “Restoration of Lifelines.”

Table 5-24 presents a notional interdependency matrix \mathbf{K}_A for a system comprised of the five regional assets, where each cell gives the percentage reduction in function of a column asset due to total disruption of a row asset. According to the model in Eq. 5-7 and the basis disruption loss in Table 5-22, the cumulative distribution function on disruption loss can be obtained such as that shown in Figure 5-15 for ground vehicle attack against the office building. A summary of results for all five assets and corresponding attack profiles is provided in Appendix B, Section B.2.

Table 5-24. First-order regional asset interdependency matrix

	Office Building	Hospital	Train Station	Stadium	Power Substation
Office Building		0	15	0	80
Hospital	0		0	0	100
Train Station	0	0		0	100
Stadium	0	0	50		100
Power Substation	0	0	0	0	

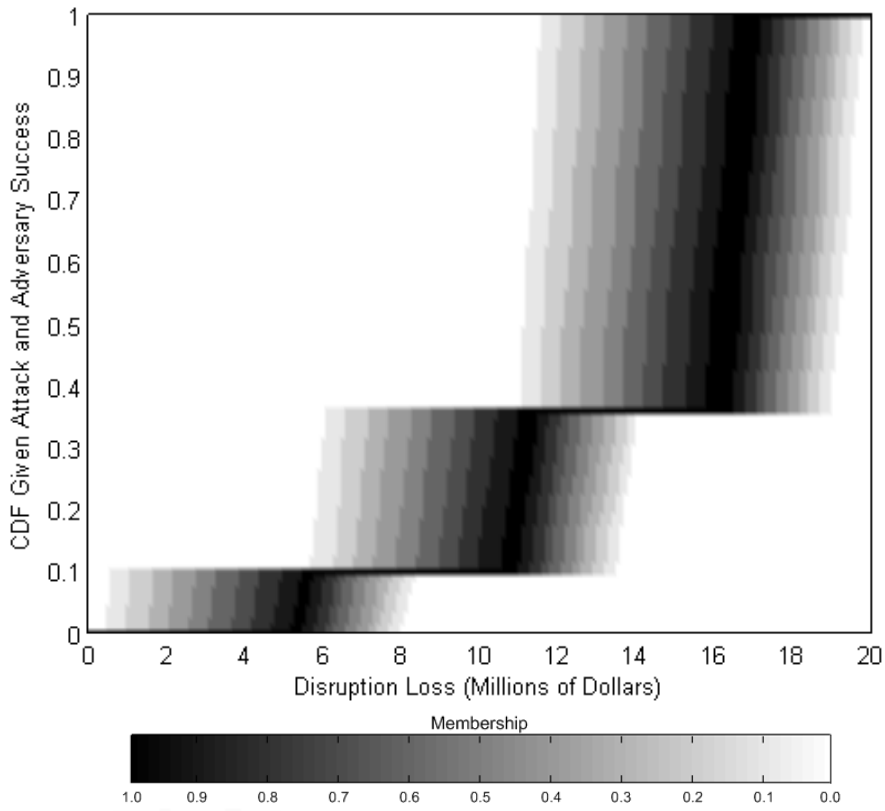


Figure 5-15. Conditional cumulative distribution on disruption loss for the office building subject to a ground vehicle attack

5.4.3. Probability of Adversary Success in Region

It is broadly accepted that the effectiveness of a security system depends on the ability of defender forces to detect, respond to, and defeat determined adversaries (McGill et al. 2007). As was done for the case of asset security, the functional relationship between adversary success probability in light of regional defenses, $\Pr(S_R | A)$ and defensive variables can be expressed in approximate form as:

$$\Pr(S_R | A) = \tilde{P}_R(W_1, W_2, W_3) \quad (5-8)$$

where the defensive criteria W_1 , W_2 , and W_3 described in Table 5-25 are linguistic variables whose values assume membership functions spanning a constructed scale on the bounded domain $[0, 10]$ (where 0 corresponds to no capability and 10 corresponds to full performance for the criteria in light of the mode of attack considered), and the consequent $\Pr(S_R|A)$ is the probability of adversary success at defeating regional defenses given attack specified over the domain $[0,1]$. The fuzzy system \tilde{P}_R in Eq. 5-8 is defined by an exhaustive set of linguistic rules of the form:

$$\text{If } W_1 \text{ and } W_2 \text{ and } W_3, \text{ then } \Pr(S_R | A) \quad (5-9)$$

Within the context of this case study, the premises W_i may take on one of five fuzzy values as shown in Figure 5-16, and the consequent $\Pr(S_R/A)$ may take on one of seven linguistic values shown in Figure 5-17. According to Eq. A-9, this results in 125 rules. A notional set of rules are provided in Table 5-26 that are broadly applicable to all attack

modes. The benchmarks for the assessment of the underlying variables, however, are different depending on attack mode.

According to the fuzzy system for regional security performance assessment described in Eq. 5.8, a set of notional probabilities for adversary success in the region (illustrated in the form of p-boxes) can be obtained such a is shown in Table 5-27.

Table 5-25. Regional Defensive criteria for probability of adversary success assessment

Variable	Defensive Criterion	Definition
W_1	Detection	Ability to detect that the attack is occurring
W_2	Response	Ability to engage the adversary once detected
W_3	Defeat	Ability to defeat or neutralize the adversary once engaged

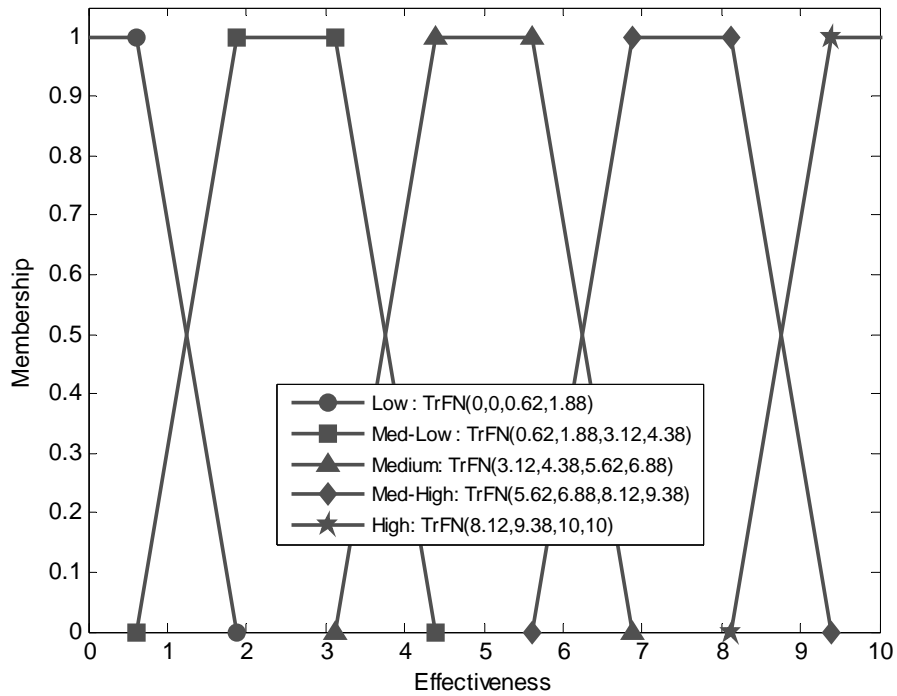


Figure 5-16. Membership functions of different states for regional defensive criteria

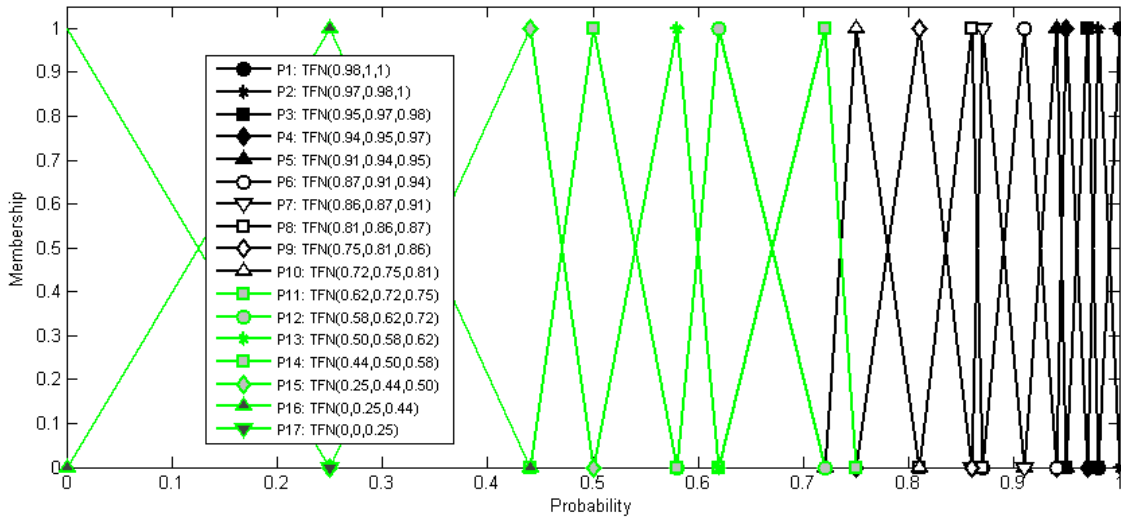
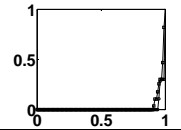
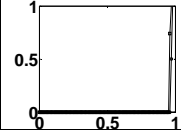
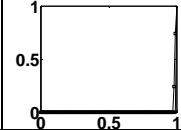
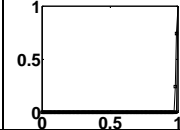
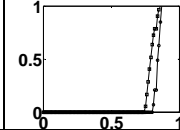


Figure 5-17. Output fuzzy sets for the regional security model.

Table 5-26. Notional rules for security system effectiveness assessment in the region

Output Set	Rule Number, Z
P01	0-30, 35, 40, 45, 50-55, 60, 65, 70, 75-80, 85, 90, 95, 100-105, 110, 115, 120
P02	31
P03	32, 36, 56
P04	33, 41, 81
P05	34, 37, 46, 57, 61, 106
P06	38, 42, 58, 66, 82, 86
P07	39, 47, 59, 62, 71, 107, 111
P08	43, 83, 91
P09	44, 48, 63, 67, 84, 87, 96, 108, 116
P10	49, 64, 72, 109, 112, 121
P11	68, 88, 92
P12	69, 73, 89, 97, 113, 117
P13	93
P14	74, 114, 122
P15	94, 98, 118
P16	99, 119, 123
P17	124

Table 5-27. Assessed values for the regional defensive criteria for each attack mode

Asset	Probability of Regional Success				
	Hand Emplaced	Ground Vehicle	Manned Aerial Vehicle	Unmanned Aerial Vehicle	Waterborne Vehicle
Detection (W_1)	1	3	1	1	2
Response (W_2)	3	3	0	0	7
Defeat (W_3)	9	5	0	0	9
$\Pr(S_R A)^*$					

*Note: Each plot shows the p-box corresponding to the random set derived from the approximate reasoning model. The left and right bounds are the cumulative plausibility and cumulative belief functions, respectively. The x-axis is the probability $\Pr(S_A|A, S_R)$ and the y-axis is the epistemic CDF on this probability.

5.5. CAPRA Risk Assessment

Elaboration on the specific initiating events under the IED class of scenarios is described in section 5.3.1. For the purpose of this study, it is assumed that the effects of an attack are independent at the asset level; that is, simultaneous attacks against multiple assets does not affect each asset's security and response and recovery system. However, when considered at the regional level, the baseline asset-level effects can be combined in a linear manner, which then can be discounted in aggregate form according to the target capabilities. This study focuses only on scenarios involving an attack against a single asset using a single delivery mode, though with additional computational resources, this model can be extended to look at multiple simultaneous attacks at regional assets.

5.5.1. Consequence and Severity Assessment

Loss conversion factors are used to bring all dimensions of loss into consistent units such as dollars to enable aggregation of loss (Ayyub 2003). For the public health and safety consequence dimension, a simple fuzzy number under the label “fuzzy value of life” (FVOL) can be constructed using the data compiled by Viscusi and Aldy (2003) on the statistical value of life used by various US regulatory agencies between 1985 and 2000 (Table 5-27). The reason for expressing value of life as a fuzzy number is due in part to the inherent inter-individual and inter-organizational ambiguity of the appropriate value of life for use in different contexts. The membership function for the FVOL used in this analysis is shown in Figure 5-18, where each α -cut corresponds to the inner α -percentile and the median is corresponds to the single-valued support at $\alpha = 1$. Treating the FVOL as a consequence conversion factor (Ayyub 2003), the total equivalent fatalities valued in dollars can be obtained by multiplying the number of fatalities by the FVOL using fuzzy interval arithmetic described in Appendix A (Ayyub and Klir 2007).

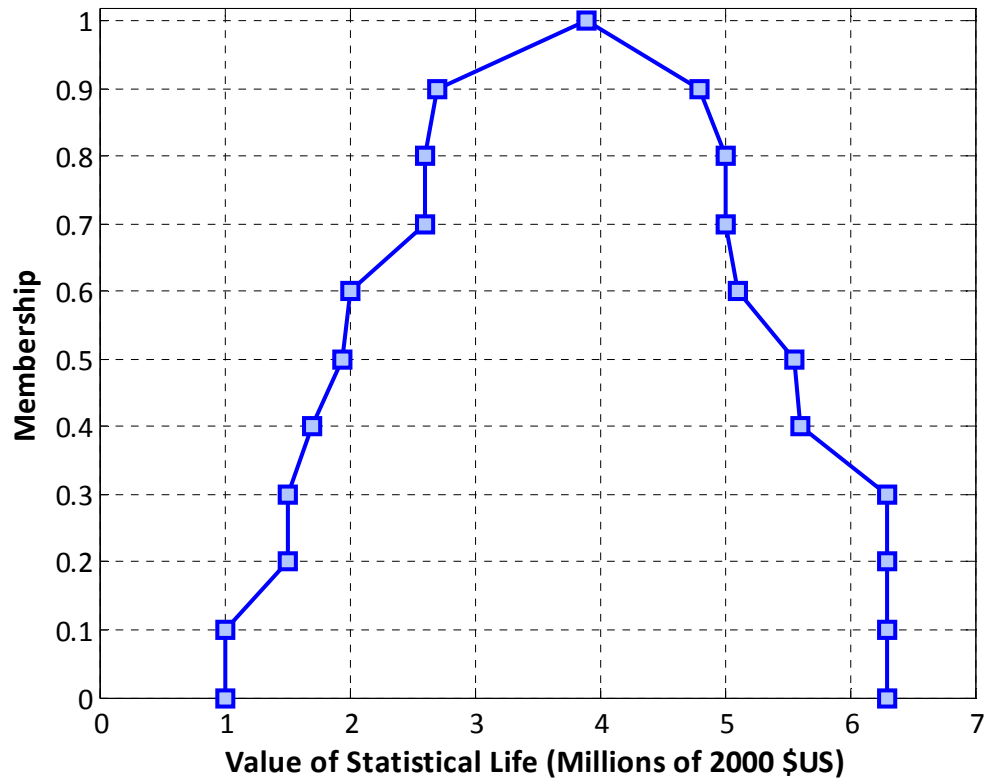


Figure 5-18. Fuzzy value of life (FVOL) derived from data of Viscusi and Aldy (2003)

Table 5-28. Date on value of statistical life (Viscusi and Aldy 2003)

Agency, Source (Rule) [Year]	Value (2000 \$US)
Federal Aviation Administration , Protective Breathing Equipment (50 FR 41452) [1985]	1.0
Environmental Protection Agency , Regulation on Fuels and Fuel Additives; Gasoline Lead Content (50 FR 9400) [1985]	1.7
Federal Aviation Administration , Improved Survival Equipment for Inadvertent Water Landings (53 FR 24890) [1988]	1.5
Environmental Protection Agency , Protection of Stratospheric Ozone (53 FR 30566) [1988]	4.8
Federal Aviation Administration , Proposed Establishment of the Harlingen Airport Radar Service Area, TX (55 FR 32064) [1990]	2.0
Food and Nutrition Service (USDA) , National School Lunch Program and School Breakfast Program (59 FR 30218) [1994]	1.7, 3.5
Consumer Product Safety Commission , Multiple Tube Mine and Shell Fireworks Devices (60 FR 34922) [1995]	5.6
Food Safety Inspection Service (USDA) , Pathogen Reduction; Hazard Analysis and Critical Control Point Systems (61 FR 38806) [1996]	1.9
Food and Drug Administration , Regulations Restricting the Sale and Distribution of Cigarettes and Smokeless Tobacco to Protect Children and Adolescents (61 FR 44396) [1996]	2.7
Federal Aviation Administration , Aircraft Flight Simulator Use in Pilot Training, Testing, and Checking and at Training Centers (61 FR 34508) [1996]	3.0
Environmental Protection Agency , Requirements for Lead-Based Paint Activities in Target Housing and Child-Occupied Facilities (61 FR 45778) [1996]	6.3
Food and Drug Administration , Medical Devices; Current Good Manufacturing Practice Final Rule; Quality System Regulation (61 FR 52602) [1996]	5.5
Environmental Protection Agency , National Ambient Air Quality Standards for Ozone (62 FR 38856) [1997]	6.3
Environmental Protection Agency , Radon in Drinking Water Health Risk Reduction and Cost Analysis (64 FR 9560) [1999]	6.3
Environmental Protection Agency , Control of Air Pollution from Motor Vehicles: Tier 2 Motor Vehicle Emissions Standards and Gasoline Sulfur Control Requirements (65 FR 6698) [1999]	3.9, 6.3
Consumer Product Safety Commission , Portable Bed Rails; Advance Notice of Proposed Rulemaking (65 FR 58968) [2000]	5.0

The consequence conversion factor for disruption depends on the nature of the specific services disrupted, and is taken as the equivalent dollar value of lost income that would otherwise be generated from services per day per percentage disruption (i.e., converts disruption time/degree into dollars). This model assumes a continuous proportionality relationship between the economic value of a service and degree and duration of disruption. Accordingly, the factor depends on the specific assets affected by

an event. The consequence conversion factors for disruption in this case study is expressed as a possibility distribution (see Table 5-7) with core centered at a nominal value and the support spanning $\pm 5\%$ to accommodate the ambiguity imposed by the qualifying adverb “about.”

The aggregate loss considering all relevant loss dimensions (public health and safety loss and disruption loss, in this case) can be obtained for each attack profile by first multiplying the conditional loss valued in the natural units of each dimension by the loss conversion factor to bring each dimension to consistent units, then summing together the losses for each dimension under the assumption of unknown, but non-negative dependence (see Appendix A, Section A-7). The only assumption made here is that, for example, there is at least a non-negative correlation between losses from each natural dimension (e.g., the probability that an increase in public health and safety loss will consistently correlate to a decrease in disruption loss is assumed to be zero). Typical results for aggregate loss from this assumption are shown in Figure 5-19, which gives the conditional cumulative distribution function on aggregate loss given a successful attack against the office building with a ground vehicle explosive. A summary of aggregate loss results for all five assets and corresponding attack profiles is provided in Appendix B, Section B.3.

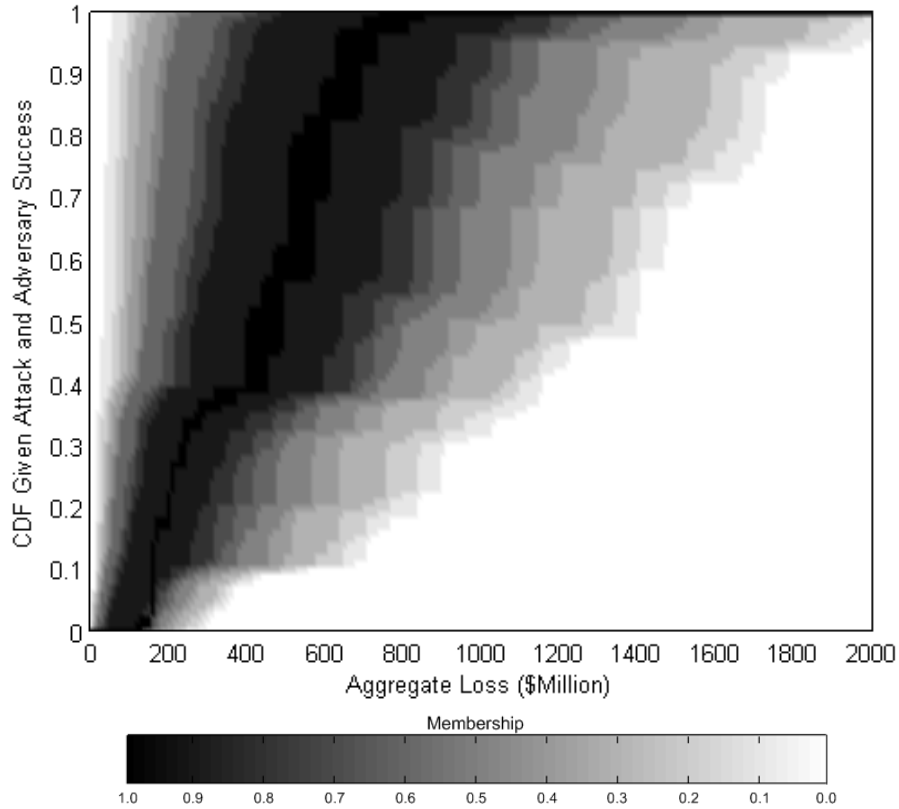


Figure 5-19. Conditional cumulative distribution on aggregate loss valued in dollars for the office building subject to a ground vehicle attack

5.5.2. Overall Vulnerability Assessment: Security Vulnerability Assessment

Given two layers of defenses, namely regional defenses and target (i.e., asset) defenses, adversary success requires the adversary to first defeat regional defenses, and if successful, defeat target defenses. The probability of adversary success, $\Pr(S | A)$, can thus be expressed as the joint probability of the adversary defeating both regional defenses (denoted by the event S_R) and target defenses (denoted by the event S_A), $\Pr(S_A, S_R | A)$ or:

$$\begin{aligned}
\Pr(S | A) &= \Pr(S_A, S_R | A) \\
&= \Pr(S_A | S_R, A) \Pr(S_R | A) \\
&= \tilde{P}_A \tilde{P}_R
\end{aligned} \tag{5-10}$$

where \tilde{P}_A and \tilde{P}_R are obtained from Eqs. 5-3 and 5-8, respectively.

5.5.3. Conditional Loss Given Attack

According to the theorem of total probability (Ayyub and McCuen 2002), the conditional cumulative distribution function on loss L , whether public health and safety, disruption, or aggregate, given attack with attack profile P can be obtained according the following Equation:

$$\Pr(L < l | P) = 1 - (1 - \Pr(L < l | S, A)) \Pr(S | A) \tag{5-11}$$

where $\Pr(S | A)$ is obtained from Eq. 5-10. Since the fuzzy systems \tilde{P}_A and \tilde{P}_R comprising $\Pr(S | A)$ produce random sets as outputs, the conditional cumulative distribution on loss in Eq. 5-11 is characterized by a random set at each level of loss l . To the author's knowledge, there is no convenient mechanism for displaying this level of uncertainty in compact form on a single plot; however, a set of *pignistic percentiles* can be constructed for each level of loss (see Appendix A), from which a series of *pignistic percentile distributions* can be constructed at different percentile levels.

5.5.4. Threat Probability Assessment

According to the assumptions underlying the proportional attractiveness model described in Chapter 3, Section 3.5.1 combined with an assumed visibility of one ($\Pr(V) = 1$) for all assets and attack profiles and a bias parameter $b = 1$, the probability of attack for each attack profile given an attack at the asset is shown in Figure 5-20. These probabilities were determined according to the 99th-percentile value of the 99th pignistic percentile conditional aggregate loss (i.e., worst-case, optimistic rational adversary) distributions described in Appendix B, Section B.4. The results in Figure 5-20 can be combined with the results for the conditional loss distributions given attack determined from Eq. 5-11 to obtain the conditional loss distribution given attack at an asset, all relevant attack profiles considered. To obtain the conditional loss distribution given attack for the region, all assets and attack profiles considered, the probability of attack at each asset is necessary. The resulting probability of attack at each asset was determined as shown in Figure 5-21.

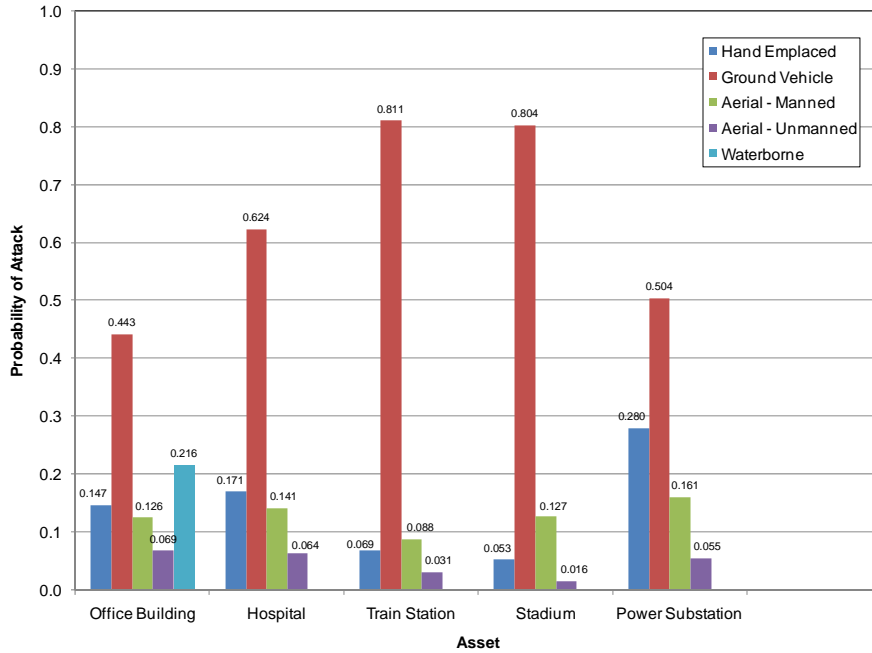


Figure 5-20. Probability of attack for alternative attack modes for each asset

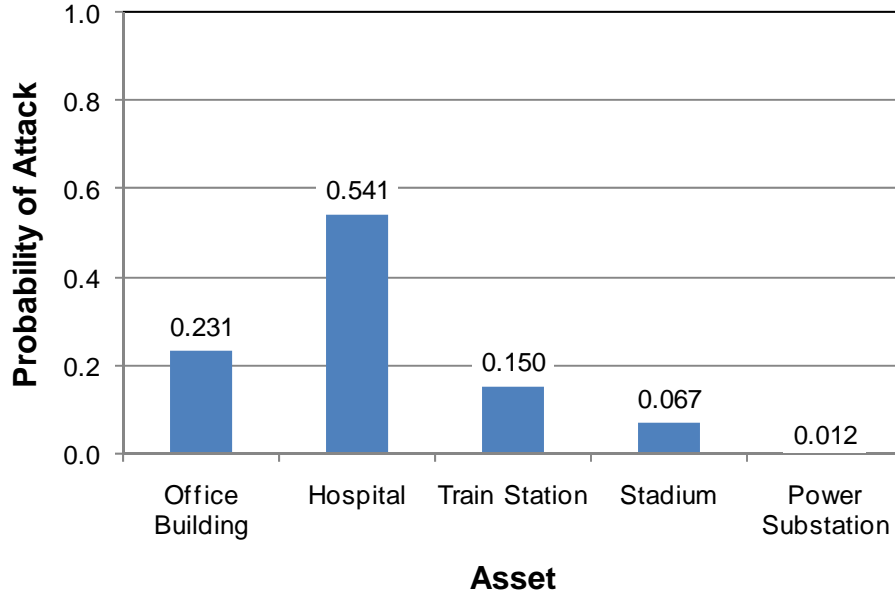


Figure 5-21. Relative probability of attack for each asset in the region

Given a baseline estimate on the rate of occurrence or probability of an attack affecting one or more of the five regional assets, an approximate model that relates a subset of the 37 capabilities to actual attack probability can be constructed leveraging approximate reasoning techniques. Table 5-2 summarizes a mapping of capabilities to the loss variable “threat occurrence.” The approximate relationship, $\tilde{\lambda}$, between relevant capabilities y_λ and percentage reduction in attack recurrence rate, λ can be expressed as:

$$\rho_\lambda = \tilde{\lambda}(y_\lambda) \quad (5-12)$$

Note that according to the arguments of the function in Eq. 5-12, this model assumes independence between the ability of the region to decrease the probability of attack and the baseline estimate for this probability. The reason for this assumption is that any dependence between capabilities and the baseline estimate, given the inherent subjectivity associated with estimating an annual recurrence rate or probability of attack, creates a situation where the output risk profiles may be overly sensitive to the initial subjective estimates of baseline probability of attack.

According to Table 5-2, 6 regional capabilities are assumed to contribute and interact toward reducing the number of fatalities following an adverse initiating event. As was done in Section 5.4 for loss, each capability Y_j is allowed to assume one of two states – “effective” or “ineffective” – with membership functions shown in Figure 5-11 constructed over the bounded domain [0,10]. This results in $2^6 = 64$ rules according to Eq. A-9. The percentage loss, ρ_λ , can assume one of five output sets as shown in Figure

5-22 constructed over the bounded domain [0,100%]. The rules for this case are given in Table 5-29.

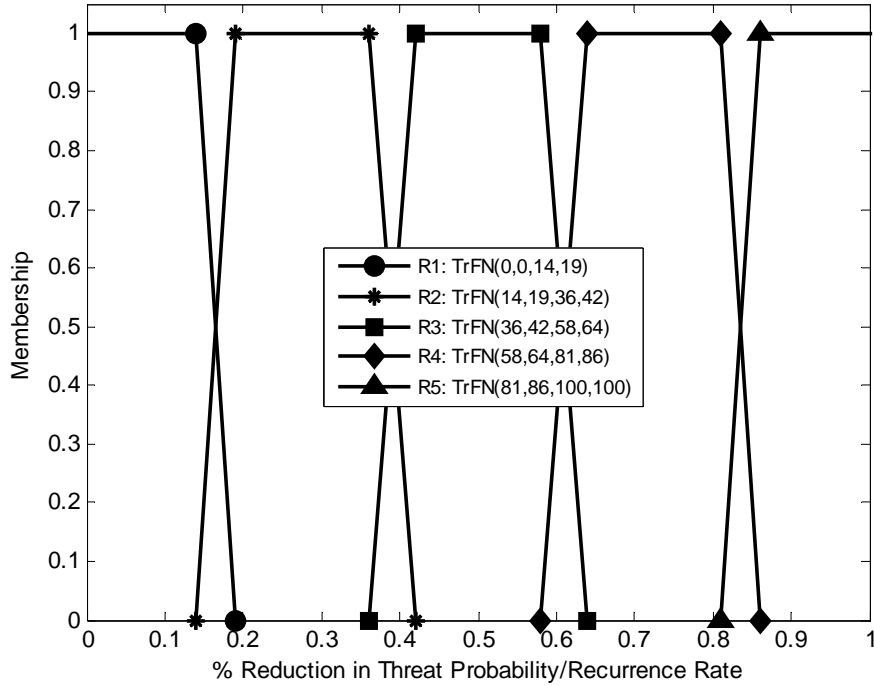


Figure 5-22. Output sets for % reduction in threat probability or recurrence rate

Table 5-29. Rules for threat probability / recurrence reduction

Output Set	Rule Number, Z
R1	0-6, 8-10, 12, 16-18, 20, 24, 32-34, 36, 40, 48
R2	7, 11, 13-14, 19, 21-22, 25-26, 28, 35, 37-38, 41-42, 44, 49-50, 52, 56
R3	15, 23, 27, 29-30, 39, 43, 45-46, 51, 53-54, 57-58, 60
R4	31, 47, 55, 59, 61, 62
R5	63

Given the output from the approximate reasoning model in Eq. 5-12, the total cumulative distribution on loss L can be determined according to the theorem of total probability as follows:

$$\Pr(L < l) = 1 - (1 - \Pr(L < l | A))\Pr(A)\rho_\lambda \quad (5-13)$$

where $\Pr(L < l | A)$ is the conditional cumulative distribution function for loss given an attack in the region, all assets and associated attack profiles considered. A summary of the conditional aggregate loss distributions and membership functions for the mean loss over a wide set of pignistic percentile distributions for each asset is provided in Appendix B, Section B.5.

5.5.5. Regional Risk Profiles and Actionable Risk Information

According to the input information and procedures described in the previous sections of this chapter and the results obtained as shown in Appendix B, the conditional aggregate loss and membership functions for different percentiles of aggregate loss given attack in the region are obtained as shown in Figures 5-24 and 5-25, respectively.

Considering a fixed assumed probability of attack of 0.05 for a time period spanning 5 years (as defined in Section 5.2), the regional risk profile for an attack occurring against a single asset among the five in the region within the next 5 years is shown in Figure 5-25.

Table 5-30 presents the results of Figure 5-25 in numerical matrix form in order to highlight the values of loss at a variety of percentile values and for a variety of pignistic percentile curves.

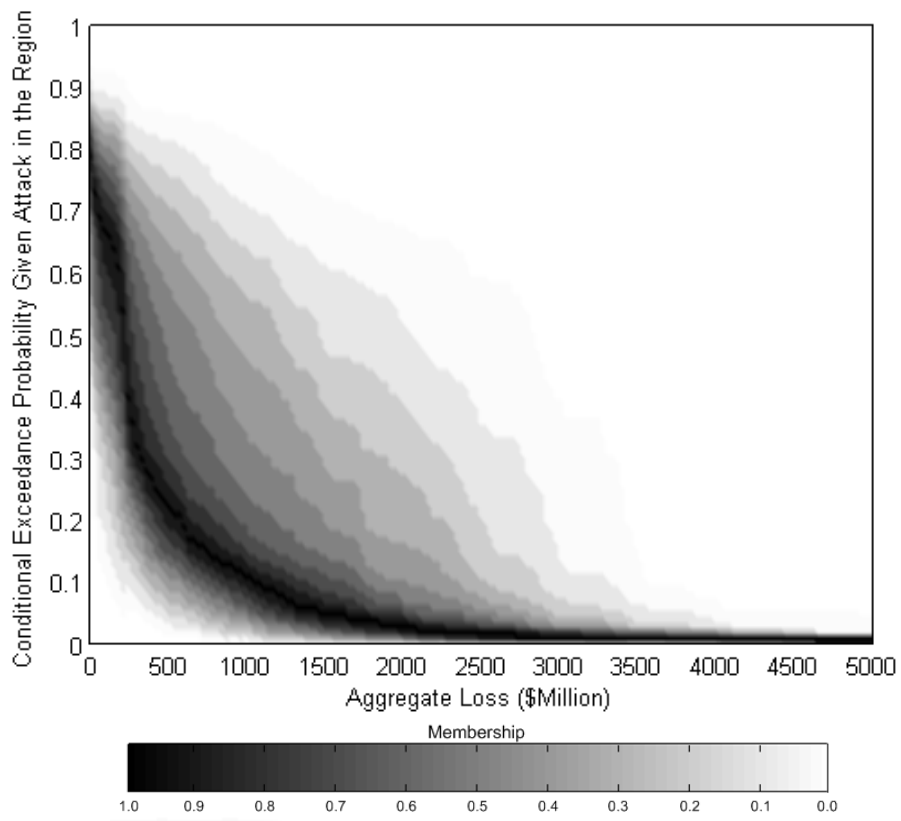


Figure 5-23. Possibilistic conditional aggregate loss-exceedance curve given an attack in the region

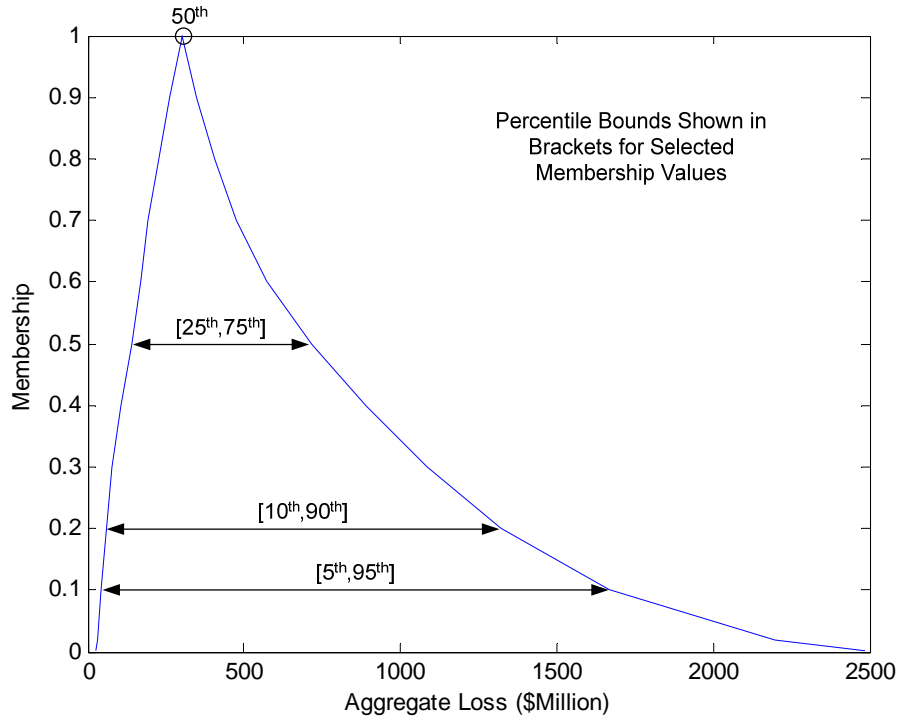


Figure 5-24. Membership function for the conditional mean aggregate loss in the region given attack

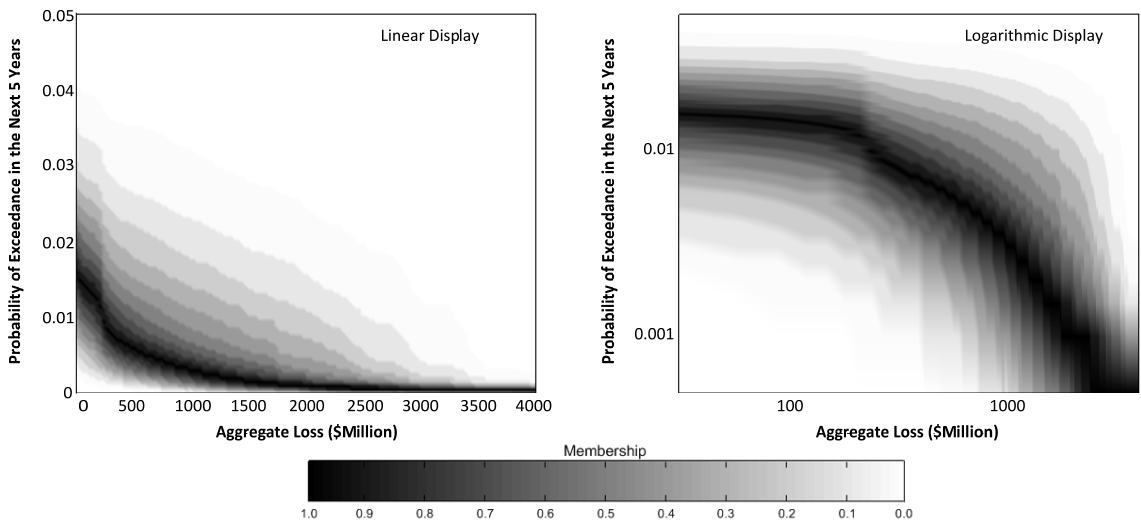


Figure 5-25. Possibilistic loss-exceedance curve in light of explosive attacks occurring in the region against one of the five assets in the next 5 years

Table 5-30. Matrix of levels of loss for different pignistic percentile distributions and degrees of probability of exceedance

Pignistic Percentile Distribution	Mean	Aggregate Loss Values (\$Millions) for Different Probabilities of Exceedance										
		0.99	0.95	0.90	0.75	0.70	0.50	0.25	0.10	0.05	0.01	
0.00	1											497
0.01	1										22	601
0.05	3										86	738
0.10	5								27	182	942	
0.25	13								184	415	1,392	
0.50	43							130	453	809	1,912	
0.75	124							328	937	1,264	2,609	
0.90	310						184	947	1,599	1,849	3,090	
0.95	493						388	1,322	1,912	2,129	3,746	
0.99	908				172	298	1096	1,829	2,339	2,458	5,039	

Note: Empty cells indicate a value of zero

To better advise decision makers on strategies for cost-effective risk reduction in the event that the decision maker's risk exposure was determined to be unacceptable, each relevant regional capability was adjusted to its maximum favorable value ($p = 100\%$) using the sensitivity analysis method described in Eq. 3-34) to determine the impact it had on various pignistic percentile distributions at different percentile levels. Table 5-31 summarizes the results from this inquiry, where from this table it is suggested that improving CBRNE detection capabilities (Y_6) and enhancing information collection and recognition of indications capabilities (Y_7) present the greatest opportunity for reducing risk. In contrast, this analysis also suggests that any improvement in planning (Y_3), counter-terror investigations (Y_9), citizen evacuation (Y_{15}), and several other capabilities (Y_{17} , Y_{26} , Y_{31} , and Y_{32}) offers no benefit risk reduction.

Table 5-31. Sensitivity of the risk results to favorable changes in each regional capability

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Universal Detection Capabilities	Mean	0.04	0.01	0.02	0.04	0.04	0.04	0.05	0.05
	0.01								
	0.05								
	0.25	0.60	0.98						
	0.50	0.26	0.16	0.46		0.00			
	0.75	0.08	0.02	0.06	0.15	0.34			
	0.95	0.03	0.01	0.00	0.04	0.06	0.14	0.20	0.61
	0.99	0.02		0.00	0.02	0.01	0.00	0.01	0.00
Improve Universal Response Capabilities	Mean	0.06	0.00	0.01	0.03	0.04	0.06	0.06	0.06
	0.01								
	0.05								
	0.25	0.53	0.82						
	0.50	0.27	0.19	0.49		0.00			
	0.75	0.10	0.02	0.07	0.22	0.27			
	0.95	0.03	0.01	0.01	0.06	0.06	0.08	0.10	0.19
	0.99	0.02		0.01	0.02	0.01	0.01	0.00	0.00
Improve Universal Defeat Capabilities	Mean	0.02		0.00	0.01	0.01	0.03	0.03	0.02
	0.01								
	0.05								
	0.25	0.12	0.13						
	0.50	0.09	0.06	0.18		0.00			
	0.75	0.02	0.01	0.02	0.08	0.06			
	0.95	0.01	0.00	0.00	0.03	0.02	0.02	0.03	0.06
	0.99	0.00			0.01	0.00	0.00		0.00
Improve Communications Capabilities (Y ₁)	Mean	0.04	0.02	0.02	0.04	0.03	0.04	0.04	0.04
	0.01								
	0.05								
	0.25	0.10	0.14						
	0.50	0.04	0.03	0.06		0.00			
	0.75	0.05	0.03	0.06	0.04	0.08			
	0.95	0.04	0.09	0.03	0.04	0.05	0.04	0.06	0.08
	0.99	0.06		0.04	0.03	0.02	0.08	0.05	0.10

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Community Preparedness and Participation Capabilities (Y ₂)	Mean	0.04	0.02	0.02	0.02	0.03	0.03	0.03	0.02
	0.01								
	0.05								
	0.25	0.21	0.31						
	0.50	0.12	0.08	0.19		0.00			
	0.75	0.04	0.02	0.03	0.08	0.12			
	0.95	0.02	0.02	0.01	0.01	0.03	0.05	0.11	0.33
	0.99	0.04			0.02	0.03	0.01	0.01	0.09
Improve Planning Capabilities (Y ₃)	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00
Improve Intelligence Information Sharing and Dissemination Capabilities (Y ₅)	Mean	0.07	0.01	0.03	0.05	0.06	0.07	0.06	0.06
	0.01								
	0.05								
	0.25	0.65	1.00						
	0.50	0.34	0.26	0.58		0.00			
	0.75	0.10	0.02	0.08	0.27	0.61			
	0.95	0.04	0.01	0.01	0.06	0.07	0.16	0.31	1.00
	0.99	0.02			0.01	0.01	0.01	0.02	0.01
Improve CBRNE Detection Capabilities (Y ₆)	Mean	0.17	0.06	0.08	0.15	0.17	0.18	0.15	0.15
	0.01								
	0.05								
	0.25	0.83	1.00						
	0.50	0.53	0.48	0.72		0.00			
	0.75	0.25	0.05	0.18	0.54	1.00			
	0.95	0.11	0.09	0.03	0.13	0.19	0.41	1.00	1.00
	0.99	0.08		0.07	0.06	0.05	0.08	0.05	0.11

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Information Gathering and Recognition of Indications and Warning Capabilities (Y ₇)	Mean	0.12	0.04	0.05	0.09	0.11	0.11	0.10	0.11
	0.01								
	0.05								
	0.25	0.73	1.00						
	0.50	0.47	0.39	0.68		0.00			
	0.75	0.18	0.03	0.13	0.43	0.98			
	0.95	0.08	0.04	0.02	0.08	0.12	0.27	0.65	1.00
	0.99	0.05		0.01	0.02	0.03	0.05	0.03	0.09
Improve Intelligence Analysis and Production Capabilities (Y ₈)	Mean	0.07	0.01	0.03	0.05	0.06	0.07	0.06	0.06
	0.01								
	0.05								
	0.25	0.65	1.00						
	0.50	0.34	0.26	0.58		0.00			
	0.75	0.10	0.02	0.08	0.27	0.61			
	0.95	0.04	0.01	0.01	0.06	0.07	0.16	0.31	1.00
	0.99	0.02			0.01	0.01	0.01	0.02	0.01
Improve Counter-Terror Investigations and Law Enforcement Capabilities (Y ₉)	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00
Improve Citizen Evacuation and Shelter-In-Place Capabilities (Y ₁₅)	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Critical Resource Logistics and Distribution Capabilities (Y_{16})	Mean	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.01
	0.01								
	0.05								
	0.25	0.06	0.10						
	0.50	0.01	0.00	0.01		0.00			
	0.75	0.02	0.01	0.01	0.02	0.07			
	0.95	0.01	0.01	0.00	0.00	0.01	0.01	0.02	0.02
	0.99	0.03			0.02	0.01	0.01	0.01	0.09
Improve Emergency Operations Center Management Capabilities (Y_{17})	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00
Improve Emergency Public Information and Warning Capabilities (Y_{18})	Mean	0.04	0.02	0.02	0.04	0.03	0.04	0.04	0.04
	0.01								
	0.05								
	0.25	0.10	0.14						
	0.50	0.04	0.03	0.06		0.00			
	0.75	0.05	0.03	0.06	0.04	0.08			
	0.95	0.04	0.09	0.03	0.04	0.05	0.04	0.06	0.08
	0.99	0.06		0.04	0.03	0.02	0.08	0.05	0.10
Improve Fatality Management Capabilities (Y_{21})	Mean	0.05	0.02	0.02	0.05	0.05	0.05	0.06	0.05
	0.01								
	0.05								
	0.25	0.12	0.16						
	0.50	0.06	0.06	0.08		0.00			
	0.75	0.07	0.04	0.09	0.06	0.09			
	0.95	0.06	0.10	0.07	0.06	0.06	0.08	0.08	0.11
	0.99	0.06		0.03	0.03	0.03	0.10	0.05	0.10

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Fire Incident Response Support Capabilities (Y ₂₂)	Mean	0.03	0.02	0.01	0.02	0.02	0.03	0.02	0.02
	0.01								
	0.05								
	0.25	0.09	0.13						
	0.50	0.02	0.02	0.02		0.00			
	0.75	0.03	0.02	0.02	0.03	0.08			
	0.95	0.03	0.09	0.02	0.03	0.02	0.02	0.04	0.05
	0.99	0.05		0.01	0.03	0.02	0.02	0.04	0.10
Improve Mass Care (Sheltering, Feeding, and Related Services) Capabilities (Y ₂₄)	Mean	0.01	0.01	0.00	0.01	0.01	0.01	0.01	0.01
	0.01								
	0.05								
	0.25	0.06	0.10						
	0.50	0.01	0.00	0.01		0.00			
	0.75	0.02	0.01	0.01	0.02	0.07			
	0.95	0.01	0.01	0.00	0.00	0.01	0.01	0.02	0.02
	0.99	0.03			0.02	0.01	0.01	0.01	0.09
Improve Medical Supplies Management and Distribution Capabilities (Y ₂₆)	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00
Improve Medical Surge Capabilities (Y ₂₇)	Mean	0.05	0.02	0.02	0.05	0.05	0.05	0.06	0.05
	0.01								
	0.05								
	0.25	0.12	0.16						
	0.50	0.06	0.06	0.08					
	0.75	0.07	0.04	0.09	0.06	0.09			
	0.95	0.06	0.10	0.07	0.06	0.06	0.08	0.08	0.11
	0.99	0.06		0.03	0.03	0.03	0.10	0.05	0.10

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles						
			0.01	0.05	0.25	0.50	0.75	0.95	0.99
Improve Onsite Incident Management Capabilities (Y_{28})	Mean	0.04	0.02	0.02	0.04	0.03	0.04	0.04	0.04
	0.01								
	0.05								
	0.25	0.10	0.14						
	0.50	0.04	0.03	0.06					
	0.75	0.05	0.03	0.06	0.04	0.08			
	0.95	0.04	0.09	0.03	0.04	0.05	0.04	0.06	0.08
	0.99	0.06		0.04	0.03	0.02	0.08	0.05	0.10
Improve Emergency Public Safety and Security Response Capabilities (Y_{29})	Mean	0.03	0.02	0.01	0.02	0.02	0.03	0.02	0.02
	0.01								
	0.05								
	0.25	0.09	0.13						
	0.50	0.02	0.02	0.02		0.00			
	0.75	0.03	0.02	0.02	0.03	0.08			
	0.95	0.03	0.09	0.02	0.03	0.02	0.02	0.04	0.05
	0.99	0.05		0.01	0.03	0.02	0.02	0.04	0.10
Improve Responder Safety and Health Capabilities (Y_{30})	Mean	0.04	0.02	0.02	0.04	0.03	0.04	0.04	0.04
	0.01								
	0.05								
	0.25	0.10	0.14						
	0.50	0.04	0.03	0.06		0.00			
	0.75	0.05	0.03	0.06	0.04	0.08			
	0.95	0.04	0.09	0.03	0.04	0.05	0.04	0.06	0.08
	0.99	0.06		0.04	0.03	0.02	0.08	0.05	0.10
Improve Emergency Triage and Pre-Hospital Treatment Capabilities (Y_{31})	Mean	0.00							
	0.01								
	0.05								
	0.25								
	0.50					0.00			
	0.75								
	0.95								
	0.99								0.00

Table 5-31. (continued)

Strategy	CDF Value	Mean	Pignistic Percentiles							
			0.01	0.05	0.25	0.50	0.75	0.95	0.99	
Improve Search and Rescue (Land Rescue) Capabilities (Y_{32})	Mean	0.00								
	0.01									
	0.05									
	0.25									
	0.50					0.00				
	0.75									
	0.95									
	0.99									0.00
Improve Economic and Community Recovery Capabilities (Y_{35})	Mean	0.04	0.02	0.02	0.04	0.03	0.04	0.04	0.04	0.04
	0.01									
	0.05									
	0.25	0.10	0.14							
	0.50	0.04	0.03	0.06		0.00				
	0.75	0.05	0.03	0.06	0.04	0.08				
	0.95	0.04	0.09	0.03	0.04	0.05	0.04	0.06	0.08	
	0.99	0.06		0.04	0.03	0.02	0.08	0.05	0.10	

5.6. Discussion

This case study focused on applying the CAPRA methodology developed in Chapter 3 to assess the risks associated with a portfolio of assets in a region due to malicious explosive events. The information used to support this analysis was highly uncertain, and consequently the outputs assumed the form of a nested set of probability boxes defined according to their percentiles values or membership values. However, as this case study demonstrates, even highly uncertain expressions of model parameters can be synthesized to produce meaningful statements of risk that avoid the *fallacy of irresponsible precision*, or rather the tendency to communicate a high degree of precision that cannot be justified on the basis of less precise inputs.

To assist in obtaining rapid assessments of probability of adversary success in light of target and regional capabilities, this case study leveraged techniques from approximate reasoning to approximate the true functional relationship between several input variable and resulting security system effectiveness. Unlike the previous case study in Chapter 4, this case study took for granted cooperation with asset owners to obtain asset-level security information. However, in practice this level of cooperation is not ensured, but rather may come at a cost in terms of reciprocal support or in terms of decrease tolerance for future interactions. In lieu of this approximate reasoning approach, the regional analyst could leverage any available information on adversary probability success at the asset so long as the approach taken to make this asset-level assessment is compatible with the CAPRA methodology. For example, the approach used in the case study in Chapter 4 could be used in place of the Chapter 5 approach provided it was employed at the asset level and the asset owner is willing to share it with regional decision makers.

Approximate reasoning techniques were also essential for mapping the 37 capabilities to risk for the purposes of demonstrating to funding agencies how an improvement in one capability will lead to decreased risk overall in order to make a business case for investment. In the interest of tailoring the specifics of the CAPRA methodology to meet the needs of a regional decision maker, approximate models were constructed to relate the degree of effectiveness of each capability to its ability to reduce consequence for any degree of basis loss and to reduce the probability of an attack occurring. However, since basis loss was expressed in terms of a simple triangular possibility distribution whose characteristic points were directly elicited from regional

decision makers, the result of this model was a series of probability boxes at different degrees of membership. While this representation of information is highly uncertain, the result from this analysis remains true to the nature of the uncertainties in the underlying model inputs and the understanding of how capabilities relate to risk. That is, this case study demonstrated that the CAPRA model can still produce useful risk information even in the face high uncertainty.

While it was not described explicitly in the case study itself, this analysis applied techniques for fuzzy systems in a way not previously done in the literature, that is, as a tool for approximating a function that would otherwise be developed using statistical or actuarial techniques. To the author's knowledge, the use of random sets in conjunction with fuzzy inference (described in detail in Appendix A) not to produce a defuzzified crisp output, but to preserve, to the maximum extent possible, all the uncertainties in inputs and model has not been discussed in the literature.

This study also demonstrated a simple first-order approach to capturing losses due to interdependencies which, in some sense, amounts to deriving a consequence conversion factor on loss that considers broader impacts than just lost service of the afflicted system. Though more rigorous methods are available for capturing the aggravating effects of secondary asset disruption due to disruption of a dependent asset (e.g., Lee et al. 2007), the approach used in this case study has the benefit of being quick, and for the most part, conservative in that it does not account for substitution effects that tend to emerge over time. However, similar to its more rigorous counterparts, the approach for considering interdependencies is limited in scope to dependencies among assets within the portfolio under study, and do not consider contributions to risk

stemming from the disruption of assets external to the portfolio. This important line of study, that is consideration of both internal and external dependencies to a portfolio, is a subject in need of future research attention. For example, the Department of Homeland Security is presently considering this problem in terms of US dependence on foreign infrastructure, or more generally, US dependence on infrastructure that is outside the national infrastructure portfolio (Poptanich 2008).

Another key innovation demonstrated in this case study was the use of a fuzzy value of life to accommodate the inherent vagueness in the appropriate value of life for different individuals and contexts. This fuzzy value of life was overlaid atop expressions for equivalent fatalities to obtain a monetarily equivalent expression for public health and safety loss. By leveraging fuzzy sets for the purposes of converting consequence expressed in one loss dimension to another, the hope was that any concern on what the actual value of life should be would be alleviated by accommodating a family of reasonable values for this factor.

Future work will explore ways in which to mine unstructured data sets to extract inference rules from previous incidents, reports, narratives, and simulation results, for the purposes of examining the role of the capabilities in reducing the consequences associated with different naturally occurring and anthropic events and for different dimensions of consequence. Data mining or machine learning techniques offer a potentially significant improvement over the current brute force approach employed in the present study for obtaining inference rules. Also, this approach would enable finer resolution models that would ultimately reduce the uncertainties associated function approximation.

Chapter 6. Conclusions and Future Work

6.1. General Discussion

The research described in the previous chapters developed an overarching methodology for critical asset and portfolio risk analysis for security events, with a demonstration for explosive attacks in particular. Homeland security risk analysis problems are large in scope, and accordingly any methodology used to make sense of the risks afflicting homeland security decision makers at any level of leadership and system abstraction necessarily must accommodate many factors, some of which whose values extend beyond the ability of a given decision maker to assess or control. This was demonstrated in the case study in Chapter 4, where the asset owner had to make conservative assumptions for model parameters to compensate for missing information on other assets and regional emergency response capabilities. However, even without values for some of the model parameters, decision makers must still make decisions. As was shown, the CAPRA methodology provides a framework for decision support despite missing information by defaulting to conservative assumptions when necessary.

The CAPRA methodology meets all of the requirements outlined in Chapter 1, Section 1.2 of this research. In particular:

- The structure of the CAPRA methodology allows for a sensitivity analysis to be performed on the baseline estimate of risk so as to provide actionable risk information to homeland security decision makers. This sensitivity analysis can be used to target specific risk variables for risk reduction, or to bolster a case for

enhanced cooperation with other stakeholders to alleviate any conservative assumptions made to compensate for missing information.

- The CAPRA methodology builds upon accepted thinking and understanding of security risk analysis (i.e., the Risk = Threat times Vulnerability time Consequence model). This methodology considers all aspects of the security risk analysis problem – to include consequence, vulnerability, and threat – and in fact, establishes a new operational definition for overall vulnerability that highlights those contributors to vulnerability beyond security countermeasures. Moreover, the CAPRA methodology redefines the role of consequence and severity assessment, in particular by using this phase to clearly articulate those consequence dimensions of concern to a decision maker and the spectrum of severity up to an event-neutral maximum potential loss. Threat probability assessment is also accommodated, even in the absence of specific information on current adversary plans and activities, to produce meaningful probabilities of attack based on adversary behavior, knowledge, and perceptions.
- The mathematical structure of the CAPRA methodology, as a purely probabilistic model at its core, expresses risk in terms of a probability distribution over suitable dimensions of loss. The high-level sequence of events between cause and consequence follow a logical progression beginning with an initiating event and then through a series of barriers or interventions to arrive at a particular degree of loss. Moreover, the CAPRA methodology allows for expression of model parameters in a variety of quantitative forms, and consequently produces risk information that remains faithful to the imprecision of the underlying inputs.

- As was demonstrated in the two case studies, the CAPRA methodology is scalable to accommodate the needs of decision makers at all levels of abstraction and leadership, including operational and strategic asset, sectoral, and regional analysis. While the CAPRA methodology accepts that each decision maker has his or her own interests, such as a focus on different dimensions and scope of loss, the general philosophy underpinning the methodology is consistent across all stakeholders. This feature promotes statements of compatibility between the results of the CAPRA methodology, and avoids any need for discussion on how the results were obtained. Moreover, under the CAPRA framework, a business case can be made for sharing of information across stakeholders for the purpose of obtaining the most accurate representations of risk possible that consider factors that are both internal and external to the decision maker's decision space.
- A key innovation described in this research is the ability of the CAPRA methodology to make judgments of threat probability without intelligence information on specific adversary activities. Rather, the proportional attractiveness model discussed in this research assumes only that the adversaries behave as rational decision makers that choose from among a variety of visible options in proportion to the perceived value added from their compromise with respect to the adversary's goals and motivations. Consequently, the CAPRA methodology accommodates the dynamic nature of human adversaries, particularly their tendencies to shift preferences in response to security investments.

In general, there is no single approach to obtaining values for the parameters of the CAPRA methodology. As the two case studies in Chapters 4 and 5 demonstrate, different techniques can be used to obtain values for, say, the security system effectiveness (i.e., systems reliability modeling in Chapter 4, and approximate reasoning in Chapter 5). As an example, some of the parameters, such as response and recovery and security system effectiveness may benefit in some context from the use of discrete event simulation or agent-based simulation. However, the CAPRA methodology provides a consistent mechanism for integrating information from various models. And more importantly, this research and the two case studies demonstrated that useful and actionable risk information can be produced even with limited information supporting precise estimates of model parameters.

6.2. Avenues for Future Research

Avenues for future research to further enhance the implementation of the CAPRA methodology in different contexts include, but are not limited to, the following:

- Considering strategies to validate the results produced by the CAPRA methodology. For example, depending on the level of abstraction at which the model is applied, such as at the regional level where the stakeholders represent public interests rather than at the asset level where the asset owner has little resources to support analysis, peer review of the parameter values and assumptions underlying their aggregation may be useful for assessing their reasonableness, and when appropriate, their accuracy. However, it must

be noted that since the CAPRA model focuses largely on security incidents, little data is available to make meaningful statistical comparisons with model predictions. More importantly, such data is typically undesirable to pursue since its availability implies humans have suffered from the effects of hazardous events. Another strategy might be to look at event precursors as a basis for assessing the probability of subsequent events that could have, but did not happen. For example, if an attack was attempted but was unsuccessful at defeating target defenses, precursor analysis would examine what would have happened had the adversary been successful for the purposes of comparison with initial predictions.

- In lieu of model validation, a promising line of research might be to bypass the validation question altogether, and instead explore the usefulness of the CAPRA methodology as a decision support tool in terms of the information and insights learned through its application. That is, to what extent does knowledge generated in the process of implementing CAPRA empower decision makers to make better decisions?
- Extending the CAPRA model to consider several or more operational states of an asset or portfolio. In general, all dimensions of vulnerability have a time element: changes in the situational environment (e.g., night versus day, rainy versus sunny, weekend versus weekday) may have an effect on one or more aspects of vulnerability. In many circumstances, an asset or system may be more or less vulnerable at different times depending on the situation at hand. It is thus important to identify an exhaustive set of *operational states*, and

independently conduct a vulnerability assessment of each. Along these lines, the CAPRA methodology can also be extended to support tactical decisions by integrating real time expressions of consequence, vulnerability, and threat likeliness and using this as a basis to allocate tactical resources so as to keep risk below a threshold level of acceptability (McGill and Ayyub 2006).

- Leverage the latest developments in human reliability analysis to assess the performance of humans (e.g., guard, first responders) in relation to the various types of situations characterized by the CAPRA methodology. For example, future work should examine the performance of guards at the individual and group level to determine probability of detection, response capabilities, and their ability to defeat specified types of adversaries. Such an implementation of human reliability analysis to security would enable more comprehensive and meaningful expressions of security system effectiveness that take into account guard training, response capabilities, cognitive and psychological factors.
- Explore the extent to which cooperation among homeland security stakeholders will yield positive (and perhaps negative) benefits to the individual and to society. As was demonstrated in the case studies in Chapters 4 and 5, different stakeholders have different needs, but in the absence of information from lower and higher levels, all decisions will be based on conservative estimates, and consequently may be suboptimal. To what extent does cooperation promote optimal decision making at both the individual and societal level? It is envisioned that the answer to such a question could

enhance arguments for or against cooperation among homeland security decision makers.

Appendix A. Fuzzy Sets, Fuzzy Logic, and Evidence Theory

A.1. Fuzzy Numbers and their Membership Functions

The basic building blocks of fuzzy logic are linguistic variables that can take on states described by fuzzy intervals. A *linguistic variable* is one that takes on linguistic values such as “strong” for a variable describing impact resistance of a crash barrier and “secure” for a variable defining the state of protection (Zadeh 1975). That is, a linguistic variable takes on values that have clear intension (“the barrier is strong”), but with a vague extension (we cannot be explicit about the resistance). In contrast to a *crisp number* whose value is precisely defined, a *fuzzy number* is a fuzzy set defined on the set of real numbers whose numeric meaning is ambiguous (Ayyub and Klir 2007). For example, the phrase “not unlikely” as a statement about likeliness and the phrase “catastrophic” as a statement about potential consequences are both fuzzy numbers in the sense that they express magnitude without precise quantification. Fuzzy numbers have been linked to possibility distributions by Zadeh (1999), which are a specific case of random sets (Alvarez 2006).

The degree of belonging or membership of a certain numeric value x to a fuzzy number X is characterized by a membership function $\mu(x)$ on the range $[0,1]$, where a membership of 1 indicates that x fully belongs to X , a membership value of 0 indicates that x does not belong to X , and values in between indicate that x partially belongs to X . Figure A-1, for example, shows a series of fuzzy numbers representing various degree of probability as derived from the data of Lichtenstein and Newman (1967) assuming a

single-valued core positioned at the published median value and the support spanning the range of responses for each probability phrase.

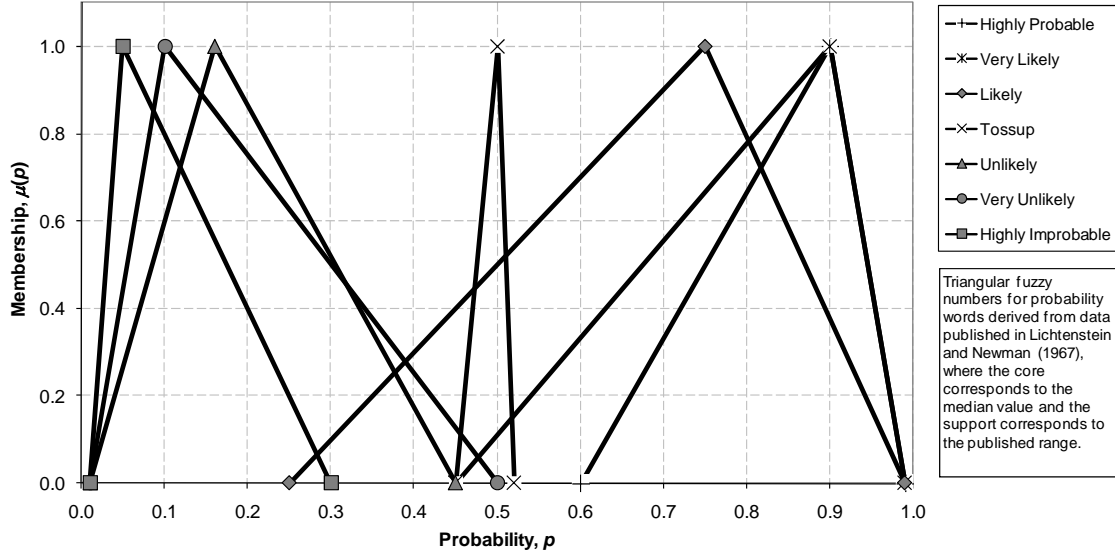


Figure A-1. Fuzzy numbers for selected probability words

The general form of a membership function for a fuzzy number X is as follows:

$$\mu(x) = \begin{cases} \mu_L(x) & a < x < b \\ 1 & b \leq x \leq c \\ \mu_R(x) & c < x < d \\ 0 & \text{Otherwise} \end{cases} \quad (\text{A-1})$$

where $\mu_L(x)$ and $\mu_R(x)$ are, respectively, non-decreasing and non-increasing functions of x on the range $[0,1]$. The fuzzy number described by the membership function in Eq. A-1 is known as a *generalized left-right fuzzy number*, or GLRFN (Dubois and Prade 1980). Note that a GLRFN is bell-shaped, and is defined by four characteristic points $\langle a, b, c, d \rangle$. The *core* of a fuzzy number X is defined as the interval where $\alpha = 1$ (i.e., $[b, c]$ in

Eq. A-1), and consists of all values of x that definitely belong to X . The *support* of a fuzzy number is defined as the interval where $\alpha > 0$ (i.e., (a, d) in Eq. A-1), and consists of all values of x that have at least a partial belonging to X . An *alpha-level* or *alpha-cut* of a fuzzy number, ${}^\alpha X$, defines the interval associated with a degree of membership α . In terms of the formulation for a GLRFN, the alpha-cut can be obtained from Eq. (A-1) as:

$${}^\alpha X = [\mu_L^{-1}(\alpha), \mu_R^{-1}(\alpha)] \quad (\text{A-2})$$

where $\mu_L^{-1}(\alpha)$ and $\mu_R^{-1}(\alpha)$ are the inverses of the functions used in Eq. A-1.

In practice, fuzzy numbers are commonly represented in a simplified or approximate form known as a *trapezoidal fuzzy number*, or TrFN. The membership function of a TrFN is *linearly increasing* on the interval $[a, b]$, *constant* on the interval $[b, c]$, and *linearly decreasing* on the interval $[c, d]$. That is, the shape of the membership function is piecewise linear with functions μ_L and μ_R of the form (from Eq. A-1):

$$\mu_L(x) = \left(\frac{x - a}{b - a} \right) \quad (\text{A-3})$$

$$\mu_R(x) = \left(\frac{d - x}{d - c} \right) \quad (\text{A-4})$$

It is common practice to denote a trapezoidal fuzzy number as $\text{TrFN}(a, b, c, d)$. The alpha-cuts of a TrFN can be obtained from Eqs. A-2, A-3, and A-4 as:

$${}^{\alpha}X = [a + \alpha(b - a), d - \alpha(d - c)] \quad (\text{A-5})$$

In the special case where $b = c$, the core collapses into a single value and the resulting TrFN is known as a *triangular fuzzy number*, or TFN. To facilitate ease of computation when dealing fuzzy numbers specified in general form, trapezoidal approximations of GLRFNs can be obtained using the methods described by Grzegorzewski and Mrowka (2005; 2007).

Given a set of linguistic variables established for a specific problem, the set of possible fuzzy values each can take must be sensitive to individual interpretation and dimensional precision. As noted by Wallsten and Budescu (1994), the location, spread, and shape of membership functions vary over individuals and depend upon context and the intent of the communicated message. Moreover, inter-individual vagueness in meaning must also be considered due to individual differences in understanding and operational lexicons, which has led researchers to suggest that words cannot be legislated (Wallsten and Budescu 1994). It is therefore important to formally elicit membership functions that are specific to each problem or variable, and if resources permit, for each user using established techniques for expert opinion elicitation (Ayyub 2001). One effective technique is the Multistimuli Membership Function Technique (MMFT) described by Budescu et al. (2003).

A.2. The Extension Principle

The membership function of a variable Y , $\mu_Y(y)$, that is a function of one or more input variables X_1, X_2, \dots, X_M characterized by fuzzy numbers with membership functions

$\mu_{X_1}(x_1), \mu_{X_2}(x_2), \dots, \mu_{X_M}(x_M)$, respectively can be obtained via the extension principle as follows (Zadeh 1965):

$$\mu_Y(y) = \sup_{y=f(x_1, x_2, \dots, x_M)} \min[\mu_{X_1}(x_1), \mu_{X_2}(x_2), \dots, \mu_{X_M}(x_M), R(x_1, x_2, \dots, x_M)] \quad (\text{A-6})$$

where $R(x_1, x_2, \dots, x_M)$ defines a constraining relation among the input variables (e.g., $x_1 + x_2 \leq x_3$) that is appropriate given the nature of the problem (Klir 1997). Alternatively, an alpha-cut approach can be used as follows (Ayyub and Klir 2006):

$${}^\alpha Y = \{f(x_1, x_2, \dots, x_M) \mid \langle x_1, x_2, \dots, x_M \rangle \in ({}^\alpha X_1 \times {}^\alpha X_2 \times \dots \times {}^\alpha X_M) \cap {}^\alpha R\} \quad (\text{A-7})$$

where the intersection of the relation R with the space of possible values of X_j constrains the corresponding set of admissible values for Y at a given α -level. Equation A-7 provides the basis for standard arithmetic operations on fuzzy numbers via interval arithmetic at each α -level (Ayyub and Klir 2006).

A.3. Constructing a Fuzzy System

A fuzzy system is a collection of “if-then” rules that link a string input of linguistic variables (i.e., the antecedent or the “if-part”) to an output value (i.e., the consequent or the “then part”) (Kosko 1997; Passino and Yurkovich 1998). More specifically, a fuzzy system \tilde{F} approximates the true function $Y = f(X_1, X_2, \dots, X_M)$ via a

set of N fuzzy inference rules defined on the input-output state space $X_1 \times X_2 \times \dots \times X_M \times Y$ of the form (shown for two input variables):

$$\text{IF } (X_1 \text{ is } A_k) \text{ AND } (X_2 \text{ is } B_k) \text{ THEN } (Y \text{ is } C_k) \quad (\text{A-8})$$

where $A_k, B_k,$ and C_k are linguistic or fuzzy values assigned to $X_1, X_2,$ and $Y,$ respectively for the k^{th} rule ($1 < k \leq N$). The approximation of a true function f by a fuzzy system \tilde{F} is achieved via a set of overlapping fuzzy rule patches such as is shown in Figure A-2 that cover part of the graph of an unknown or unascertained function. If each X_j ($1 < j \leq M$) can assume one of n_j linguistic or fuzzy values, the total number of rules N that describe \tilde{F} is:

$$N = \prod_{j=1}^M n_j \quad (\text{A-9})$$

Accordingly, a higher resolution approximation with a more precise coverage of the unknown or unascertained function follows from a larger set of finely-tuned inference rules. For illustration, a fuzzy system consisting of 6 input variables each with three possible states is characterized by $3^6 = 729$ rules. If each variable could take on one of four possible states, the fuzzy system would then be characterized by $4^6 = 4,096$ rules. Thus, as the number of possible states for each linguistic variable increases, so too does the required number of inference rules; this is known as the “curse of dimensionality” (Kosko 1997). The challenge is to balance the need for analytical resolution with

simplicity and available computational resources, which thus requires a trade-off between the number of input states permitted for each linguistic variable in a fuzzy inference rule and the decision makers' tolerance for precision.

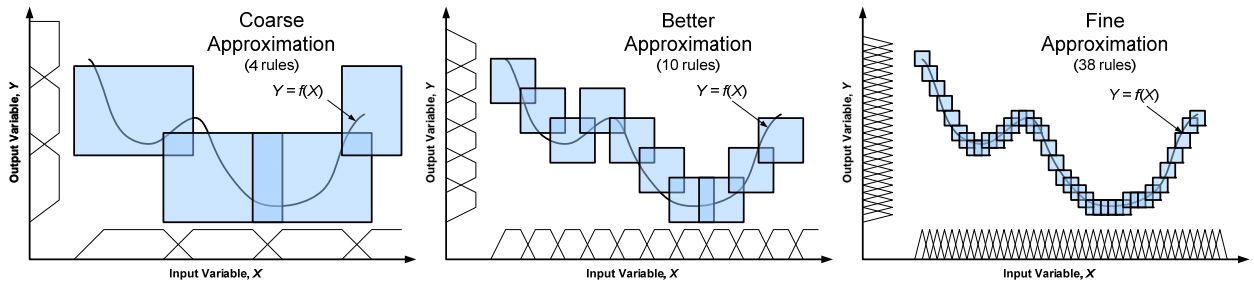


Figure A-2. Approximation of a function $Y = f(x)$ with a set of fuzzy rule patches

Constructing a fuzzy system requires systematically evaluating the consequent or output value for each of N antecedents to generate a complete set of fuzzy inference rules. This can be done manually by an expert or a panel of experts using techniques for expert opinion elicitation (Ayyub 2001), or if empirical data is available, can be done using numerical techniques (see, for example, Chiu 1999). While the simplest and most primitive approach to establishing a complete set of fuzzy inference rules is to use brute-force to evaluate the consequent for each individual antecedent in turn, this method can be time consuming if the number of rules is large or cognitively prohibitive if the number of input variables exceeds the mental abilities of a group of experts to process them into an opinion (Miller 1956). Fortunately, the fuzzy control literature is replete with suggestions on efficiently obtaining and updating a complete set of fuzzy inference rules, such as the recent article by Kuo et al. (2008) using genetic algorithm-based fuzzy neural networks.

A.4. Fuzzification and Rule Matching

Given a fuzzy system \tilde{F} consisting of a set of N inference rules that map input variables X_j ($1 < j \leq M$) to an output Y , a series of crisp input values x_j can be processed through the rule base (e.g., collection of rules) to obtain an approximation of y with associated uncertainty. In particular, given a set of crisp input values x_j , the membership values $\mu(x_j)$ for all linguistic values or fuzzy numbers that can be assigned to X_j are determined. This is known as *fuzzification*, or the process of encoding a crisp number for use with a fuzzy rule base. For example, given a probability value $p = 0.5$, the corresponding degree of membership for each fuzzy number in Figure A-1 is $\mu_{\text{Even Chance}}(0.5) = 1$, $\mu_{\text{Likely}}(0.5) = 0.5$, $\mu_{\text{Very Likely}}(0.5) \cong 0.1$, and $\mu(0.5) = 0$ for all others. Thus, if the linguistic variable X represents a probability, the fact that the $p = 0.5$ means that X is “Tossup” to the degree 1.0, X is “Likely” to the degree 0.5, and so forth.

Once the membership values for the fuzzy numbers evaluated at x_j are obtained, the next step is to determine which of the N rules are relevant (i.e., which rules are “on” or are “firing”) with respect to the given the input state. That is, the rule matching step assigns a degree of membership to each inference rule according to the degree of membership of its premises associated with x_j . Considering the example in the preceding paragraph, the rule “If X is ‘Likely’ then Y is ‘Bad’” would have a membership of 0.5 since $\mu_{\text{Likely}}(0.5) \cong 0.5$, whereas the rule “If X is ‘Unlikely’ then Y is ‘Good’” would have membership of zero in the set of relevant rules since $\mu_{\text{Unlikely}}(0.5) \cong 0.0$. For a set of rules with M premises, the membership, $\mu_{\text{Rule},k}$, for the k^{th} rule can be determined according to the inputs x_j from the product rule (a popular type of T-norm) as follows (Kosko 1997):

$$\mu_{\text{Rule},k}(x_1, x_2, \dots, x_M) = \prod_{j=1}^M \mu_{X_j}^k(x_j) \quad (\text{A-10})$$

where $\mu_{X_j}^k$ is the membership function of the fuzzy number assigned to X_j according to rule k . If the collection of fuzzy numbers for each x_j collectively span its entire domain and if the sum of the memberships among all possible fuzzy sets is exactly one for all x_j contained in X_j , the sum of the memberships assigned to all rules from Eq. A-10 for an arbitrary input state x is exactly equal to one, and is otherwise known as a *fuzzy partition* (Klir and Yuan 1995). Accordingly, the membership determined for rule k from Eq. A-10 can be interpreted as a mass assigned to the random set associated with the consequent of rule k , and the total mass distributed among all consequents would sum to one as required by the theory of evidence (Shafer 1976). Alternative T-norms can be used (e.g., maximum, minimum), but these have less discriminatory power and may not meet the requirement that the memberships sum to one (Kosko 1997).

Given a fuzzy system with M input parameters where each can take on n_j linguistic states ($j = 1, 2, \dots, M$), an unique integer rule number Z can be assigned to each of the N fuzzy inference rules (Eq. A-9) as follows:

$$Z = \hat{X}_0 + \sum_{j=1}^M \left(\hat{X}_j \prod_{k=1}^{j-1} n_k \right) \quad (\text{A-11})$$

where $\hat{X}_j \in \{0, 1, \dots, n_j - 1\}$ is an integer value for the state of each input variable, where the value 0 corresponds to the first rule, 1 the second rule, and so forth up until the last

rule $n_j - 1$. For example, if X_j could take on linguistic values “Low”, “Medium”, and “High”, the corresponding integer states could be 0, 1, and 2, respectively.

A.5. Fuzzy Inference: Evidence Theory Approach

In this final step, an aggregate output basic belief density (bbd) function, $m_Y([u, v])$, defined on a bounded continuous frame of discernment $\Omega \in \mathfrak{R}^2$ is constructed from the consequents of each inference rule discounted by the memberships obtained from Eq. A-10. In light of a complete partition of the input space by fuzzy numbers, the total mass distributed among all consequent fuzzy sets must sum to one as required by the theory of evidence, that is:

$$\int_{-\infty}^{\infty} \int_x^{\infty} m_Y([u, v]) dv du + m_Y(\emptyset) = 1 \quad (\text{A-11})$$

where \emptyset indicates the null or empty set (Smets 2005).

Assuming each fuzzy consequent takes the form of a bell-shaped GLRFN with characteristic points $\langle a, b, c, d \rangle$ (see section 5.2.1), the corresponding contribution, m_Y^k , to the aggregate output bbd from each rule with membership $\mu_{\text{Rule},k}$ can be obtained as:

$$m_Y^k([\gamma(v), u]) = \begin{cases} \mu_{\text{Rule},k} [\gamma(v) - v] \frac{d\mu_Y^k(v)}{dv} & c \leq v \leq d \\ 0 & \text{Otherwise} \end{cases} \quad (\text{A-12})$$

where $\gamma(v)$ satisfies $\mu(\gamma(v)) = \mu(v)$. Closed-form expressions for $\gamma(b)$ associated with different bell-shaped distributions are given in Table A-5. The aggregate output bbd can be obtained from the results of Eq. A-12 as:

$$m_Y([u, v]) = \sum_{k=1}^N m_Y^k([u, v]) \quad (\text{A-13})$$

To account for the less than perfect quality associated with a given item of evidence, its corresponding bbd can be discounted by a quality factor c as follows:

$$m_Y^c([u, v]) = cm_Y([u, v]), \quad \forall [u, v] \in \Omega, [u, v] \neq \Omega \quad (\text{A-14})$$

and

$$m_{Y,c}(\Omega) = cm_Y(\Omega) + 1 - c \quad (\text{A-15})$$

where $m_{Y,c}(\cdot)$ denotes the bbd after discounting. Note from Eqs. A-14 and A-15 that mass removed from intervals $[u, v]$ is transferred to Ω , which reflects transfer of mass from a state of full or partial knowledge to a state of ignorance. This manner of discounting can be referred to as *vacuous discounting*. Values for the quality factor c in consider the credibility and competence of the expert as well as the reliability of the underlying inference model; a value of one indicates perfect information, whereas values less than one indicate lesser quality information.

Alternatively and for practical reasons, the mass removed from $[u,v]$ can be transferred to the most conservative state A as follows:

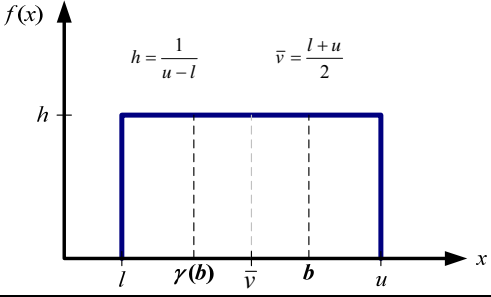
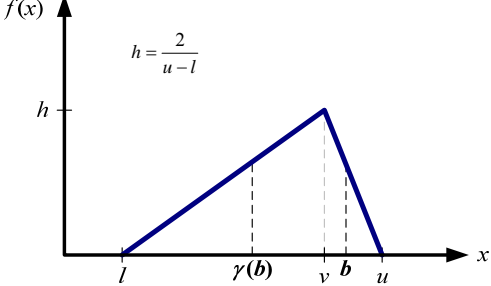
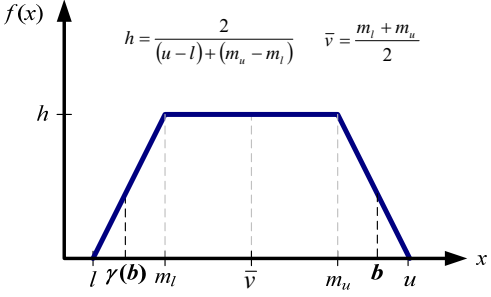
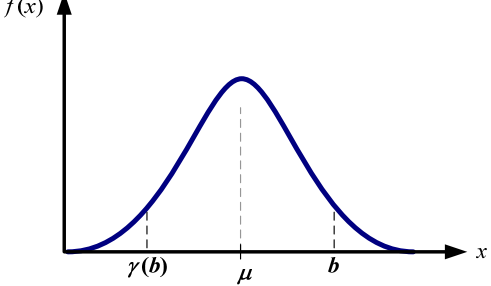
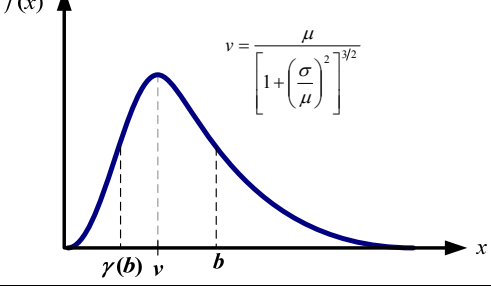
$$m_Y^c([u,v]) = cm_Y([u,v]), \quad \forall [u,v] \in \Omega, [u,v] \neq A \quad (\text{A-16})$$

and

$$m_{Y,c}(A) = cm_Y(A) + 1 - c \quad (\text{A-17})$$

The manner of discounting described in Eqs. A-16 and A-17 can be referred to as *conservative discounting*. For example, if the belief function is constructed over a space representing the probability of adversary success for a given attack type, discounting the belief function by a factor c according to conservative discounting would transfer the uncommitted mass $1 - c$ to the focal element corresponding to a probability of one, that is $A = [1,1]$ and $m_{Y,c}([1,1]) = cm_Y([1,1]) + 1 - c$. While the conservative discounting approach is arguably unjustified on epistemological grounds, it does err on the side of caution in light of expert opinions that are less than perfectly credible and pushes the value toward the worst case (e.g., 1.0) rather than the least informative (e.g., 0.5); this feature is more desirable from a decision support perspective.

Table A-1. $\gamma(b)$ for selected continuous bell-shaped functions (McGill and Ayyub 2008)

Distribution	Expression for $\gamma(b)$	Illustration
Uniform	For $\bar{v} \leq b \leq u$: $\gamma(b) = 2\bar{v} - b$	
Triangular	For $v \leq b \leq u$: $\gamma(b) = v - (b - v) \left(\frac{v - l}{u - v} \right)$	
Trapezoidal	For $\bar{v} \leq b \leq m_u$: $\gamma(b) = 2\bar{v} - b$ For $m_u < b \leq u$: $\gamma(b) = m_l - (b - m_u) \left(\frac{m_l - l}{u - m_u} \right)$	
Normal	For $b \geq \mu$: $\gamma(b) = 2\mu - b$	
Lognormal	For $b \geq v$: $\gamma(b) = \frac{v^2}{b} = \frac{\mu^2 / b}{\left[1 + \left(\frac{\sigma}{\mu} \right)^2 \right]^3}$	

In the academic literature, the term $m_Y(\emptyset)$ has been referred to the *strength of conflict* (Rakar et al. 1999; Rakar and Juricic 2002). A non-zero value cannot be assigned to $m_Y(\emptyset)$ directly, but rather emerges through the conjunctive combination of two or more partially contradictory or conflicting belief functions via the unnormalized Dempster's rule of combination (Smets and Kennes 1994). Given two distinct bdds (Smets 1992) $m_1([a, b])$ and $m_2([a, b])$ defined on continuous frames of real numbers, such as would be the case if two distinct expert provided inputs to the inference model or if a single expert provided inputs into two distinct, yet competing models, the unnormalized Dempster's rule of combination yields a combined bbd as follows (Smets 2005):

$$m_{12}^{\Omega}([a, b]) = \int_{-\infty}^{\infty} \int_x^{\infty} m_2^{\Omega}([x, y])[a, b] m_1^{\Omega}([x, y]) dy dx \quad (\text{A-18})$$

where the expression $m^{\Omega}([x, y])[a, b]$ can be determined from:

$$m^{\Omega}([c, d])[a, b] = \begin{cases} m^{\Omega}([a, b]) & \text{if } c < a \leq b < d \\ \int_{-\infty}^c m^{\Omega}([x, b]) dx & \text{if } c = a \leq b < d \\ \int_d^{\infty} m^{\Omega}([a, y]) dy & \text{if } c < a \leq b = d \\ q^{\Omega}([c, d]) & \text{if } c = a \leq b = d \\ 1 - pl^{\Omega}([c, d]) & \text{if } [a, b] = \emptyset \\ 0 & \text{otherwise} \end{cases} \quad (\text{A-19})$$

The notation $m^\Omega[[c,d]]([a,b])$ can be interpreted as the mass density a belief holder would assign to the focal element $[a,b]$ given that $[c,d]$ was accepted as true. According to Smets (2005), Eq. A-18 is both associative and commutative, that is, the bbd obtained for the combination of n items of evidence is the same regardless of the order of aggregation.

In the event of non-zero strength of conflict, the mass assigned to \emptyset must be redistributed among non-empty focal elements to obtain a “normalized” bbd \hat{m}_Y either by normalization as in the standard Dempster’s rule of combination (Shafer 1976):

$$\hat{m}_Y([u,v]) = \frac{m_Y([u,v])}{1 - m_Y(\emptyset)} \quad (\text{A-20})$$

or by transferring $m_Y(\emptyset)$ entirely to the vacuous state $m_Y((-\infty, \infty))$ according to Yager’s rule of combination (Yager 1987):

$$\begin{aligned} \hat{m}_Y([u,v]) &= m_Y([u,v]) \\ \hat{m}_Y((-\infty, \infty)) &= m_Y((-\infty, \infty)) + \hat{m}_Y(\emptyset) \end{aligned} \quad (\text{A-21})$$

Sentz and Ferson (2002) describe other approaches to dealing with the strength of conflict after conjunctive combination of two or more conflicting belief functions.

There exist dual measures under the theory of evidence framework that can be derived from a bbd: *belief* and *plausibility*. The *degree of belief* associated with a closed

interval $[a,b]$, $bel_Y([a,b])$, quantifies the total amount of justified specific support that can be given to $[a,b]$, and can be determined as:

$$bel_Y([a,b]) = \int_a^b \int_u^b m_Y([u,v]) dv du + m_Y(\emptyset) \quad (\text{A-22})$$

The *degree of plausibility* associated with a closed interval $[a,b]$, $pl_Y([a,b])$, quantifies the maximum amount of potential specific support that could be given to $[a,b]$, and can be determined as:

$$pl_Y([a,b]) = \int_{-\infty}^b \int_{\max(a,u)}^{\infty} m_Y([u,v]) dv du \quad (\text{A-23})$$

Belief and plausibility measures are dual in the sense that the following relationship holds:

$$pl_Y([a,b]) = bel_Y((-\infty, \infty)) - bel_Y(\overline{[a,b]}) \quad (\text{A-24})$$

where by definition $bel_Y((-\infty, \infty)) = 1 - m_Y(\emptyset)$. The belief and plausibility functions bound the set of probability functions, $\text{Pr}_Y([a,b])$, that can be derived via a probabilistic transformation, that is:

$$bel_Y([a,b]) \leq \text{Pr}_Y([a,b]) \leq pl_Y([a,b]), \quad \forall a \leq b \quad (\text{A-25})$$

The cumulative belief function $Cbel_Y(b)$ and cumulative plausibility function $Cpl_Y(b)$ can be obtained as:

$$Cbel_Y(b) = bel_Y((-\infty, b]) \quad (A-26)$$

$$Cpl_Y(b) = pl_Y((-\infty, b]) \quad (A-27)$$

Together, the cumulative belief and plausibility function form the bounds on the true CDF of the underlying probability distribution (Ferson et al. 2004). The plausibility (belief) associated with a single point value can be obtained by collapsing the interval $[a, b]$ in Eq. A-23 (A-22) to a single point $[a, a]$. The resulting plausibility (belief) distribution can be obtained by calculating $pl_Y([a, a])$ (or the belief alternative) for all permissible values of a . If the bbd is consonant in that it is constructed over a nested set of intervals, the plausibility (belief) distribution is called a possibility (necessity) distribution. As noted by Zadeh (1999), possibility distributions are linked to fuzzy sets in that the possibility associated with a given value a is equivalent to the membership of a .

In the event that a single probability distribution or point estimate of Y is needed, beliefs are transferred from the *credal state* where uncertainty is characterized by belief functions over a Borel sigma algebra to a *pignistic state* where uncertainty is characterized by a probability distribution over the space of real numbers via a *pignistic transformation* (Smets and Kennes 1994; Smets 2005b). Given a normalized bbd $m_Y([a, b])$, a *pignistic probability density function* can be determined as (Smets 2005):

$$Betf_Y(y) = \lim_{\varepsilon \rightarrow 0} \int_{-\infty}^y \int_{y+\varepsilon}^{\infty} \left(\frac{1}{v-u} \right) m_Y([u, v]) dv du \quad (A-28)$$

From Eq. A-28, a *pignistic cumulative distribution function* can be determined as:

$$BetF_Y(y) = \int_{-\infty}^y Betf_Y(u) du = \Pr(Y \leq y) \quad (A-29)$$

where $\Pr(Y \leq y)$ gives the pignistic probability that the true value lies within the interval $(-\infty, y]$. The pignistic transformation is grounded in the principle of insufficient reason – in the absence of information available to discriminate between two or more alternatives, the available mass is divided equally among the alternatives (Smets 2005b). A *pignistic percentile* describes the y value in Eq. A-29 that yields a specified value on the pignistic cumulative distribution function.

Following standard procedures of determining moments of a probability distribution (Ayyub and McCuen 2003), the mean, \bar{y} , and variance, σ_Y^2 , of $f_Y(y)$ can be determined as:

$$\bar{y} = \int_{-\infty}^{\infty} y Betf_Y(y) dy \quad (A-30)$$

$$\sigma_Y^2 = \int_{-\infty}^{\infty} (y - \bar{y})^2 Betf_Y(y) dy \quad (A-31)$$

The mean and variance obtained in Eqs. A-30 and A-31 provide a basis for defuzzification to obtain crisp outputs from the fuzzy system. The next section describes an alternative defuzzification approach based on the standard additive model, or SAM.

A.6. Fuzzy Inference: Standard Additive Model Approach

As an alternative to the evidence theory approach to fuzzy inference described in the previous section, a crisp output y corresponding to the input state defined by x_j is obtained by combining all rules for which $\mu_{\text{Rule}} > 0$ to obtain a fuzzy representation of Y , then converting the aggregate fuzzy output into a crisp value. More specifically, the aggregate fuzzy representation for Y , $b_Y(x)$, is obtained from the linear combination of fuzzy numbers representing the output for each rule, each weighted according to the membership of the corresponding rule k ($1 < k \leq N$) as determined from Eq. A-10:

$$b_Y(x_1, x_2, \dots, x_M, y) = \sum_k^N \mu_{\text{Rule},k}(x_1, x_2, \dots, x_M) \mu_Y^k(y) \quad (\text{A-32})$$

where $\mu_Y^k(y)$ is the membership function of the fuzzy number assigned to the output linguistic variable Y according to rule k . The crisp output for $y = \tilde{F}(x)$ (letting x imply x_1, x_2, \dots, x_M for brevity) is obtained through *defuzzification* of Y via the *center of gravity method* as follows (Kosko 1997):

$$\bar{y} = \tilde{F}(x) = \frac{\int_{-\infty}^{+\infty} u b_Y(x, u) du}{\int_{-\infty}^{+\infty} b_Y(x, u) du} \quad (\text{A-33})$$

The fuzzy system obtained via the aggregation and defuzzification operations in Eqs. A-30 and A-31 is known as an *additive fuzzy system* (Kosko 1997).

The crisp value for y obtained from Eq. A-33 can be interpreted as the expected value of the output y given the input state defined by x_j . Moreover, it can be shown that by defining $p_k(x)$ (the discrete probability attached to the centroidal value of the k -th output fuzzy set) as:

$$p_k(x) = \frac{m_{\text{Rule},k}(x)V_Y^k}{\sum_{i=1}^N m_{\text{Rule},i}(x)V_Y^i} \quad (\text{A-34})$$

where $V_Y^k = \int_{-\infty}^{+\infty} m_Y^k(y)dy$ is the total area of under the curve associated with the

membership function $m_Y^k(y)$, Eq. A-33 can be rewritten as:

$$\tilde{F}(x) = \sum_{k=1}^M p_k(x)c_Y^k \quad (\text{A-35})$$

where the centroid c_Y^k of the membership function $m_Y^k(y)$ along the y -axis can be

calculated as:

$$c_Y^k = \frac{1}{V_Y^k} \int_{-\infty}^{+\infty} ym_Y^k(y)dy \quad (\text{A-36})$$

The standard deviation of the output y given the input state defined by x_j , $\sigma_{Y|X}$, can now be expressed as:

$$\sigma_{Y|X}(x) = \sqrt{\sum_{k=1}^M p_k(x) \sigma_{Y,k}^2 + \sum_{k=1}^M p_k(x) (c_Y^k - F(x))^2} \quad (\text{A-37})$$

where:

$$\sigma_{Y,k}^2 = \frac{1}{V_Y^k} \int_{-\infty}^{\infty} (y - c_Y^k)^2 m_Y^k(y) dy \quad (\text{A-38})$$

The standard deviation in Eq. A-37 captures the epistemic uncertainty induced by the imprecision of the fuzzy numbers used for defining the functional relationship between input and output variables.

A.7. Arithmetic on Random Sets with Unknown or Uncertain Dependence

A generic arithmetic operation $@$ on two numbers A and B represented by random sets on a continuous frame with focal elements a and b produces an output $C = A @ B$ with focal elements c as follows:

$$c = \left[\min(\underline{a} @ \underline{b}, \bar{a} @ \underline{b}, \underline{a} @ \bar{b}, \bar{a} @ \bar{b}), \max(\underline{a} @ \underline{b}, \bar{a} @ \underline{b}, \underline{a} @ \bar{b}, \bar{a} @ \bar{b}) \right] \quad (\text{A-39})$$

In the case where A and B are independent credal variables, the basic belief assignment associated with each focal element of C , $m(C)$, can be obtained as:

$$m(c) = m(a)m(b) \quad (\text{A-40})$$

In general, a copula C exists that characterizes the dependency between the variables X and Y . In the case of unknown dependency between two variables X and Y , Williamson and Downs (1990), and later made more explicit by Ferson et al. (2004), showed that the cumulative belief and plausibility functions for the output variable Z , $Cbel(z)$ and $Cpl(z)$, following an arithmetic operation on X and Y both characterized by random sets can be obtained as follows:

Addition

$$Cbel(z) = \sup_{z=x+y} \max(Cbel(x) + Cbel(y) - 1, 0) \quad (\text{A-41})$$

$$Cpl(z) = \inf_{z=x+y} \min(Cpl(x) + Cpl(y), 1) \quad (\text{A-42})$$

Multiplication

$$Cbel(z) = \sup_{z=xy} \max(Cbel(x) + Cbel(y) - 1, 0) \quad (\text{A-43})$$

$$Cpl(z) = \inf_{z=x \cdot y} \min(Cpl(x) + Cpl(y), 1) \quad (\text{A-44})$$

Subtraction

$$Cbel(z) = \sup_{z=x-y} \max(Cbel(x) + Cpl(y), 0) \quad (\text{A-45})$$

$$Cpl(z) = 1 + \inf_{z=x-y} \min(Cpl(x) + Cbel(y), 0) \quad (\text{A-46})$$

Division

$$Cbel(z) = \sup_{z=x/y} \max(Cbel(x) + Cpl(y), 0) \quad (\text{A-47})$$

$$Cpl(z) = 1 + \inf_{z=x/y} \min(Cpl(x) + Cbel(y), 0) \quad (\text{A-48})$$

Ferson et al. (2004) also provide procedures for performing arithmetic operations that accommodates partial information about the dependency between X and Y , such as the lower bound on the copula or the sign of dependence is known. Most relevant to this research is the case where the dependency is only known to be non-negative. In this case, the cumulative belief and plausibility functions for the output Z following the addition of two variables X and Y known to be *positive quadrant dependent* is given as:

$$Cbel(z) = \inf_{z=x+y} (1 - (1 - Cbel(x))(1 - Cbel(y))) \quad (\text{A-49})$$

$$Cpl(z) = \sup_{z=x+y} (Cpl(x) + Cpl(y)) \quad (\text{A-50})$$

Appendix B. Results of the Regional Case Study

B.1. Conditional Public Health & Safety Loss Distribution Given Successful Attack

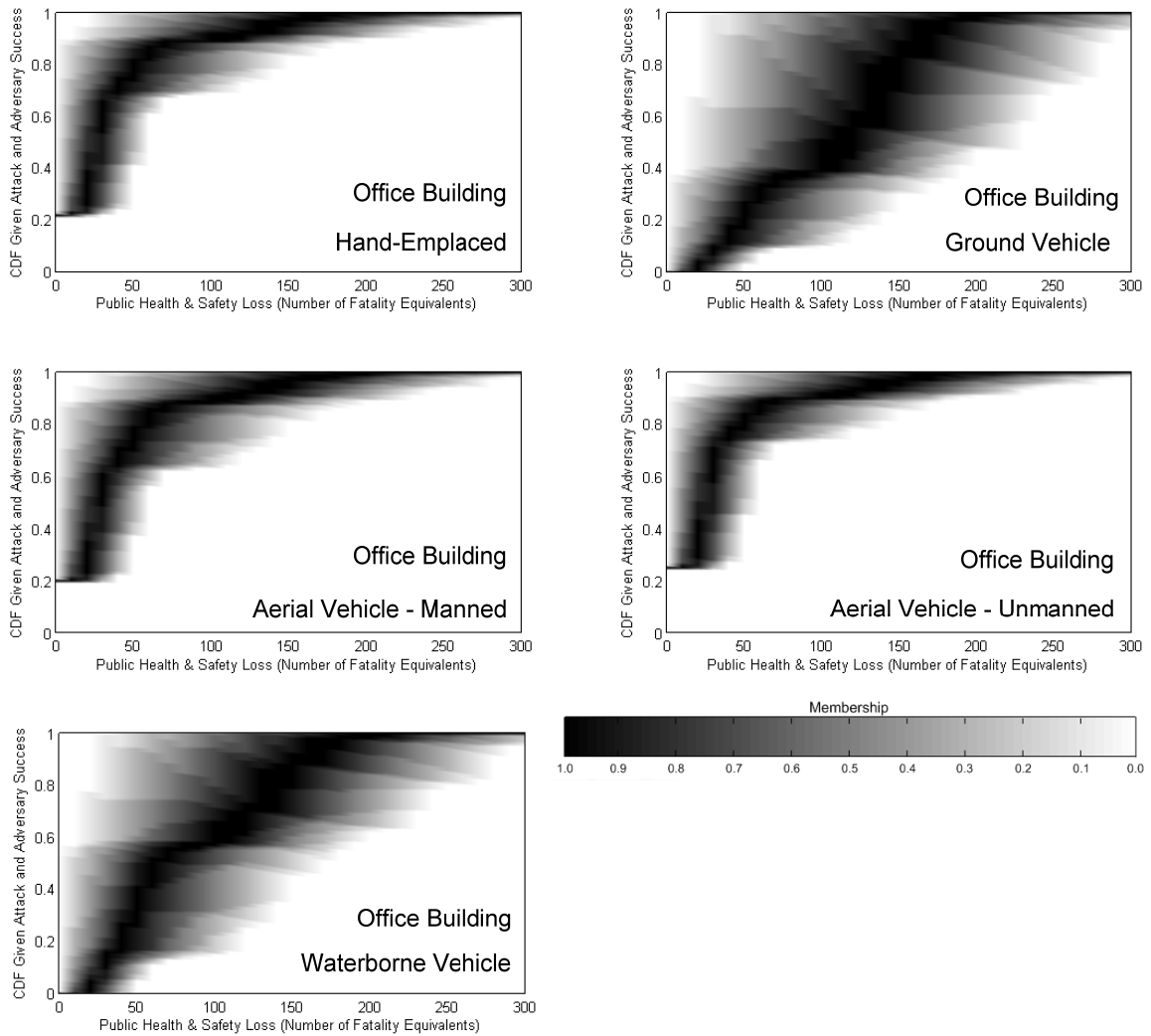


Figure B-1. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (office building)

Table B-1. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (office building)

Percentile	Public Health & Safety Loss (Fatality Equivalentents)				
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)	Waterborne
1	6.92	19.11	7.51	6.44	16.24
5	8.01	26.53	8.69	7.33	21.58
25	17.17	59.00	19.04	15.24	49.50
50	31.79	107.70	35.04	28.39	90.05
75	49.30	154.70	54.19	43.70	132.60
95	63.04	193.60	70.15	55.40	169.50
99	65.89	203.30	73.31	57.68	178.80

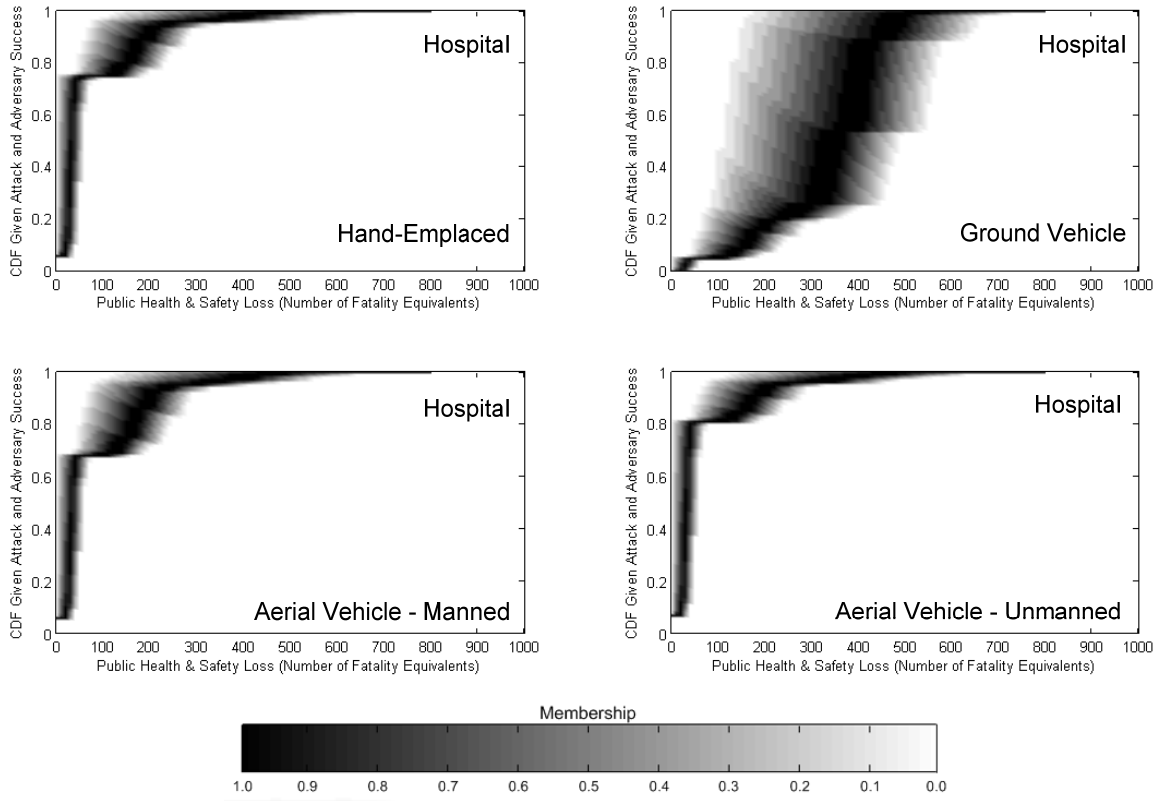


Figure B-2. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (hospital)

Table B-2. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (hospital)

Percentile	Public Health & Safety Loss (Fatality Equivalents)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	21.58	104.05	24.83	18.22
5	24.09	123.95	27.90	20.06
25	41.48	207.11	47.34	35.05
50	73.04	329.65	82.86	63.10
75	93.58	404.90	105.17	81.12
95	107.92	452.30	121.03	93.72
99	110.58	464.60	123.98	95.97

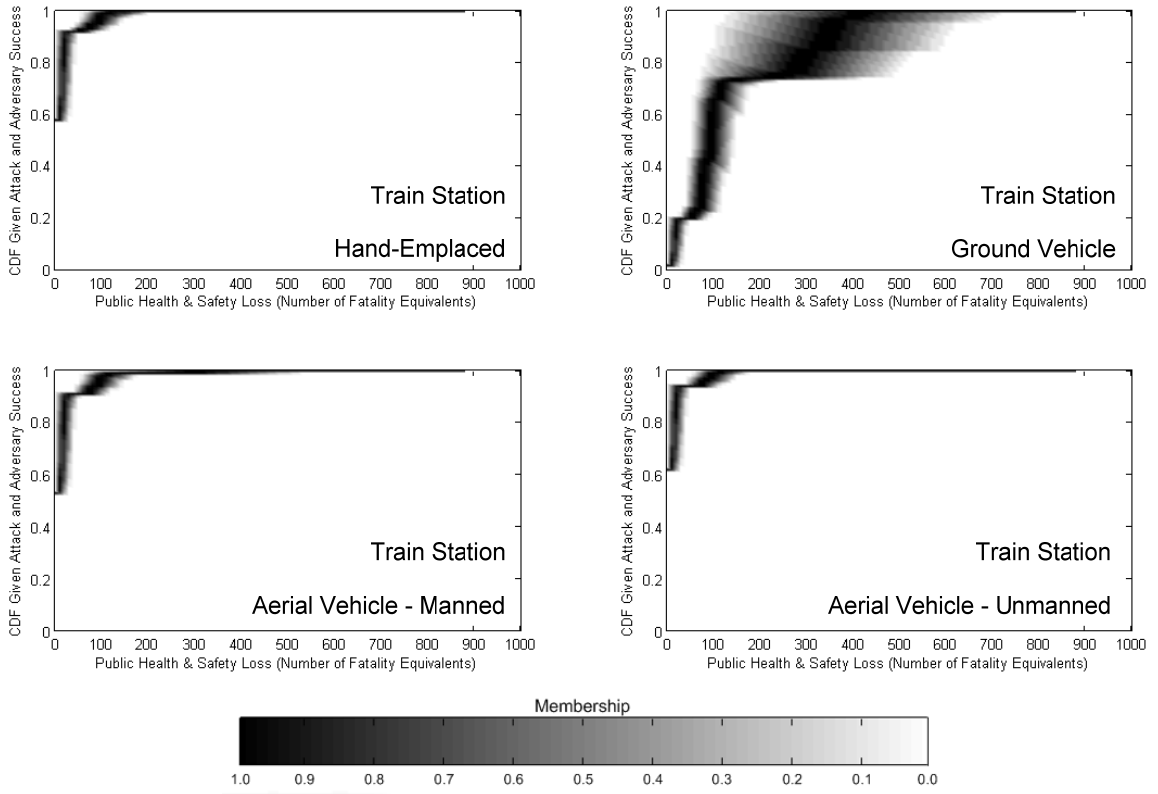


Figure B-3. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (train station)

Table B-3. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (train station)

Percentile	Public Health & Safety Loss (Fatality Equivalents)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	2.95	56.45	3.86	2.18
5	3.03	62.95	4.00	2.22
25	3.61	90.89	4.74	2.70
50	6.24	138.38	8.88	4.79
75	8.90	189.29	12.48	6.83
95	10.66	225.52	15.12	8.23
99	11.27	234.63	16.03	8.74

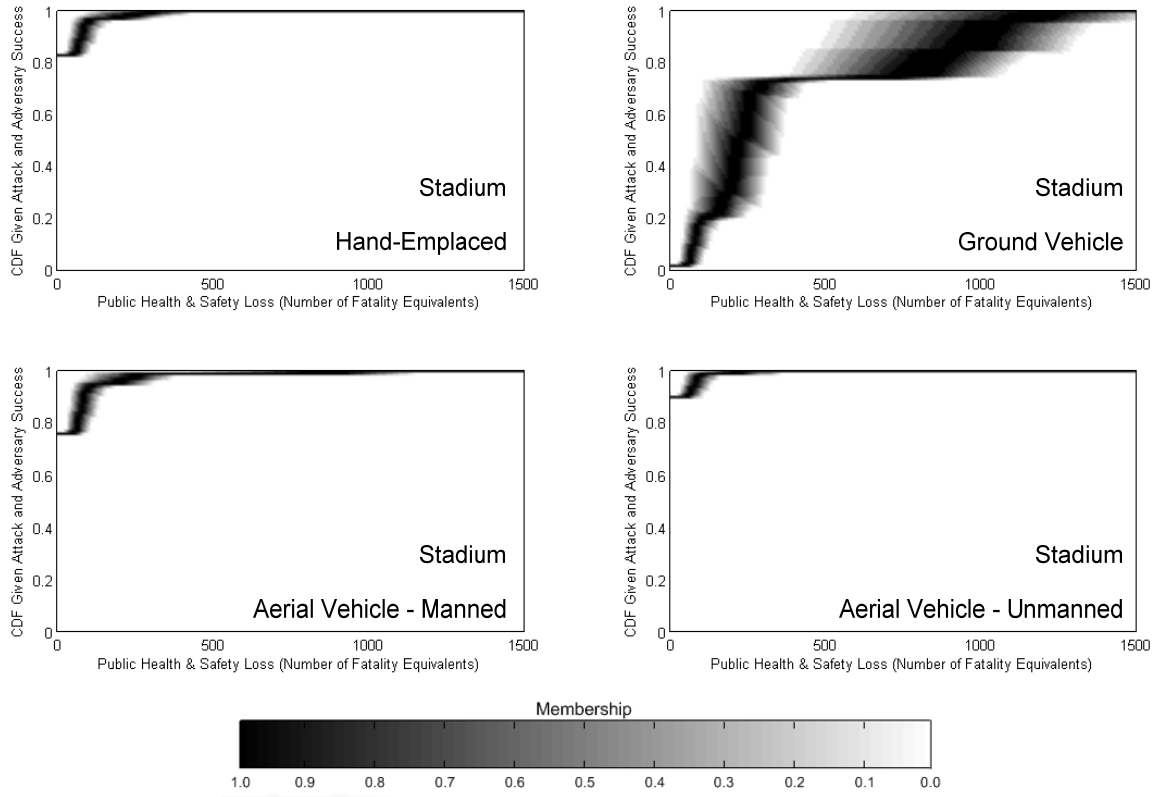


Figure B-4. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (stadium)

Table B-4. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (stadium)

Percentile	Public Health & Safety Loss (Fatality Equivalents)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	1.25	167.03	2.76	0.36
5	1.33	184.49	2.97	0.37
25	1.78	255.50	4.00	0.48
50	3.22	374.85	8.06	0.95
75	4.39	464.21	10.63	1.36
95	5.17	518.46	12.28	1.66
99	5.33	533.41	12.65	1.72

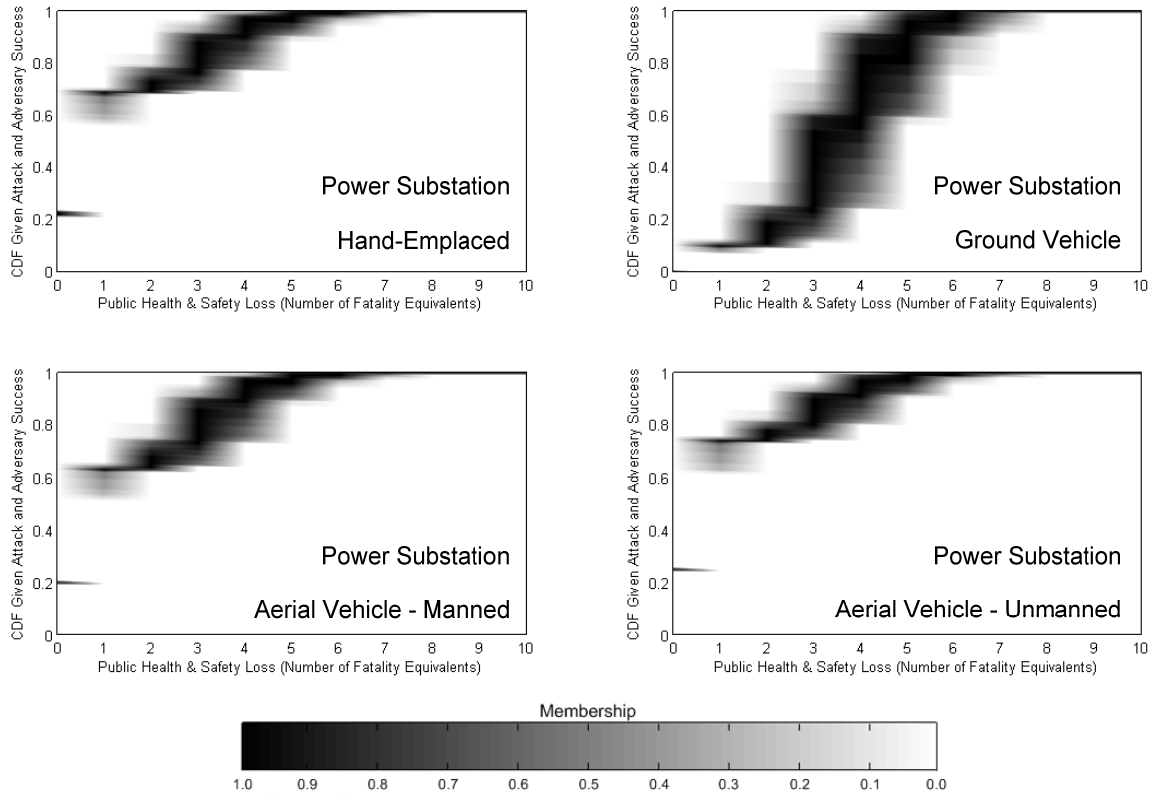


Figure B-5. Conditional possibilistic cumulative distribution function for public health and safety loss given adversary success for each attack profile (power substation)

Table B-5. Mean values of selected percentile conditional cumulative distribution functions for public health and safety loss given adversary success for each attack profile (power substation)

Percentile	Public Health & Safety Loss (Fatality Equivalents)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	0.94	2.71	1.07	0.85
5	0.98	2.86	1.12	0.88
25	1.03	3.05	1.18	0.92
50	1.28	3.82	1.45	1.11
75	1.59	4.82	1.81	1.35
95	1.71	5.11	1.94	1.47
99	1.75	5.19	1.98	1.50

B.2. Conditional Disruption Loss Distribution Given Successful Attack

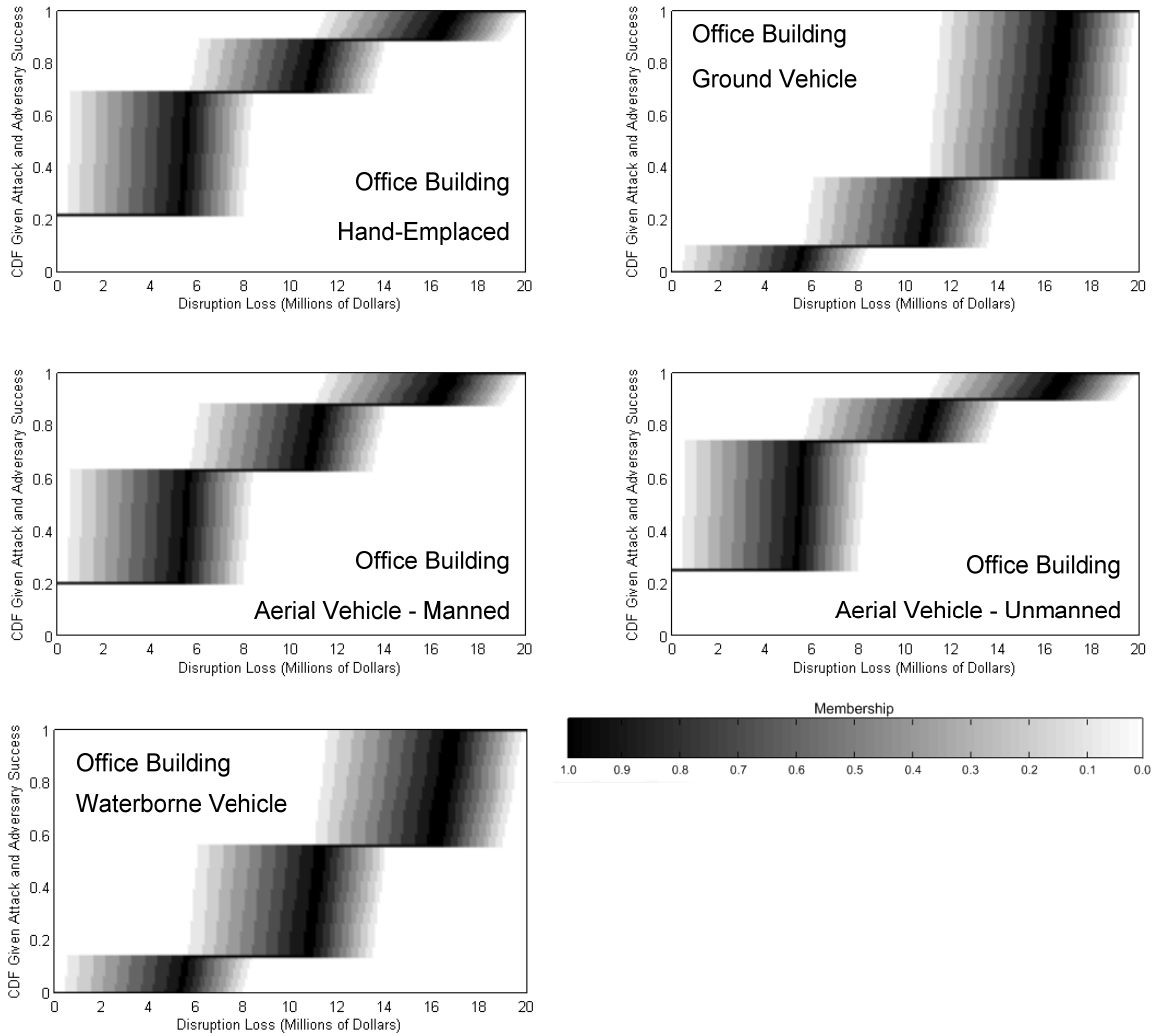


Figure B-6. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (office building)

Table B-6. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (office building)

Percentile	Disruption Loss (in Millions of Dollars)				
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)	Waterborne
1	1.98	8.64	2.34	1.66	7.36
5	2.29	9.15	2.66	1.94	7.87
25	3.56	11.26	4.01	3.11	9.98
50	5.15	13.98	5.68	4.58	12.67
75	6.02	15.35	6.60	5.38	14.00
95	6.72	16.46	7.34	6.03	15.11
99	6.90	16.74	7.52	6.19	15.39

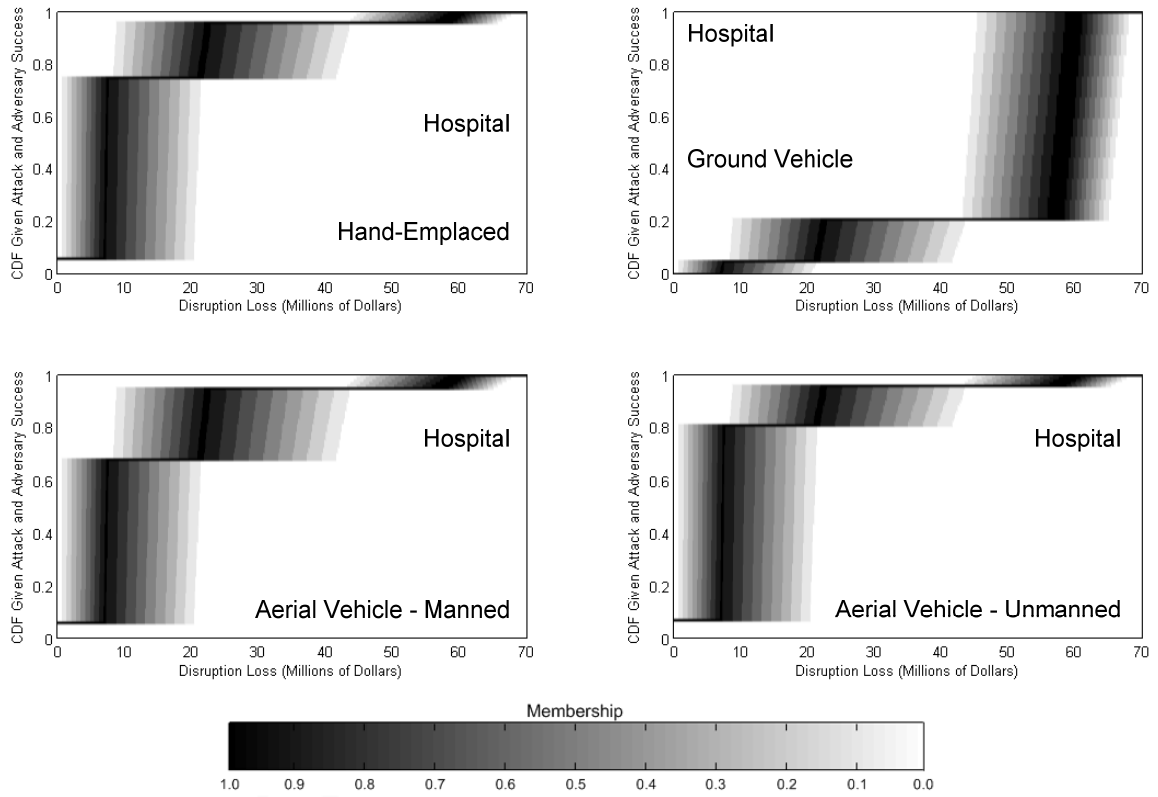


Figure B-7. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (hospital)

Table B-7. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (hospital)

Percentile	Disruption Loss (in Millions of Dollars)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	3.36	35.57	4.20	2.88
5	4.16	36.91	5.04	3.63
25	7.27	42.38	8.33	6.51
50	11.26	50.01	12.55	10.25
75	17.46	55.10	18.93	16.12
95	23.27	59.12	24.88	21.65
99	24.73	60.14	26.37	23.03

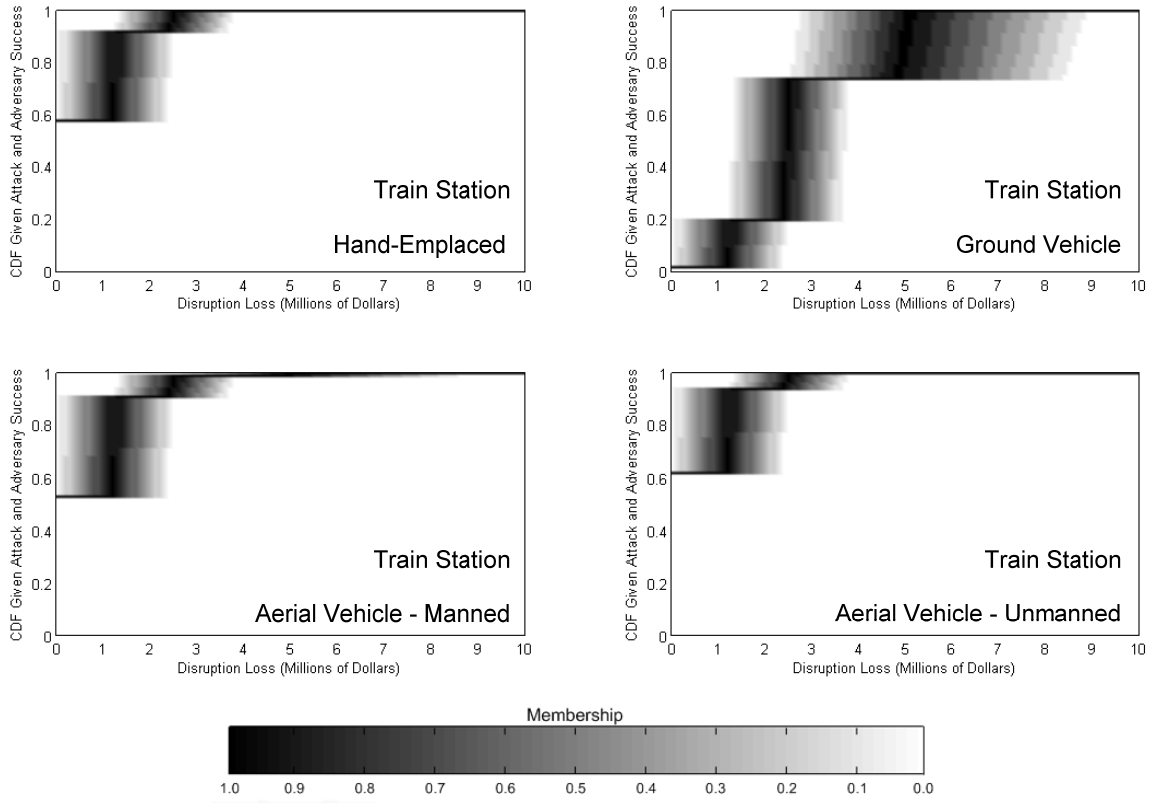


Figure B-8. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (train station)

Table B-8. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (train station)

Percentile	Disruption Loss (in Millions of Dollars)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	0.05	1.39	0.07	0.04
5	0.08	1.53	0.10	0.06
25	0.16	2.11	0.21	0.13
50	0.27	2.83	0.35	0.21
75	0.38	3.72	0.49	0.30
95	0.47	4.47	0.61	0.38
99	0.49	4.67	0.63	0.39

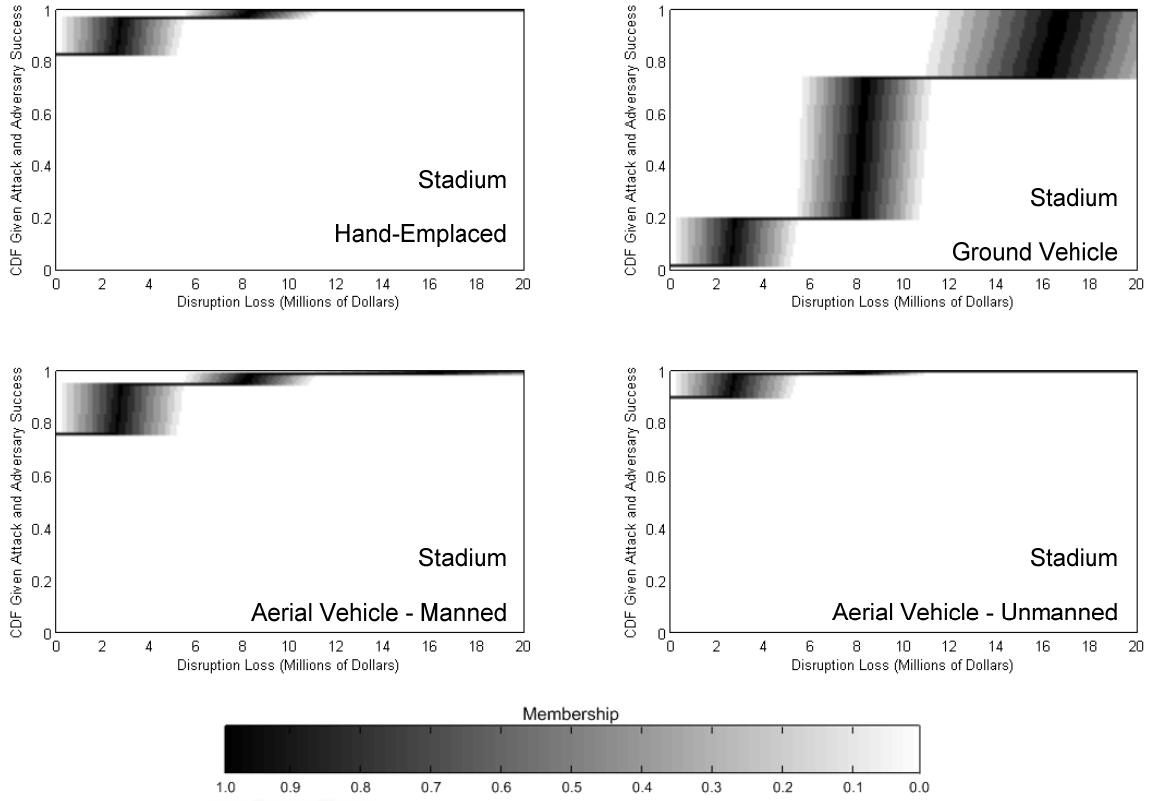


Figure B-9. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (stadium)

Table B-9. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (stadium)

Percentile	Disruption Loss (in Millions of Dollars)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	0.02	5.71	0.06	0.00
5	0.03	6.00	0.08	0.00
25	0.06	7.30	0.13	0.01
50	0.11	9.00	0.24	0.03
75	0.15	10.69	0.33	0.05
95	0.18	6.59	0.35	0.06
99	0.19	6.81	0.36	0.06

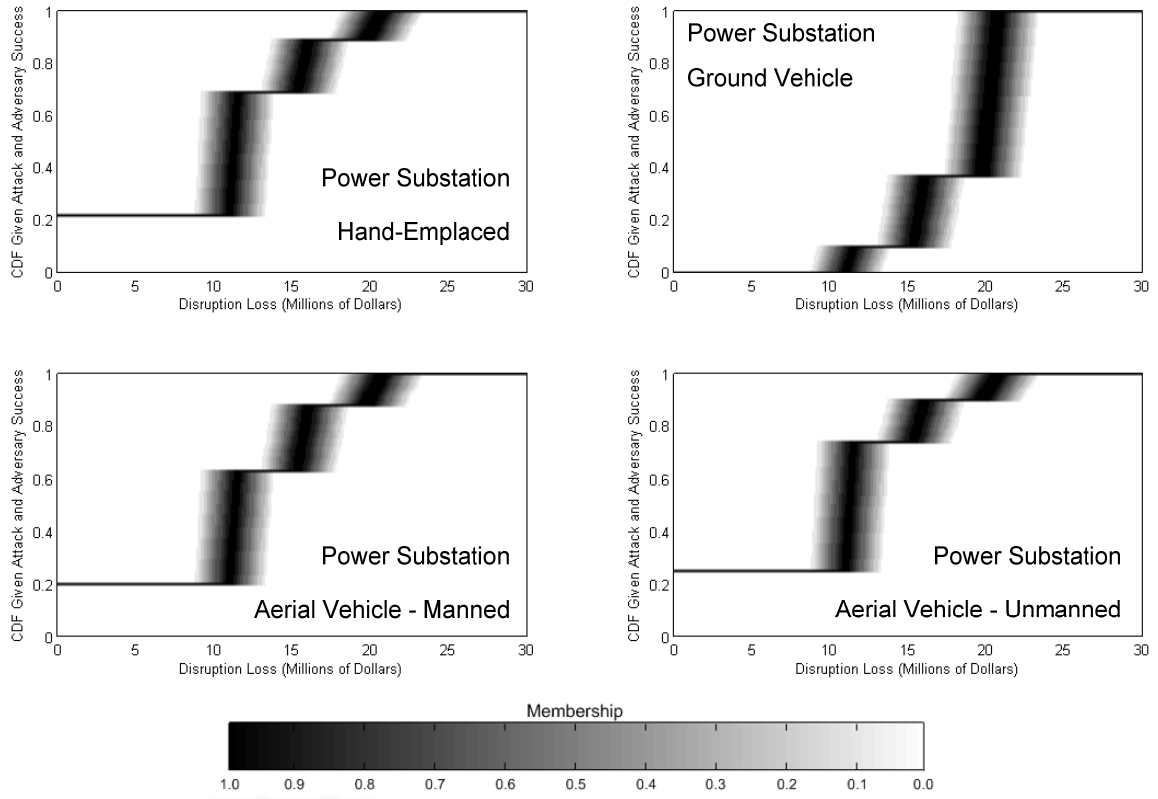


Figure B-10. Conditional possibilistic cumulative distribution function for disruption loss given adversary success for each attack profile (power substation)

Table B-10. Mean values of selected percentile conditional cumulative distribution functions for disruption loss given adversary success for each attack profile (power substation)

Percentile	Disruption Loss (in Millions of Dollars)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	6.69	15.40	7.25	6.04
5	6.86	15.66	7.43	6.19
25	7.35	16.51	7.94	6.65
50	8.33	18.15	8.97	7.56
75	9.21	19.37	9.90	8.36
95	9.77	20.30	10.49	8.88
99	9.90	20.51	10.63	9.00

B.3. Conditional Aggregate Loss Distribution Given Successful Attack

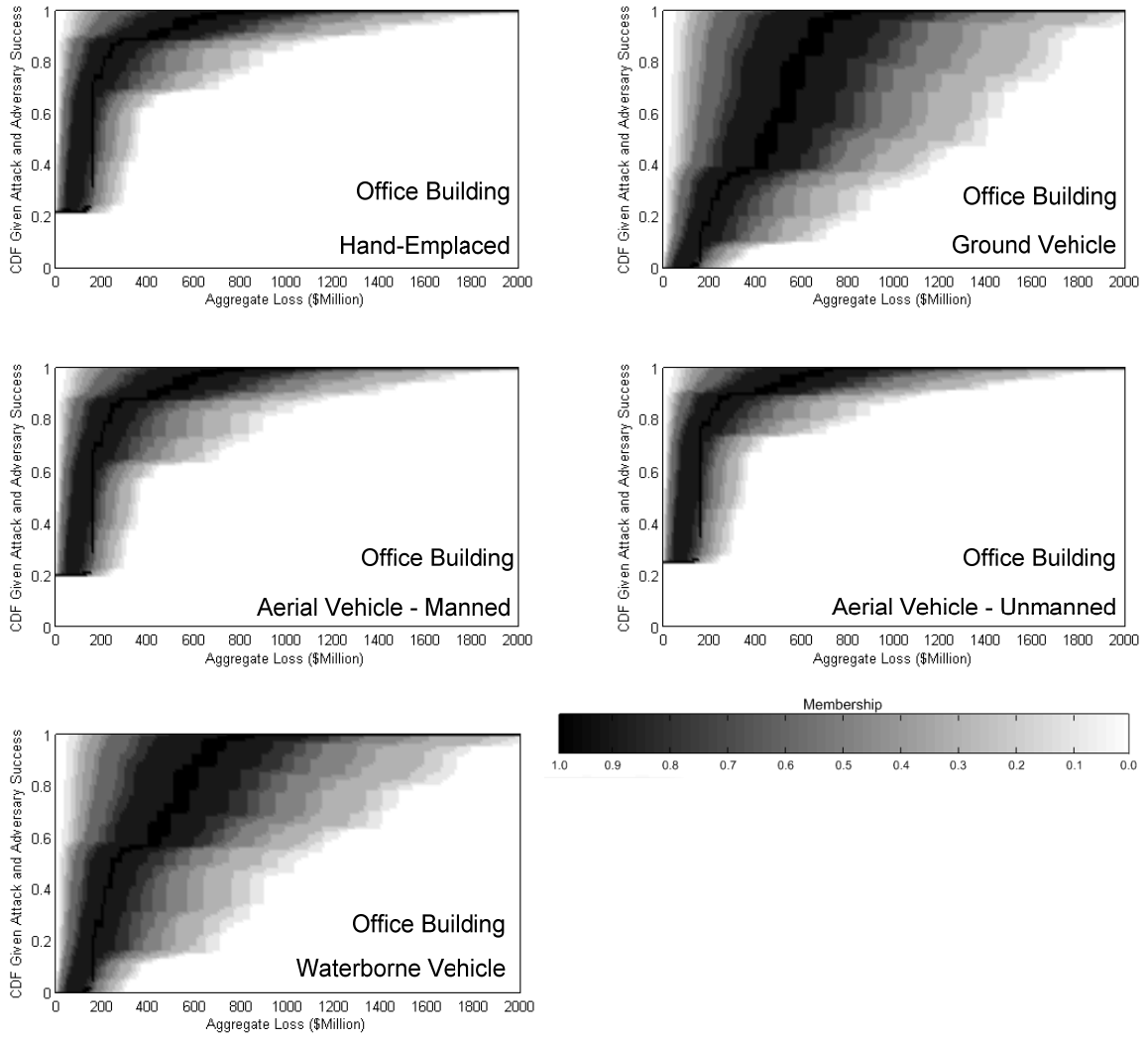


Figure B-11. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (office building)

Table B-11. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (office building)

Percentile	Aggregate Loss (\$Millions)				
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)	Waterborne
1	11.55	33.26	12.56	10.36	28.71
5	15.02	53.76	16.51	13.32	44.55
25	34.96	126.52	38.87	30.78	105.24
50	140.63	422.60	152.00	127.73	355.95
75	236.37	765.00	260.66	207.94	652.50
95	375.25	1178.80	417.07	329.38	1027.50
99	400.06	1244.40	445.34	350.66	1089.00

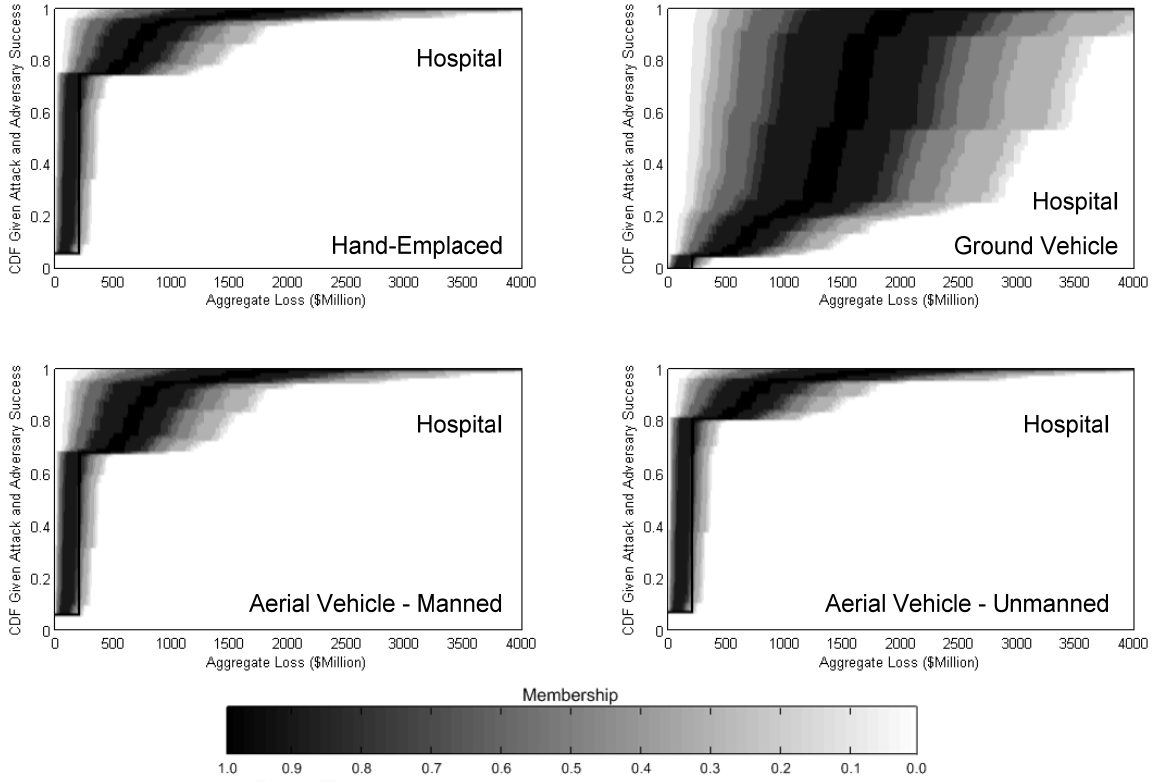


Figure B-12. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (hospital)

Table B-12. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (hospital)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	31.25	159.79	35.90	26.86
5	42.87	240.17	50.41	35.42
25	86.49	467.38	100.07	73.05
50	334.92	1320.60	369.75	298.39
75	481.18	2079.90	543.50	417.92
95	663.67	2843.10	750.31	576.97
99	687.33	2915.00	774.63	597.84

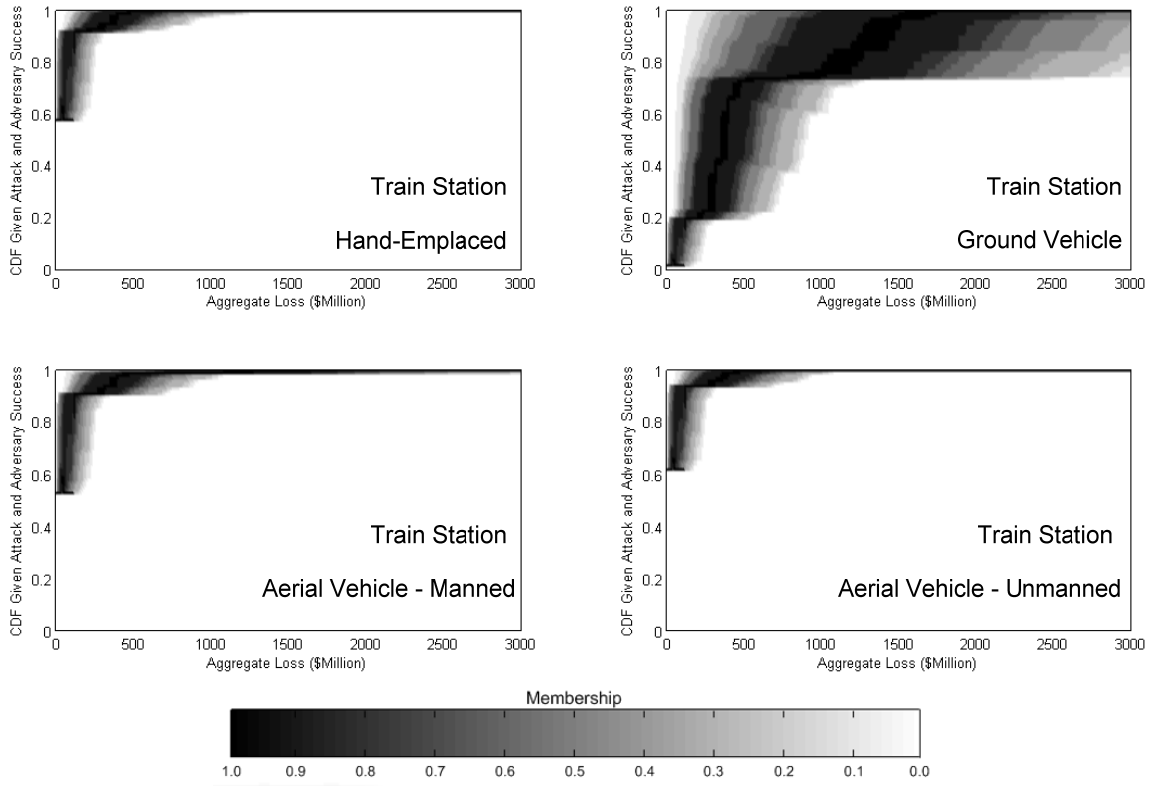


Figure B-13. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (train station)

Table B-13. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (train station)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	3.12	61.11	4.14	2.33
5	3.98	97.19	5.24	2.89
25	6.97	184.49	9.25	5.14
50	28.90	535.91	40.40	22.71
75	41.62	929.71	59.28	31.86
95	62.74	1367.69	89.33	48.48
99	66.56	1426.69	94.80	51.48

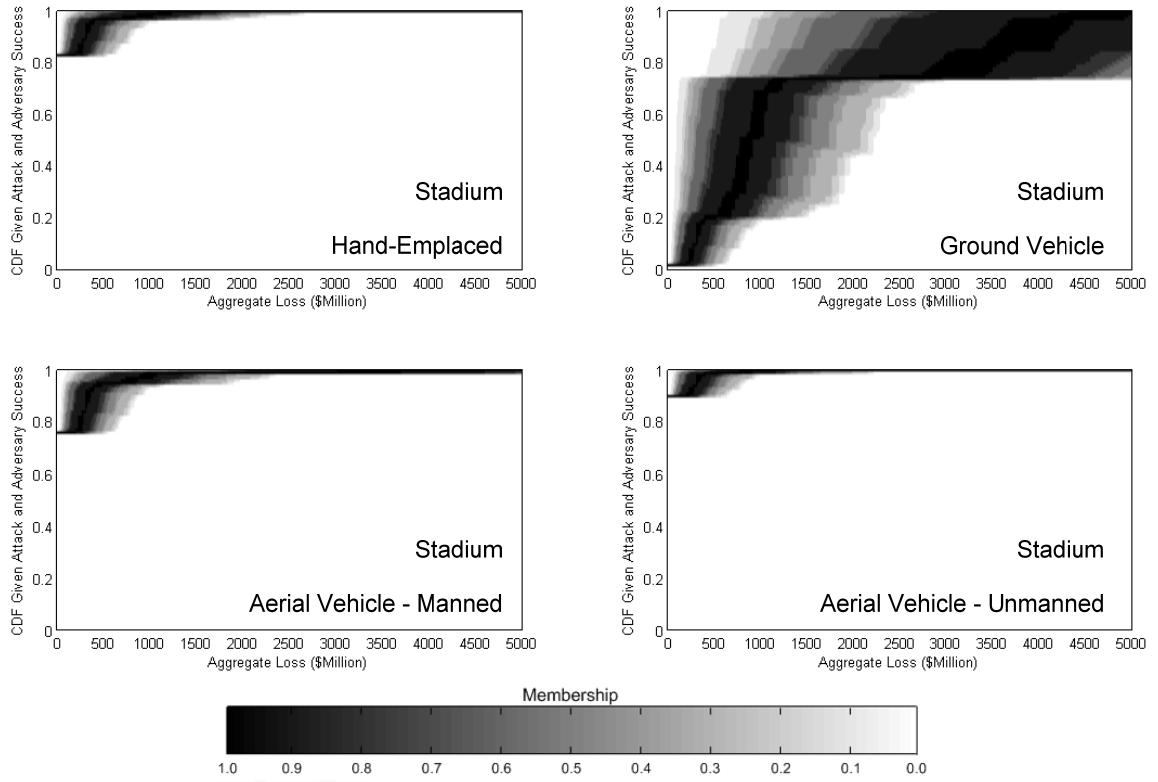


Figure B-14. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (stadium)

Table B-14. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (stadium)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	1.34	180.81	2.97	0.38
5	2.05	288.87	4.55	0.57
25	3.54	524.29	8.00	0.94
50	12.18	1449.08	30.74	3.57
75	21.65	2145.03	52.28	6.67
95	31.21	2527.97	69.83	9.98
99	32.42	2571.23	72.00	10.40

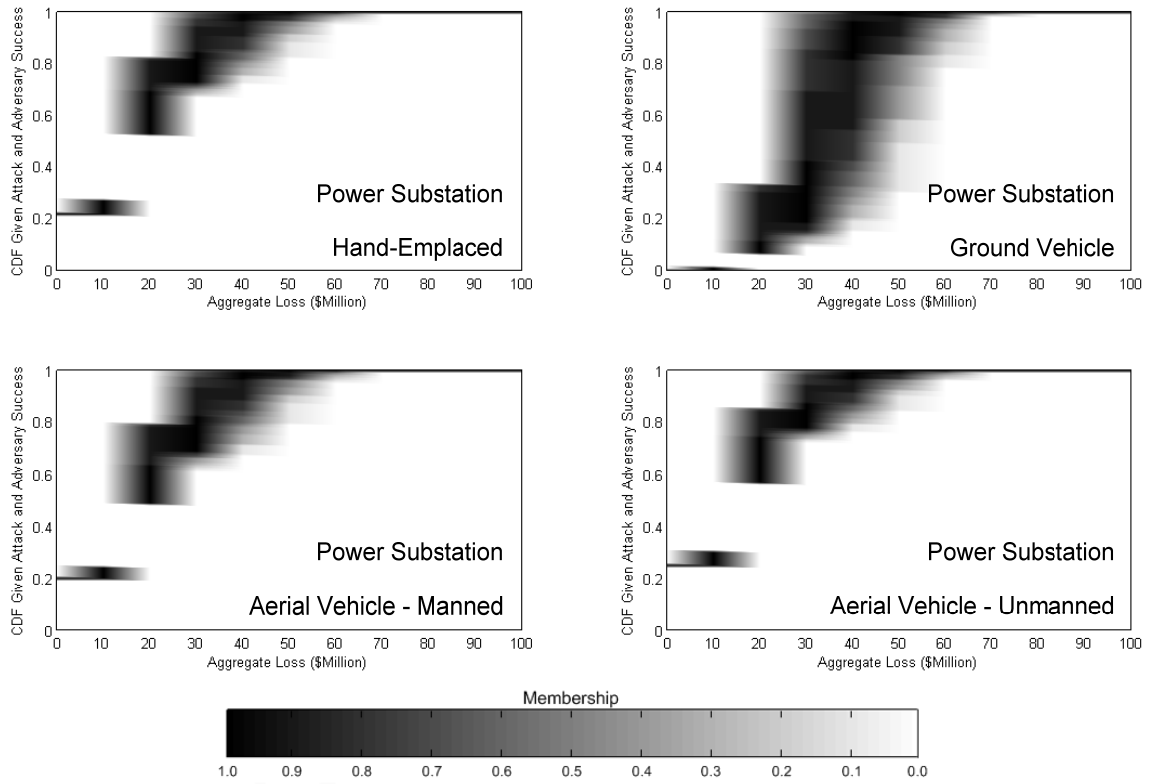


Figure B-15. Conditional possibilistic cumulative distribution function for aggregate loss given adversary success for each attack profile (power substation)

Table B-15. Mean values of selected percentile conditional cumulative distribution functions for aggregate loss given adversary success for each attack profile (power substation)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	12.78	26.04	13.75	11.62
5	12.78	26.04	13.75	11.62
25	12.78	26.04	13.75	11.62
50	16.85	37.15	18.28	15.11
75	19.99	46.20	21.63	17.86
95	21.57	52.70	23.57	19.08
99	22.36	55.60	24.71	19.84

B.4. Conditional Aggregate Loss Given Attack: By Attack Profile

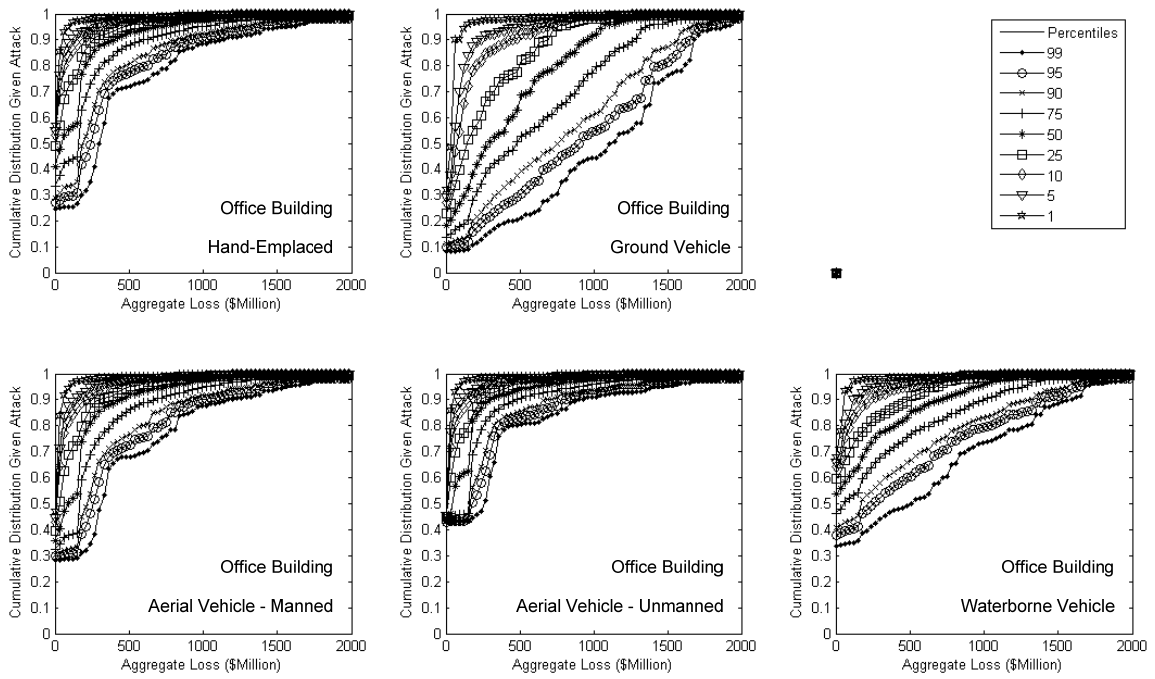


Figure B-16. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (office building)

Table B-16. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (office building)

Percentile	Aggregate Loss (\$Millions)				
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)	Waterborne
1	13.62	39.52	19.11	17.95	10.12
5	23.38	79.03	33.02	27.64	19.89
10	32.30	115.68	45.14	36.23	29.12
25	54.14	202.11	73.29	54.74	52.59
50	92.44	332.24	112.22	77.59	92.17
75	150.01	497.66	168.51	109.23	158.42
90	216.28	688.19	230.47	140.03	243.07
95	256.75	799.47	267.66	158.57	298.88
99	320.45	944.16	319.08	182.77	395.86

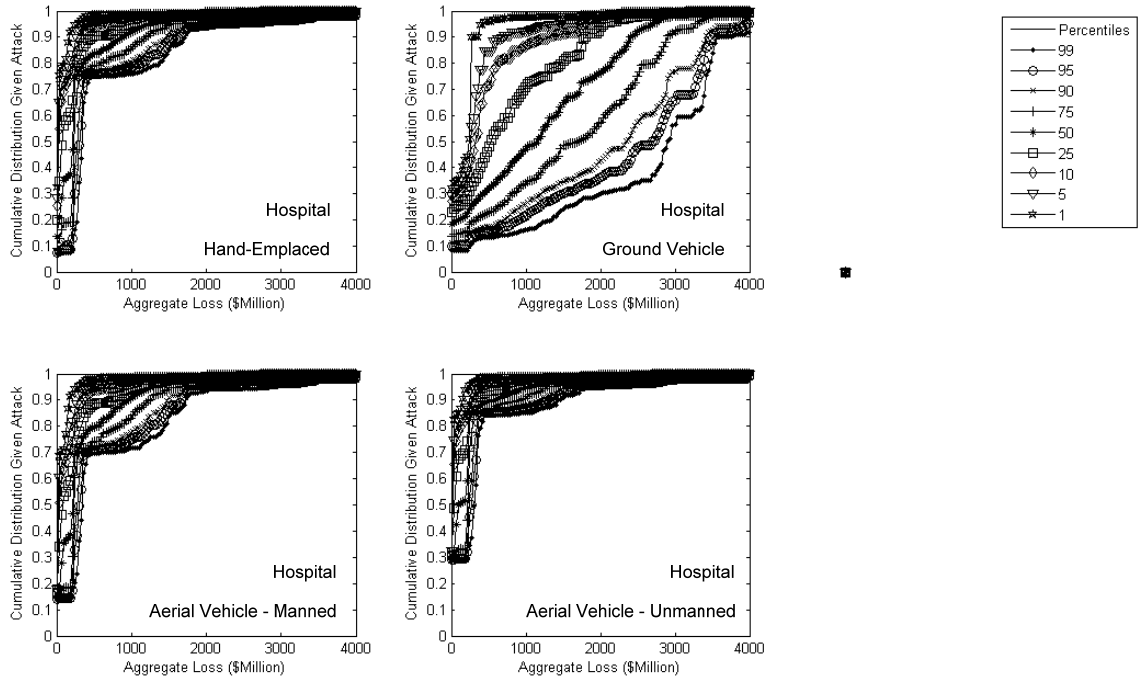


Figure B-17. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (hospital)

Table B-17. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (hospital)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	54.44	147.66	77.38	46.00
5	87.79	247.92	114.37	65.01
10	118.23	346.92	147.34	83.52
25	188.57	586.55	215.61	121.62
50	290.23	952.55	306.06	171.63
75	401.63	1371.06	404.71	224.16
90	501.43	1786.58	491.34	268.14
95	557.05	2009.29	542.80	294.39
99	629.70	2291.81	609.96	329.66

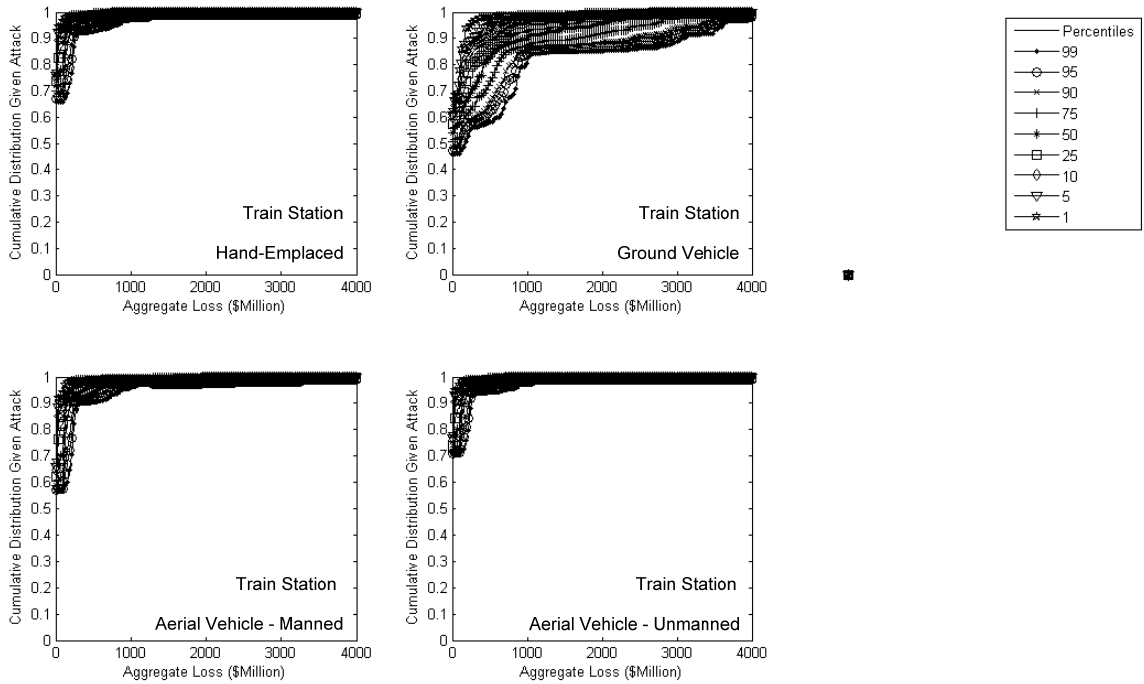


Figure B-18. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (train station)

Table B-18. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (train station)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	3.77	27.14	9.83	3.31
5	5.24	43.77	13.72	4.59
10	6.66	58.94	17.56	5.83
25	9.90	90.57	25.75	8.68
50	15.02	141.04	37.85	12.97
75	20.87	210.32	49.28	16.99
90	28.20	287.08	62.14	21.60
95	32.84	331.99	69.83	24.17
99	40.17	393.09	80.80	27.51

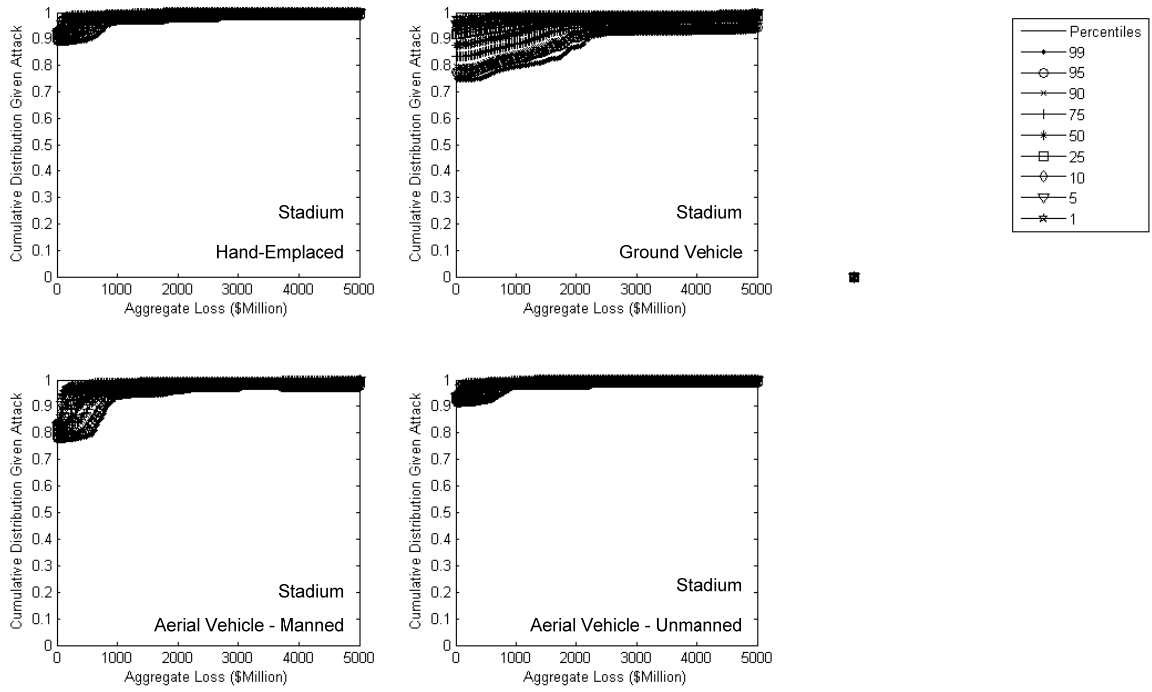


Figure B-19. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (stadium)

Table B-19. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (stadium)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	1.45	1.45	9.78	0.89
5	2.14	3.63	13.11	1.19
10	2.66	5.74	16.14	1.53
25	3.71	12.45	21.32	2.19
50	5.11	29.19	27.81	2.91
75	6.81	56.07	36.52	3.75
90	8.79	90.85	46.82	4.63
95	10.01	114.28	52.70	5.14
99	11.56	152.95	60.77	5.81

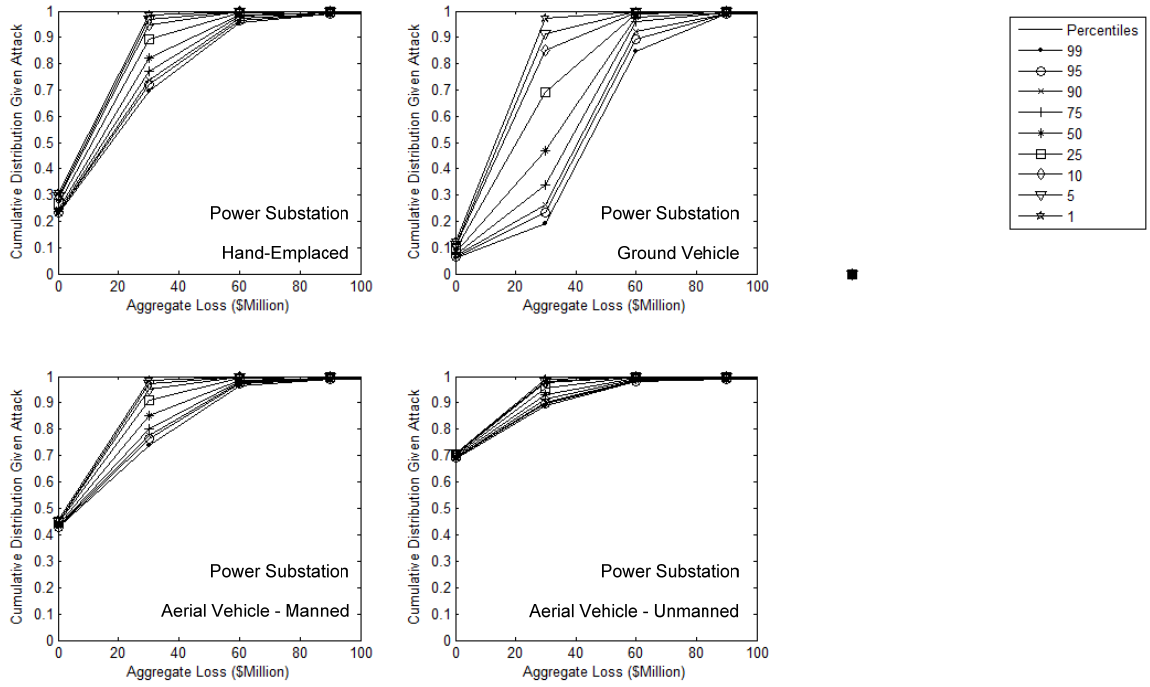


Figure B-20. Pignistic percentile cumulative distribution functions for aggregate loss given attack for each attack profile (power substation)

Table B-20. Mean values of selected pignistic percentile conditional cumulative distribution functions for aggregate loss given attack for each attack profile (power substation)

Percentile	Aggregate Loss (\$Millions)			
	Hand-Emplaced	Ground Vehicle	Aerial Vehicle (Manned)	Aerial Vehicle (Unmanned)
1	14.61	23.71	9.02	2.63
5	15.63	25.91	9.56	2.70
10	16.45	28.03	9.91	2.80
25	18.40	33.15	10.82	3.05
50	21.04	40.10	11.99	3.31
75	22.69	44.57	12.88	3.52
90	23.76	48.06	13.44	3.67
95	24.30	50.03	13.77	3.73
99	25.15	52.77	14.34	3.81

B.5. Conditional Loss-Exceedance Given Attack

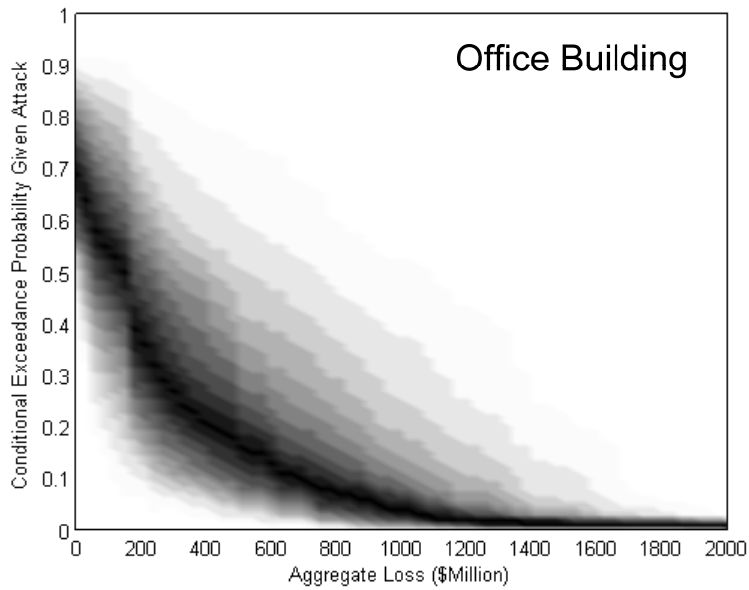


Figure B-21. Possibilistic conditional loss-exceedance curve given attack (office building)

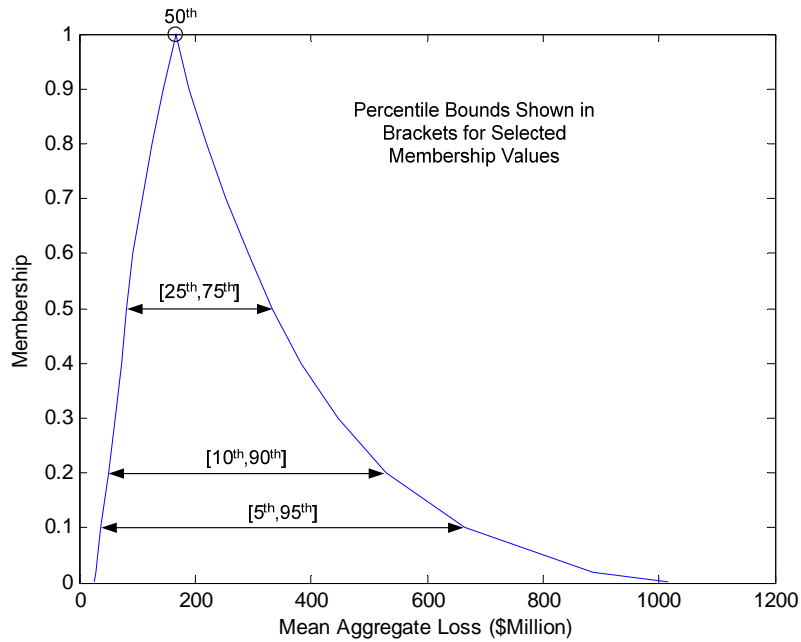


Figure B-22. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (office building)

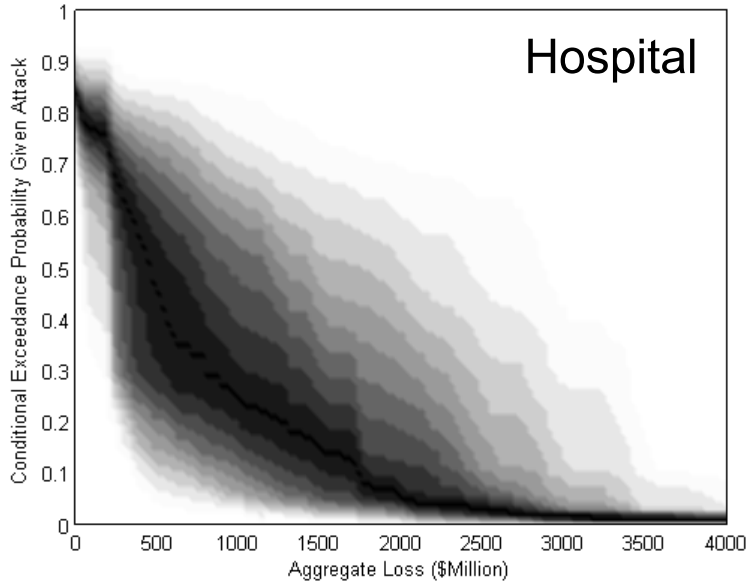


Figure B-23. Possibilistic conditional loss-exceedance curve given attack (hospital)

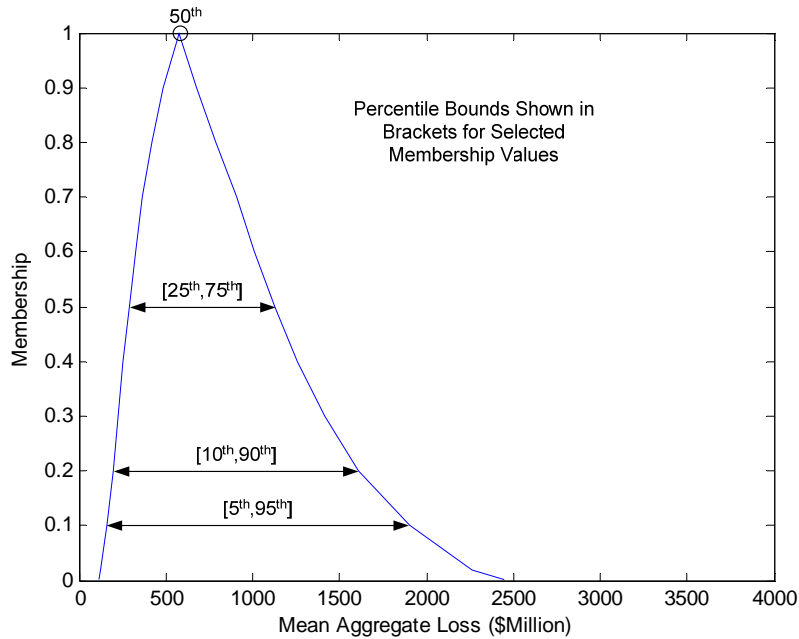


Figure B-24. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (hospital)

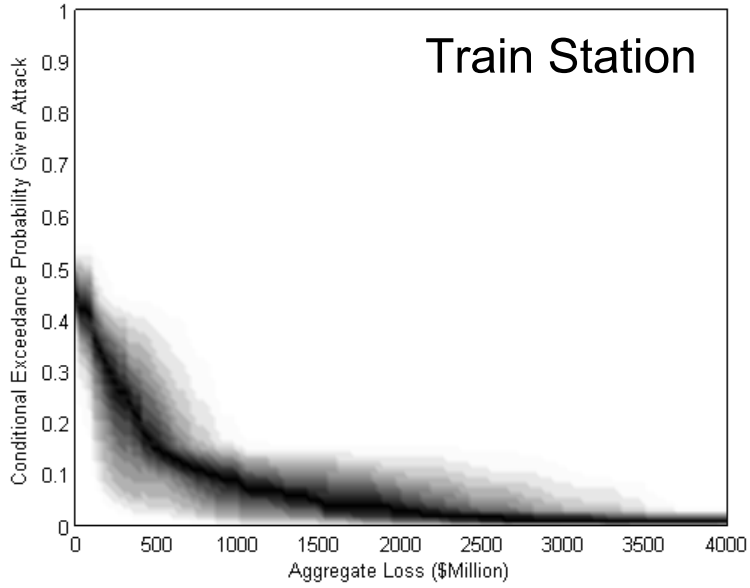


Figure B-25. Possibilistic conditional loss-exceedance curve given attack (train station)

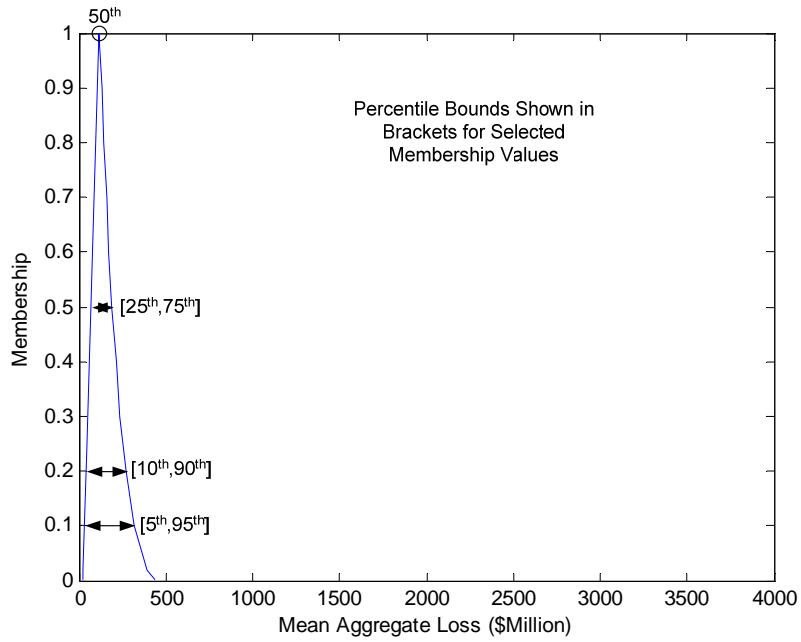


Figure B-26. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (train station)

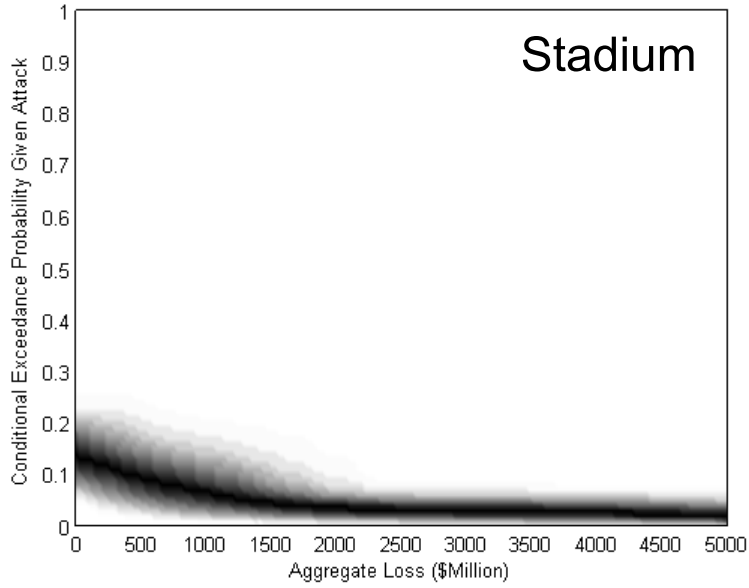


Figure B-27. Possibilistic conditional loss-exceedance curve given attack (stadium)

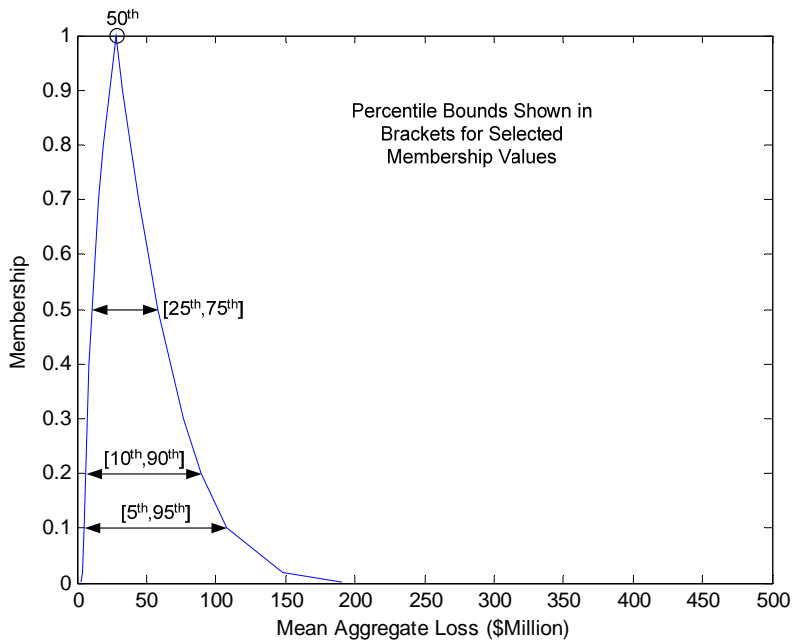


Figure B-28. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (stadium)

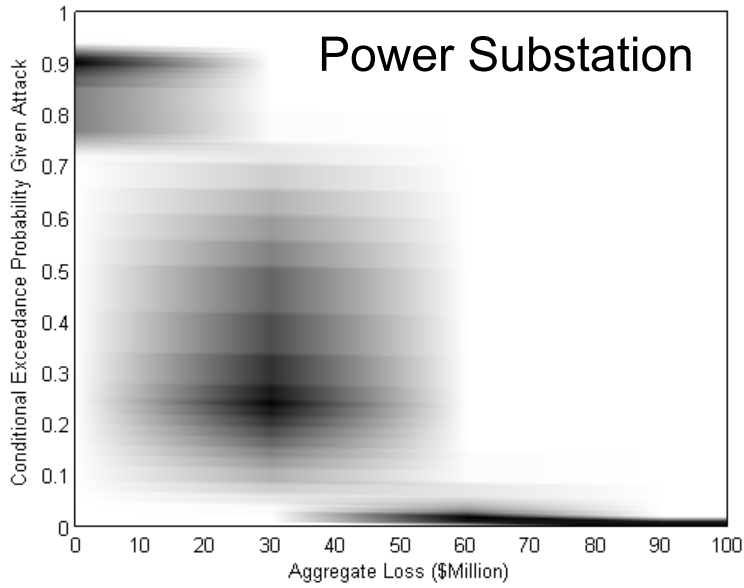


Figure B-29. Possibilistic conditional loss-exceedance curve given attack (power substation)

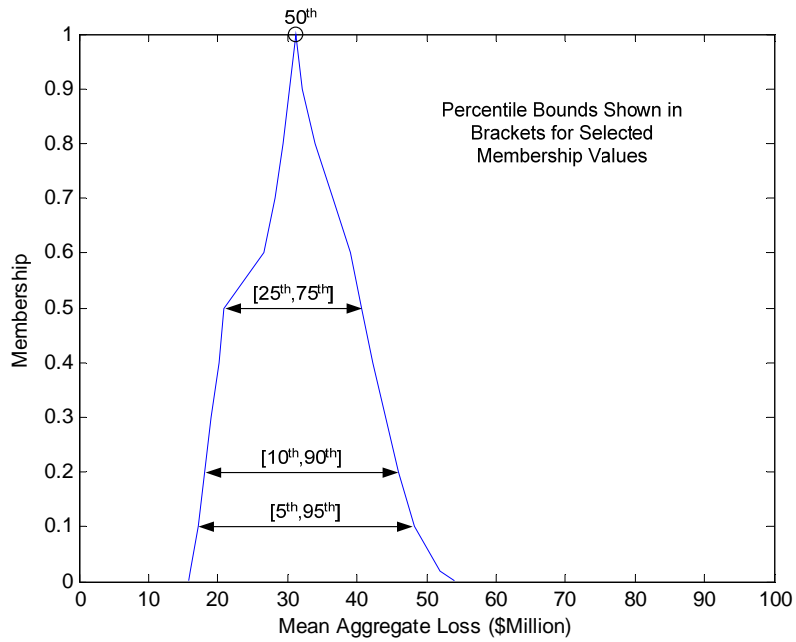


Figure B-30. Possibility distribution for the mean conditional loss given attack for selected pignistic percentiles (power substation)

Appendix C. Publications Resulting From This research

C.1. Accepted Publications to Peer-Reviewed Journals

Ayyub, B. M., McGill, W. L., and Kaminskiy, M. P. (2007). "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework." *Risk Analysis*, Vol. 27, No. 4, pp. 789-801.

McGill, W. L., and Ayyub, B. M. (2007). "Estimating Parameter Distributions in Structural Reliability Assessment Using the Transferable Belief Model." *Computers & Structures*, Vol. 86, No. 10, pp. 1052-1060.

McGill, W. L., and Ayyub, B. M. (2008b). "Multicriteria Security System Performance Assessment Using Fuzzy Logic." *Journal of Defense Modeling and Simulation*, Vol. 5, No. 1.

McGill, W. L., Ayyub, B. M., and Kaminskiy, M. P. (2007). "Risk Analysis for Critical Asset Protection." *Risk Analysis*, Vol. 27, No. 5, pp. 1265-1281.

C.2. Publications Submitted for Peer Review

McGill, W. L., and Ayyub, B. M. (2007). "Discussion of 'Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges' by James C. Ray." *Journal of Bridge Engineering*, Submitted.

C.3. Book Chapters

McGill, W. L., and Ayyub, B. M. (2007b). "The Meaning of Vulnerability in the Context of Critical Infrastructure Protection." in Jackson, E. ed. *Critical Infrastructure*

Protection: Elements of Risk. George Mason University Critical Infrastructure Protection Program.

McGill, W. L., and Ayyub, B. M. (2008). "Defeating Surprise through Threat Anticipation and Possibility Management." *Wiley Handbook of Science and Technology for Homeland Security*, Accepted for publication.

C.4. Conference Proceedings

Ayyub, B. M., and McGill, W. L. (2007). "An All-Hazards Methodology for Critical Asset and Portfolio Risk Analysis." *The Fourth Civil Engineering Conference in the Asian Region*, CECAR, Taipei, Taiwan, 25-28 June 2007.

C.5. Presentations

McGill, W. L. (2005), "Infrastructure Risk Analysis and Technology Surprise," Presented at the Second Annual DIA Technology Surprise Symposium, Institute for Defense Analyses, Alexandria, VA, 28-30 November 2005.

McGill, W. L., and Ayyub B. M. (2005), "A Quantitative Approach to Intelligence Analysis: Application of the Transferable Belief Model to the Analysis of Competing Hypotheses," Presented at the Society for Risk Analysis 2005 Annual Meeting, Orlando, FL, 05-07 December 2005.

Ayyub, B. M., and McGill, W. L. (2006), "Risk Analysis for Informing Resource Allocation Decisions," Presented at the Second Annual Intelligence Conference and Exhibition (INTELCON), Rockville, MD, 7-9 May 2006.

- McGill, W. L. (2006), "Quantitative Methods for Technology Warnings Analysis,"
Presented to DIA/DWO-4, 18 May 2006.
- McGill, W. L. (2006), "Risk Methods for Problems of National Interest," Presented to
ENME Lunchtime Seminar, 23 June 2006.
- McGill, W. L. "Risk Methods for Security and Intelligence Problems." Presented at the
National Conference on Security Analysis and Risk Management, 13-15 May
2008, George Mason University, Arlington, VA.
- Ayyub, B. M., and McGill, W. L. (2006), "Critical Asset and Portfolio Risk Analysis,"
Presented at the All-Hazards Forum in Baltimore Maryland, 12 October 2006.
- McGill, W. L., and Ayyub, B. M. (2006). "Evidence Theory-Based Parameter
Assessment for Homeland Security Risk Analysis." Presented at the INFORMS
2006 Annual Meeting, Pittsburgh, PA, 6-8 Nov 2006. (Invited)
- Ayyub, B. M., and McGill, W. L. (2006). "Critical Asset & Portfolio Risk Analysis:
Overview, Implementation, and Future Directions." Presented at the INFORMS
2006 Annual Meeting, Pittsburgh, PA, 6-8 Nov 2006. (Invited)
- Ayyub, B. M., and McGill, W. L. (2006). "The Critical Asset and Portfolio Risk Analysis
Methodology for Critical Infrastructure Protection." Presented at the Society for
Risk Analysis 2006 Annual Meeting, Baltimore, MD, 4-6 Dec 2006. (Invited)
- McGill, W. L. (2008). "Techniques for Adversary Threat Probability Assessment."
Presented at the *Critical Infrastructure Protection: Metrics and Tools Workshop*,
Center for Homeland Defense and Security, Naval Postgraduate School,
Monterey, CA, 5-7 June 2008.

- McGill, W. L., and Ayyub, B. M. (2006). "Quantitative Methods for Terrorism Warnings Analysis." Presented at the Society for Risk Analysis 2006 Annual Meeting, Baltimore, MD, 4-6 Dec 2006.
- McGill, W. L., and Ayyub, B. M. (2007). "On Vulnerability and Surprise in the Context of Critical Asset Protection." Presented at the Society for Risk Analysis 2007 Annual Meeting, San Antonio, TX, 9-12 Dec 2007.
- McGill, W. L., and Pikus, I. (2008). "A Workshop on Open Standards for Characterizing and Comparing Security Risk Analysis Methodologies." Presented at the National Conference on Security Analysis and Risk Management, 13-15 May 2008, George Mason University, Arlington, VA.

Appendix D. Curriculum Vitae

EDUCATION

University of Maryland, College Park, MD, *Doctor of Philosophy (In progress)*, 8/03–8/08

- Uncertainty modeling and analysis; risk analysis for homeland security; reliability analysis of civil and mechanical systems
- Thesis topic: “Critical Asset and Portfolio Risk Analysis for Homeland Security”
- Advisor: Professor Bilal M. Ayyub

National Defense Intelligence College, Washington, DC, 11/04–2/08

University of Maryland, College Park, MD, *Master of Science*, 8/01–5/03

University of Southern California, Los Angeles, CA, *Bachelor of Science*, 8/97–5/01

PROFESSIONAL EXPERIENCE

Pennsylvania State University, State College, PA, *Instructor*, 4/08–Present

- Conducts applied research in risk analysis, uncertainty modeling and decision analysis applied to homeland security, defense, and intelligence problems
- Develops and teaches undergraduate courses in security risk management as part of the security risk analysis program

Defense Intelligence Agency, Washington, DC, *Intelligence Officer*, 10/07–4/08

- Develops training courses and analytical capabilities within the intelligence and homeland security community in the areas of risk analysis, uncertainty modeling, and logical reasoning, and explores and evaluates new methodologies that enhance the quality and rigor of intelligence analysis while accommodating all relevant types of uncertainty
- Consulting methodologist charged with evaluating and developing approaches to solving challenging intelligence problems, including problems related to the protection of defense critical infrastructure

Consultant Risk Engineer and Uncertainty Analyst, 10/05–Present

- Applied structured analytical methodologies in support of intelligence, risk, reliability, and uncertainty analysis for the intelligence, defense, and homeland security communities; recent work included participating in the development of a capsizing risk assessment tool for naval vessels, risk-based fatigue life assessment tool for naval vessels, a risk assessment engine for the New Orleans hurricane protection system, and risk and reliability models for personal floatation devices
- Performed technology assessments for various emerging technologies; recent work focused on brain-computer interface and grey systems theory to support national policy decisions
- Facilitator for several expert elicitation sessions to obtain data to support quantitative risk modeling
- Peer-reviewer and expert panelist for various technology, vulnerability and risk analysis studies and methodologies spanning the homeland security and intelligence communities

University of Maryland, College Park, MD, *Research Assistant*, 8/05–Present

- Conducts basic and applied research in risk, uncertainty, and reliability analysis, including both probabilistic and non-probabilistic methods with applications in the areas of structural engineering, homeland security and intelligence analysis
- Developed innovative methodologies for target capabilities performance assessment and security system effectiveness assessment under a research grant from the Maryland Emergency Management Agency

- Provides instructor support for undergraduate and graduate courses in risk, uncertainty, and reliability analysis, and mentors undergraduate research projects in the areas of risk and uncertainty analysis

Defense Intelligence Agency, Washington, DC, *Technology Intelligence Analyst*, 6/04–9/05

- Produced technology assessments of emerging foreign technologies in support of senior decision maker requests; focus was on structural materials, infrastructure, and disruptive technologies
- Develop methodologies for assessing the types and significance of emerging terrorist technologies with respect to the risks faced by US critical infrastructure
- Program manager and COTR for a variety of government contracts in support of intelligence analysis; managed programs collectively valued at \$1.5-million and was recognized as a leader in marshalling funds from the community for technology assessments

American Society for Mechanical Engineers, Washington, DC, *Federal Fellow*, 6/03–6/04

- 2003 fellow to the Department of Homeland Security, Information Analysis and Infrastructure Protection Directorate
- Assisted DHS in developing first-generation approaches to critical infrastructure risk assessment and management for defensible resource allocation decisions
- Developed and applied terrorism risk analysis methodologies to establish priorities for critical infrastructure protection
- Conducted vulnerability assessments of critical infrastructure systems with respect to modern terrorist tactics

Swales Aerospace Inc., Beltsville, MD, *Structural Engineer*, 5/01–6/03

- Assessed the performance of mechanical and structural systems using classical (hand) and finite element analysis; supervised and draft test plans for structural environmental tests and consistently demonstrated correlation of test results with predictions
- Combined analytical skills with sound engineering judgment to determine the root cause of failure for failed structural and mechanical components leveraging results from material testing in conjunction with finite element analysis
- Provided structured training in finite element modeling and analysis to company engineers

TEACHING EXPERIENCE

Howard Community College, Columbia, MD, *Adjunct Instructor*, 9/06–12/07

- Provided undergraduate instruction in lower-division mathematics courses, including trigonometry, discrete structures, and differential equations

University of Maryland, College Park, MD, *Teaching Assistant/Substitute Instructor*, 9/05–9/07

- Teaching assistant or substitute instructor for several undergraduate courses within the school of engineering, including numerical methods and probability and statistics
- Substitute lecturer and course assistant for several graduate courses within the school of engineering, including risk analysis, uncertainty modeling; provided advice to graduate students on course projects
- Mentored several undergraduate researchers on projects related to uncertainty modeling and analysis for homeland security as part of the University of Maryland Undergraduate Research Program

University of Southern California, Los Angeles, CA, *Teaching Assistant*, 8/00–5/01

- Lab instructor for the third-year instrumentation course within the aerospace and mechanical engineering department

PUBLICATIONS AND REPORTS

- Ayyub, B. M., McGill, W. L., and Kaminskiy, M. (2007). "Critical Asset and Portfolio Risk Analysis for Homeland Security: An All-Hazards Framework." *Risk Analysis*, Volume 27, Number 4, Pages 789-801.
- McGill, W. L., and Ayyub, B. M. (2007). "A Transferable Belief Model for Estimating Parameter Distributions in Structural Reliability Assessment," *Computers & Structures*, Volume 86, Number 10, Pages 1052-1060.
- McGill, W. L., Ayyub, B. M., and Kaminskiy, M. (2007). "Risk Analysis for Critical Asset Protection," *Risk Analysis*, Volume 27, Number 5, Pages 1265-1281.
- McGill, W. L., and Ayyub, B. M. (2007). "The Meaning of Vulnerability in the Context of Critical Infrastructure Protection." George Mason University Monograph on Risk Analysis for Critical Infrastructure Protection.
- McGill, W. L., and Ayyub, B. M. (2007). "Defeating Surprise through Threat Anticipation and Possibility Management." *Wiley Handbook of Science and Technology for Homeland Security*, Accepted for publication.
- McGill, W. L., and Ayyub, B. M. (2007). "Multicriteria Security System Performance Assessment Using Fuzzy Logic." *Journal of Defense Modeling and Simulation*, Volume 5, Number 1.
- Ayyub, B. M., Foster, J., and McGill, W. L. (2008). "Risk Analysis of a Protected Hurricane-Prone Region: Methodology Development." *Natural Hazards Review*, Accepted for Publication.
- Ayyub, B. M., McGill, W. L., Foster, J., and Jones, H. W. (2008). "Risk Analysis of a Protected Hurricane-Prone Region: Computations and Illustration." *Natural Hazards Review*, Accepted for Publication.
- McGill, W. L. (2007). "Ungoverned Technology Assessment: Brain Computer Interface and Neurologically-Controlled Systems." Institute for Defense Analyses.
- McGill, W. L. (2007). "Ungoverned Technology Assessment: Grey-Systems Technology." Institute for Defense Analyses.
- McGill, W. L., and Ayyub, B. M. (2007). "Discussion of 'Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges' by James C. Ray." *Journal of Bridge Engineering*, Under Review.
- Ayyub, B. M., and McGill, W. L. (2007). "Fatigue Reliability and Life Assessment of the USCG NSC." BMA Engineering, Inc. Technical Report, Prepared for Engineering Logistics Center, United States Coast Guard, Department of Homeland Security.
- Ayyub, B. M., and McGill, W. L. (2007). "An All-Hazards Methodology for Critical Asset and Portfolio Risk Analysis." Presented at the CECA 2007, Taipei, Taiwan, and Submitted for publication in a forthcoming ASCE monograph.
- McGill, W. L., and White, R. H. (2008). "Emerging Adversarial Threats: Methods for Target Susceptibility Assessment and Criticality Screening." To be submitted to *Wiley Handbook of Science and Technology for Homeland Security*.

PRESENTATIONS AT CONFERENCES, SEMINARS, AND WORKSHOPS

- McGill, W. L. (2005), "Infrastructure Risk Analysis and Technology Surprise," *Presented at the Second Annual DIA Technology Surprise Symposium, Institute for Defense Analyses, Alexandria, VA, 28-30 November 2005.*
- McGill, W. L., and Ayyub B. M. (2005), "A Quantitative Approach to Intelligence Analysis: Application of the Transferable Belief Model to the Analysis of Competing Hypotheses," *Presented at the Society for Risk Analysis 2005 Annual Meeting, Orlando, FL, 05-07 December 2005.*
- Ayyub, B. M., and McGill, W. L. (2006), "Risk Analysis for Informing Resource Allocation Decisions," *Presented at the Second Annual Intelligence Conference and Exhibition (INTELCON), Rockville, MD, 7-9 May 2006.*
- McGill, W. L. (2006), "Quantitative Methods for Technology Warnings Analysis," *Presented to DIA/DWO-4, 18 May 2006.*

- McGill, W. L. (2006), "Risk Methods for Problems of National Interest," *Presented to ENME Lunchtime Seminar*, 23 June 2006.
- Ayyub, B. M., and McGill, W. L. (2006), "Critical Asset and Portfolio Risk Analysis," *Presented at the All-Hazards Forum in Baltimore Maryland*, 12 October 2006.
- McGill, W. L., and Ayyub, B. M. (2006). "Evidence Theory-Based Parameter Assessment for Homeland Security Risk Analysis." *Presented at the INFORMS 2006 Annual Meeting, Pittsburgh, PA, 6-8 Nov 2006.* (Invited)
- Ayyub, B. M., and McGill, W. L. (2006). "Critical Asset & Portfolio Risk Analysis: Overview, Implementation, and Future Directions." *Presented at the INFORMS 2006 Annual Meeting, Pittsburgh, PA, 6-8 Nov 2006.* (Invited)
- Ayyub, B. M., and McGill, W. L. (2006). "The Critical Asset and Portfolio Risk Analysis Methodology for Critical Infrastructure Protection." *Presented at the Society for Risk Analysis 2006 Annual Meeting, Baltimore, MD, 4-6 Dec 2006.* (Invited)
- McGill, W. L., and Ayyub, B. M. (2006). "Quantitative Methods for Terrorism Warnings Analysis." *Presented at the Society for Risk Analysis 2006 Annual Meeting, Baltimore, MD, 4-6 Dec 2006.*
- McGill, W. L. (2007). "Risk Methods for Warnings Analysis." *Presented to DIA/DWO-4*, 11 July 2007.
- McGill, W. L. (2007). "Risk Methods for Warnings Analysis." *Presented to J2W*, August 2007.
- McGill, W. L. (2007). "On Vulnerability and Surprise in the Context of Critical Asset Protection." *Presented at the Society for Risk Analysis 2007 Annual Meeting, San Antonio, TX, 9-12 Dec 2007.*
- McGill, W. L. (2008). "Security Effectiveness Assessment with Approximate Reasoning." *To be presented at the 2nd National Conference on Security Analysis and Risk Management, 13-15 May 2008, Arlington, VA.*
- McGill, W. L., and Ayyub, B. M. (2008). "Techniques for Adversary Threat Probability Assessment." *Presented at the Critical Infrastructure Protection: Metrics and Tools Workshop, Naval Postgraduate School, 5-7 June 2008, Monterey, CA.*

CERTIFICATIONS AND AWARDS

- Appointed ASME Federal Fellow to the Department of Homeland Security, 2003-2004
- Recipient of best paper award, 2006 Society for Risk Analysis Annual Meeting, Economics and Benefits Section
- Recipient of student travel award, 2007 Society for Risk Analysis Annual Meeting
- Registered Professional Engineer (State of Maryland)
- Certified Reliability Engineer (via the American Society of Quality)

PROFESSIONAL MEMBERSHIPS

- Security Analysis and Risk Management Association (SARMA)
- Society for Risk Analysis (SRA)
- American Society for Civil Engineers (ASCE)
- ASME International (ASME)
- International Association for Intelligence Education (IAFIE)

Bibliography

- Ackerman, G. A. (2006). "It Is Hard to Predict the Future: The Evolving Nature of Threats and Vulnerabilities." *Rev. sci. tech. Off. int. Epiz.* Vol. 25, No. 1, pp. 353-360
- Acton, J. M., Rogers, M. B., and Zimmerman, P. D. (2007). "Beyond the Dirty Bomb: Re-Thinking Radiological Terror." *Survival: Global Politics and Strategy*, Vol. 49, No. 3, pp. 151-168.
- American Chemistry Council (2002). *Modified Security Vulnerability Analysis Methodology for Tier 4 Facilities*. American Chemistry Council, Arlington, VA.
- American Heritage Dictionary (2007). *American Heritage Dictionary of the English Language*. Fourth Edition. Houghton Mifflin Company.
- American Petroleum Institute (2003). *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*. American Petroleum Institute, Washington, DC.
- American Society for Industrial Security (2003). *General Security Risk Assessment Guidelines*. ASIS International, Alexandria, VA.
- Amin, M. (2002). "Toward Secure and Resilient Interdependent Infrastructures." *Journal of Infrastructure Systems*, Vol. 8, No. 3, pp. 67-75.
- Ang, A. H-S., and Tang, W. H. (1975). *Probability Concepts in Engineering Planning and Design: Basic Principles Vol. 1*. Wiley.
- Apostolakis, G. E. (2004). "Redundancy and Nuclear Security." *Risk Analysis*, Vol. 24, No. 4, pp. 947-948.

- Apostolakis, G. E., and Lemon, D. M. (2005). "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism." *Risk Analysis*, Vol. 25, No. 2, pp. 361-376.
- Arboleda, C. A., Abraham, D. M., and Lubitz, R. (2007). "Simulation As a Tool to Assess the Vulnerability of the Operation of a Health Care Facility." *Journal of Performance of Constructed Facilities*, Vol. 21, No. 4, pp. 302-312.
- Arnold, J. L. (2002). "Disaster Medicine in the 21st Century: Future Hazards, Vulnerabilities, and Risk." *Prehospital and Disaster Medicine*, Vol. 17, No. 1, pp. 3-11.
- Association of Metropolitan Sewerage Agencies (2002). *Asset Based Vulnerability Checklist for Wastewater Facilities*. AMSA, Washington, DC.
- Aven, T. (2003). *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. Wiley.
- Aven, T. (2007). "A Unified Framework for Risk and Vulnerability Analysis Covering Both Safety and Security." *Reliability Engineering & System Safety*, Vol. 92, No. 6, pp. 745-754.
- Aven, T. (2008). *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities*. Wiley.
- Ayyub, B. M. (2001). *Elicitation of Expert Opinions for Uncertainty and Risks*, Boca Raton, FL: Chapman & Hall/CRC.
- Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. Florida: Chapman & Hall/CRC Press.

- Ayyub, B. M. (2005). *State of Maryland Guide for the Protection of Critical Infrastructure and Key Resources for Homeland Security Volume 1: Critical Asset & Portfolio Risk Analysis (CAPRA) Methodology*. DRAFT dated 29 Nov 2005.
- Ayyub, B. M., and Klir, G. J. (2006). *Uncertainty Analysis in Engineering and the Sciences*. Boca Raton, FL: Chapman & Hall/CRC Press.
- Ayyub, B. M., and McCuen, R. H. (1999). *Probability, Statistics, and Reliability for Engineers and Scientists*. 2nd Ed. Boca Raton, FL: Chapman & Hall/CRC.
- Ayyub, B. M., and McGill, W. L. (2007). "An All-Hazards Methodology for Critical Asset and Portfolio Risk Analysis." *The Fourth Civil Engineering Conference in the Asian Region*, CECAR, Taipei, Taiwan, 25-28 June 2007.
- Ayyub, B. M., McGill, W. L., and Kaminskiy, M. P. (2007). "Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework." *Risk Analysis*, 27(4): 789-801.
- Baker, J. C., Lachman, B. E., Frelinger, D. R., O'Connell, K. M., Hou, A. C., Tseng, M. S., Orletsky, D., and Yost, C. (2004). Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information, RAND Document MG-142-NGA.
- Baird, R. A. (2006). "Pyro-Terrorism - The Threat of Arson-Induced Forest Fires as a Future Terrorist Weapon of Mass Destruction." *Studies in Conflict & Terrorism*, Vol. 29, No. 5, pp. 415-428.
- Baldwin, T. E., Ramaprasad, A., and Samsa, M. E. (2008). "Understanding Public Confidence in Government to Prevent Terrorist Attacks." *Journal of Homeland Security and Emergency Management*, Vol. 5, No. 1, Article 4.

- Barnett, N., Graudioso, J., and Salerno, R. M. (2005). "Security Risk Assessment Methodology for Bioscience Facilities." SAND 2005-2729C, Sandia National Laboratories, Albuquerque, NM.
- Bashor, M. M. (1998). "International Terrorism and Weapons of Mass Destruction." *Risk Analysis*, Vol. 18, No. 6, pp. 675-678.
- Berresford, A., and Dando, M. (1978). "Operational Research for Strategic Decision Making: The Role of World View." *Journal of the Operational Research Society*, Vol. 29, No. 2, pp. 137-146.
- Bier, V. M., Nagaraj, A., and Abhichandani, V. (2005). "Protection of Simple Series and Parallel Systems with Components of Different Values." *Reliability Engineering & System Safety*, Vol. 87, pp. 313-323.
- Bier, V., Oliveros, S., and Samuleson, L. (2006). "Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker." *Journal of Public Economic Theory*, Vol. 9, No. 4, pp. 563-587.
- Blockley, D. I. (ed.) (1982). *Engineering Safety*, London: McGraw-Hill.
- Booz Allen Hamilton, Inc. (2000). *Analytical Risk Management*.
- Borio, L., Inglesby, T., Peters, C. J., Schmaljohn, A. L., Hughes, J. M., Jahrling, P. B., Ksiazek, T., Johnson, K. M., Meyerhoff, A., O'Toole, T., Ascher, M. S., Bartlett, J., Breman, J. G., Eitzen Jr., E. M., Hamburg, M., Hauer, J., Henderson, D. A., Johnson, R. T., Kwik, G., Layton, M., Lillibridge, S., Nabel, G. J., Osterholm, M. T., Perl, T. M., Russell, P., and Tonat, K. (2002). "Hemorrhagic Fever Viruses as Biological Weapons: Medical and Public Health Management." *Journal of the American Medical Association*, Vol. 287, pp. 2391-2405.

- Broder, J. F. (1984). *Risk Analysis and the Security Survey*. Massachusetts: Butterworth Publishers.
- Budescu, D. V., Karelitz, T. M., and Wallsten, T. S. (2003). "Predicting the Directionality of Probability Words from their Membership Functions." *Journal of Behavioral Decision Making*, 16(3): 159-180.
- Bunker, R. J. (2008). "Terrorists and Laser Weapons Use: An Emergent Threat." *Studies in Conflict & Terrorism*, Vol. 31, No. 5, pp. 434-455.
- Bunn, M. (2004). "Thinking About How Many Guards Will Do The Job." *Risk Analysis*, Vol. 24, No. 4, pp. 949-953.
- Bush, G. W. (2003). "Critical Infrastructure Identification, Prioritization, and Protection." HSPD-7.
- Caddell, J. W. (2004). *Deception 101 – Primer on Deception*. United States Army War College, Carlisle Barracks.
- Carroll, J. S. (2004). "Redundancy as a Design Principle and an Operating Principle." *Risk Analysis*, Vol. 24, No. 4, pp. 955-957.
- Center for Chemical Process Safety (2002). *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*.
- Cepin, M., Cizelj, L., Leskovar, M., and Mavko, B. (2006). "Vulnerability Analysis of a Nuclear Power Plant Considering Detonations of Explosive Devices." *Journal of Nuclear Science and Technology*, Vol. 43, No. 10, pp. 1258-1269.
- Chang, Y. H. J., and Mosleh, A. (2007). "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents: Part 1:

- Overview of the IDAC Model.” *Reliability Engineering & System Safety*, Vol. 92, No. 8, pp. 997-1013.
- Chapman, A. (2006). “Regulating Chemicals – From Risks to Riskiness.” *Risk Analysis*, Vol. 26, No. 3, pp. 603-616.
- Chapman, R. E., and Leng, C. J. (2004). “Cost Effective Responses to Terrorist Risks in Constructed Facilities.” NISTIR 7073, National Institute of Standards and Technology, Washington, DC.
- Chen, Y. Y., Liu, X. M., and Ren, F. T. (2002). "Disaster Risk Analysis of Transportation Infrastructure System." *Journal of Highway and Transportation Research and Development*, Vol. 19, No. 4, pp. 79-82.
- Chen, W. H., Jiang, Q. Y., Cao, Y. J., and Han, Z. X. (2005). "Risk Based Vulnerability Assessment in Complex Power Systems." *Power System Technology*, Vol. 29, No. 4, pp. 12-17.
- Cheng, S., Stough, R. R., and Kocornik-Mina, A. (2006). “Estimating the Economic Consequences of Terrorist Disruptions in the National Capital Region: An Application of Input-Output Analysis.” *Journal of Homeland Security and Emergency Management*, Vol. 3, No. 3, Article 12.
- Chiu, S. L. (1999). “Extracting Fuzzy Rules from Data for Function Approximation and Pattern Classification.” In Dubois, D., Prade, H., and Yager, R. eds. (1997). *Fuzzy Information Engineering: A Guided Tour of Applications*. Wiley & Sons.
- Chowdhury, L. M. and Sarkar, P. K. (2008). "Radiological Risk Analysis of Particle Accelerators." *Reliability Engineering & System Safety*, Vol. 93, No. 8, pp. 1250-1256.

- City of Livermore (2002). *All Hazard Vulnerability Assessment*. Annex D of the *Comprehensive Emergency Management Plan*.
- Cooke, R. M., and Goosens, L. H. J. (2004). "Expert Judgment Elicitation for Risk Assessments of Critical Infrastructures." *Journal of Risk Research*, Vol. 7, No. 6, pp. 643-656.
- Copes, W. S., Sacco, W. J., Champion, H. R., and Bain, L. W. (1998). "Progress in Characterising Anatomic Injury." In *Proceedings of the 33rd Annual Meeting of the Association for the Advancement of Automotive Medicine, Baltimore, MD, USA*, pp. 205-218.
- Copi, I. M. (1969). *Introduction to Logic*, 3rd Ed. The Macmillan Company, London.
- Cox Jr., L. A. (2002). *Risk Analysis: Foundations, Models and Methods*. Kluwer Academic Publishers, London.
- Cox, L. A., and Babayev, D. A. (2003). "Defending Networked Resources Against Intelligent Attacks." Source Unknown.
- Cox, L. A., Babayev, D., and Huber, W. (2005). "Some Limitations of Qualitative Risk Rating Systems," *Risk Analysis*, Vol. 25, No. 3, pp. 651-662.
- Crowe, T. D. (1991). *Crime Prevention Through Environmental Design*. Butterworth-Heinemann.
- Darby, J. L. (2006). "Evaluation of Risk from Acts of Terrorism: The Adversary/Defender Model Using Belief and Fuzzy Sets." *Journal of Nuclear Materials Management*, Vol. 35, No. 2, pp. 9-24.
- Deisler Jr., P. F. (2002). "A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism." *Risk Analysis*, Vol. 22, No. 3, pp. 405-413.

- Dessent, G. H. (1987). "Prison Perimeter Cost Effectiveness." *Journal of the Operational Research Society*, Vol. 10, pp. 975-980.
- Douglas, W. O. (1929). "Vicarious Liability and Administration of Risk I." *The Yale Law Journal*, Vol. 38, No. 5, pp. 584-604.
- Doyon, L. R. (1981). "Stochastic Modeling of Facility Security Systems for Analytical Solutions." *Computers & Industrial Engineering*, Vol. 5, No. 2, pp. 127-138.
- Drake, C. J. M. (1998). "The Role of Ideology in Terrorists' Target Selection." *Terrorism and Political Violence*, Vol. 10, No. 2, pp. 53-85.
- Dubois, D., and Prade, H. (1980). *Fuzzy Sets and Systems: Theory and Applications*. Elsevier Science & Technology Books.
- Dubois, D., Prade, H., and Smets, P. (2008). "A Definition of Subjective Possibility." *International Journal of Approximate Reasoning*, Vol. 48, No. 2, pp. 353-364.
- Einarsson, S., and Rausand, M. (1998). "An Approach to Vulnerability Analysis of Complex Industrial Systems." *Risk Analysis*, Vol. 18, No. 5, pp. 535-546.
- Eisenhower, S., Bott, T., and Rao, D. V. (2003). "Assessing the Risk of Nuclear Terrorism Using Logic Evolved Decision Analysis." LA-UR-03-3467, Los Alamos National Laboratory.
- Ellingwood, B. (2001). "Earthquake Risk Assessment of Building Structures." *Reliability Engineering & System Safety*, Vol. 74, No. 3, pp. 251-262.
- Elms, D. G. (1992). "Risk Assessment." in Blockley, D. I. (ed.) (1982). *Engineering Safety*, London: McGraw-Hill.
- Elms, D. G. (2004). "Structural Safety – Issues and Progress." *Progress in Structural Engineering Materials*, Vol. 6, No. 2, pp. 116-126.

- Enders, W., and Sandler T. (2005), "After 9/11: Is It All Different Now?," Working Paper, Available at http://www.cba.ua.edu/~wenders/after_911_ms.pdf.
- Ericson, R. V. (2006). "Ten Uncertainties of Risk Management Approaches to Security." *Canadian Journal of Criminology and Criminal Justice*, June, pp. 345-358.
- ExxonMobil (2002). *Chemical Facility Safeguards and Security Risk Assessment Methodology*.
- Ezell, B. C., Farr, J. V., and Wiese, I. (2000). "Infrastructure Risk Analysis Model." *Journal of Infrastructure Systems*, Vol. 6, No. 3, pp. 114-117.
- Fedra, K. (2008). Technology Risk Assessment and Management: Can We Integrate Terrorist Attacks? in Coskun, H. G. *Integration of Information for Environmental Security*. pp. 353-373.
- Ferson, S., Nelsen, R. B., Hajagos, J., Berleant, D. J., Zhang, J., Tucker, W. T., Ginzburg, L. R., and Oberkampf, W. L. (2004). *Dependence in Probabilistic Modeling, Dempster-Shafer Theory, and Probability Bounds Analysis*, SANDIA Technical Report, SAND2004-3072.
- Filliben, J. J., Gurley, K., Pinelli, J-P, and Simiu, E. (2002). "Fragility Curves, Damage Matrices, and Wind-Induced Loss Estimation." *Proceedings from the Third International Conference on Computer Simulation in Risk Analysis and Hazard Mitigation, June 19-21, 2002, Sintra, Portugal*, pp. 119-126.
- Fischer, R. J., & Green, G. (2004). *Introduction to Security*. 7th Ed., MA: Elsevier.
- Flax, L. K., Jackson, R. W., and Stein, D. N. (2001). "Community Vulnerability Assessment Tool Methodology." *Natural Hazards Review*, Vol. 3, No. 4, pp. 163-176.

- Fontaine, F., Debray, B., and Salvi, O. (2007). "Protection of Hazardous Installations and Critical Infrastructures - Complementarity of Safety and Security Approaches." *Managing Critical Infrastructure Risks*. I. Linkov ed., Springer, pp. 65-78.
- Fuqua, P., and Wilson, J. V. (1977). *Terrorism: The Executive's Guide to Survival*. Texas: Gulf Publishing Company.
- Garcia, M. L. (2006). *Vulnerability Assessment of Physical Protection Systems*. Elsevier Butterworth-Heinemann, Amsterdam.
- Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., Van Arsdale, L. A., and Zebroski, E. L. (2004). "Confronting the Risks of Terrorism: Making the Right Decisions." *Reliability Engineering and System Safety*, Vol. 86, No. 2, pp. 129-176.
- Gibson, S. D. (2003). "The Case for 'Risk Awareness'." *Security Journal*, Vol. 16, No. 3, pp. 55-64.
- Grabisch, M., Kojadinovic, I., and Meyer, P. (2007). "A Review of Methods for Capacity Identification in Choquet Integral Based Multi-Attribute Utility Theory: Applications of the Kappalab R Package." *European Journal of Operations Research*, In press.
- Grabo, C. M. (2002). *Anticipating Surprise: Analysis for Strategic Warning*. Joint Military Intelligence College, Washington, DC.
- Grzegorzewski, P., and Mrowka, E. (2005). "Trapezoidal Approximations of Fuzzy Numbers." *Fuzzy Sets and Systems*, Vol. 153, No. 1, pp. 115-135
- Grzegorzewski, P., and Mrowka, E. (2007). "Trapezoidal Approximations of Fuzzy Numbers - Revisited." *Fuzzy Sets and Systems*, Vol. 158, No. 7, pp. 757-768.

- Gutting, B. W., Channel, S.R., Berger, A. E., Gearhart, J. M., Andrews, G. A., Sherwood, R. L., and Nichols, T. L. (2008). "Mathematically Modeling Inhalation Anthrax." *Microbe*, Vol. 3, No. 2, pp. 78-85.
- Haimes, Y. Y. (1981). "Total Risk Management." *Risk Analysis*, Vol. 11, No. 2, pp. 169-171.
- Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*. 2nd Ed. Wiley, NY.
- Haimes, Y. Y., and Jiang, P. (2001). "Leontif-Based Model of Risk in Complex Interconnected Infrastructures." *Journal of Infrastructure Systems*, Vol. 7, No. 1, pp. 1-12.
- Haimes, Y. Y. (2006). "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures." *Risk Analysis*, Vol. 26, No. 2, pp. 293-296.
- Hammit, J. K. (2002). "QALYs versus WTP." *Risk Analysis*, Vol. 22, No. 5, pp. 985-1001.
- Hammond, J. (2005). "Mass Casualty Incidents: Planning Implications for Trauma Care." *Scandinavian Journal of Surgery*, Vol. 94, No. 4, pp. 267-271.
- Haque, C. E., and Etkin, D. (2007). "People and Community as Constituent Parts of Hazards: The Significance of Societal Dimensions in Hazards Analysis." *Natural Hazards*, Vol. 41, pp. 271-282.
- Harris, B. (2004). "Mathematical Methods in Combatting Terrorism." *Risk Analysis*, Vol. 24, No. 4, pp. 985-988.
- Hart, S. V. (2002). *A Method to Assess the Vulnerability of U.S. Chemical Facilities*, National Institute of Justice.

- Herabat, P., Barry, W., and Sunkpho, J. (2003). "Vulnerability Assessment and Security Planning for Thailand's Ground Transportation Infrastructures." *Journal of the Eastern Asia Society for Transportation Studies*, Vol. 5, pp. 3126-3141.
- Hicks, M. J., Snell, M. S., Sandoval, J. S., & Potter, C. S. (1999). "Physical Protection - Systems – Cost and Performance Analysis: A Case Study." *IEEE AES Systems Magazine*, April 1999.
- Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press.
- Hollenstein, K. (2005). "Reconsidering the Risk Assessment Concept: Standardizing the Impact Description as a Building Block for Vulnerability Assessment." *Natural Hazards and Earth System Sciences*, Vol. 5, pp. 301-307.
- Hollenstein, K., Bieri, O., and Stuckelberger, J. (2002). Modellierung der Vulnerability von Schadenobjekten gegenüber Naturgefahrenprozessen.
- Hunter, D. E. (1984). *Political / Military Applications of Bayesian Analysis: Methodological Issues*. Boulder, CO, Westview Press.
- Johnson, C. W. (2006). "What Are Emergent Properties And How Do They Affect the Engineering of Complex Systems?" *Reliability Engineering & System Safety*, Vol. 91, No. 12, pp. 1475-1481.
- Kaplan, S. (2002). Applying the General Theory of Quantitative Risk Assessment (QRA) to Terrorism Risk. 10th United Engineering Foundation Conference. Y. Y. Haimes, D. A. Moser and E. Z. Stakhiv. Santa Barbara, CA, ASCE.
- Kaplan, S., and Garrick, B. J. (1981). "On the Quantitative Definition of Risk." *Risk Analysis*, Vol. 1, No. 1, pp. 11-27.

- Kaplan, S., Haimes, Y. Y., and Garrick, B. J. (2001). "Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk." *Risk Analysis*, Vol. 21, No. 5, pp. 807-
- Kaplan, S., Visnopolshi, S., Zlotin, B., and Zusman, A. (1999). *New Tools for Failure & Risk Analysis: Anticipatory Failure Determination (AFD) & the Theory of Scenario Structuring*. Ideation International.
- Kapur, J. N. (1990). *Maximum Entropy Models in Science and Engineering*, Wiley & Sons.
- Karimi, I. (2006). *Risk Management of Natural Disasters: A Fuzzy-Probabilistic Methodology and its Application to Seismic Hazard*. Department of Structural Statics and Dynamics. Aachen, Germany, RWTH Aachen University. Doctor of Engineering.
- Karimi, I., and Hüllermeier, E. (2007). "Risk Assessment System for Natural Hazards: A New Approach Based on Fuzzy Probability." *Fuzzy Sets & Systems*, Vol. 158, No. 9, pp. 987-999.
- Kean, T. H., Hamilton, L. H., Ben-Veniste, R., Kerrey, B., Fielding, F. F., Lehman, J. F., Gorelick, J. S., Roemer, T. J., Gorton, S., and Thompson, J. R. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. US Government Printing Office.
- Keeney, R. L. (1981). "Measurement Scales for Quantifying Attributes." *Behavioral Science*, Vol. 26, No. 1, pp. 29-36.

- Kemp, R. L. (2007). "Vulnerability Assessments for Public and Private Facilities." *Journal of Business Continuity & Emergency Planning*, Vol. 1, No. 3, pp. 245-251.
- Kipfer, B. A. (Ed.). (2005). *Webster's New Millennium Dictionary of English* (preview edition v. 0.9.6). Long Beach, CA: Lexico Publishing Group.
- Klir, G. J. (1997). "Fuzzy Arithmetic with Requisite Constraints." *Fuzzy Sets and Systems*, Vol. 91, No. 2, pp. 165-175.
- Klir, G. J., and Yuan, B. (1995). *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Pearson Education.
- Kobza, J. E., and Jacobson, S. H. (1997). "Probability Models for Access Security System Architectures." *Journal of the Operational Research Society*, Vol. 48, pp. 255-263.
- Kondratov, S., and Steinhausler, F. (2006). "Why There is a Need to Revise the Design Basis Threat Concept." *International Journal of Nuclear Law*, Vol. 1, No. 2, pp. 182-188.
- Kosko, B. (1997). *Fuzzy Engineering*. Prentice Hall: Upper Saddle River, NJ.
- Kotz, S. (2003). *The Stress-Strength Model and Its Generalizations: Theory and Applications*. World Scientific.
- Kowalski, W. J. (2002). *Immune Building Systems Technology*. McGraw-Hill.
- Kumamoto, H. and Henley, E. J. (2000). *Probabilistic Risk Assessment and Management for Engineers and Scientists*. IEEE Press.
- Kunreuther, H. (2002). "The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage." *Risk Analysis*, Vol. 22, No. 3, pp. 427-437.

- Kuo, R. J., Hong, S. M., Sheu, J.-B., Lin, Y., and Huang, Y. C. (2008). "Continuous Genetic Algorithm-Based Fuzzy Neural Network for Learning Fuzzy IF-THEN Rules." *Neurocomputing*, Article In Press.
- Lamadrid, R. G. U. (2002). *Seismic Hazard and Vulnerability Assessment in Turrialba, Costa Rica*. International Institute for Geo-Information Science and Earth Observation. Enschede, The Netherlands.
- Lave, L. (2002). "View Point: Risk Analysis and the Terrorism Problem in Two Parts." *Risk Analysis*, Vol. 22, No. 3, pp. 403.
- Lee, E., Mitchell, J. E., and Wallace, W. A. (2007). "Restoration of Services in Interdependent Infrastructure Systems: A Network Flows Approach." *IEEE Transactions on Systems, Man, and Cybernetics Part C*, Vol. 37, No. 6, pp. 1303-1317.
- Leone, K., Liu, R. (2006). "Analysis of Security Systems Designs for Ferry Transportation." *Transportation Research Record: Journal of the Transportation Research Board*, No. 1955, pp. 8-13.
- Leung, M., Lambert, J. H., and Mosenthal, A. (2004). "A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks." *Risk Analysis*, Vol. 24, No. 4, pp. 963-984.
- Li, B., Li, M., and Smidts, C. (2005). "Integrating Software into PRA: A Test-Based Approach." *Risk Analysis*, Vol. 25, No. 4, pp. 1061-1077.
- Li, B., Li, M., Chen, K., and Smidts, C. (2006). "Integrating Software into PRA: A Software-Related Failure Mode Taxonomy." *Risk Analysis*, Vol. 26, No. 4, pp. 997-1012.

- Lichtenstein, S., and Newman, J. R. (1967). "Empirical Scaling of Common Verbal Phrases Associated with Numerical Probabilities." *Psychonomic Science*, 9(10): 563-564.
- Mahoney, E. E. (2007). *Analyzing the Effects of Blast Loads on Bridges Using Probability, Structural Analysis, and Performance Criteria*. Department of Civil and Environmental Engineering. College Park, MD, University of Maryland. Master of Science.
- Mairal, G. (2008). "Narratives of Risk." *Journal of Risk Research*, Vol. 11, No. 1, pp. 41-54.
- Manunta, G. (1999a). "Security Decision Making and PRA Methodology: Does PRA Methodology Effectively Assist Security Decision Makers?." *Journal of Security Administration*, Vol. 22, No. 2, pp. 1-9.
- Manunta, G. (1999b). "What is Security?" *Security Journal*, Vol. 12, No. 3, pp. 57-66.
- Manunta, G. (2002). "Risk and Security: Are They Compatible Concepts?" *Security Journal*, Vol. 15, No. 3, pp. 43-55.
- Martz, H. F., and Johnson, M. E. (1987). "Risk Analysis of Terrorist Attacks." *Risk Analysis*, Vol. 7, No. 1, 35-47.
- Masse, T., O'Neil, S., and Rollins, J. (2007). "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress." CRS RL33858, Congressional Research Service, Washington, DC.
- Matalucci, R. V. (2002). "Risk Assessment Methodology for Dams (RAM-D)." *Proceedings of the 6th International Conference on Probabilistic Safety*

Assessment and Management (PSAM6), 23-28 June 2002, San Juan, Puerto Rico, USA, Vol. 1, 169-176.

McGill, W. L. (1957). "How a State Prepares for Disaster." *The Annals of the American Academy of Political and Social Science*, Vol. 309, No. 1, pp. 89-97.

McGill, W. L. (2008). "Techniques for Adversary Threat Probability Assessment." Presented at the *Critical Infrastructure Protection: Metrics and Tools Workshop*, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA, 5-7 June 2008.

McGill, W. L., and Ayyub, B. M. (2006). "Quantitative Methods for Terrorism Warnings Analysis." Presented at the *Society for Risk Analysis 2006 Annual Meeting*, Baltimore, MD, 4-6 Dec 2006.

McGill, W. L., and Ayyub, B. M. (2007a). "Estimating Parameter Distributions in Structural Reliability Assessment Using the Transferable Belief Model." *Computers & Structures*, Vol. 86, No. 10, pp. 1052-1060.

McGill, W. L., and Ayyub, B. M. (2007b). "The Meaning of Vulnerability in the Context of Critical Infrastructure Protection." in Jackson, E. ed. *Critical Infrastructure Protection: Elements of Risk*. George Mason University Critical Infrastructure Protection Program.

McGill, W. L., and Ayyub, B. M. (2008a). "Defeating Surprise through Threat Anticipation and Possibility Management." *Wiley Handbook of Science and Technology for Homeland Security*, Submitted.

- McGill, W. L., and Ayyub, B. M. (2008b). "Multicriteria Security System Performance Assessment Using Fuzzy Logic." *Journal of Defense Modeling and Simulation*, Vol. 5, No. 1.
- McGill, W. L., Ayyub, B. M., and Kaminskiy, M. P. (2007). "Risk Analysis for Critical Asset Protection." *Risk Analysis*, Vol. 27, No. 5, pp. 1265-1281.
- McGill, W. L., and Pikus, I. (2008). "A Workshop on Open Standards for Characterizing and Comparing Security Risk Analysis Methodologies." *Presented at the National Conference on Security Analysis and Risk Management*, 13-15 May 2008, George Mason University, Arlington, VA.
- Mendonca, D., and Wallace, W. A. (2006). "Impacts of the 2001 World Trade Center Attack on New York City Critical Infrastructures." *Journal of Infrastructure Systems*, Vol. 12, No. 4, pp. 260-270.
- Mileti, D. S. (1999). *Disasters by Design: A Reassessment of Natural Hazards in the United States*. Joseph Henry Press.
- Miller, G. A. (1956). "The Magical Number Seven, Plus or Minus Two: Some Limits On Our Capacity for Processing Information." *The Psychological Review*, 63(2): 81-97.
- Modarres, M. M. (1992). *What Every Engineer Should Know About Reliability and Risk Analysis*. CRC Press.
- Modarres, M. M., Kaminskiy, M., and Krivstov, V. (1999), *Reliability Engineering and Risk Analysis: A Practical Guide*, Marcel Dekker, NY.
- Molchanov, I. (2005). *Theory of Random Sets*. Springer.

- Moore, D. A. (2006). "Application of the API/NPRA SVA Methodology to Transportation Security Issues." *Journal of Hazardous Materials*, Vol. 130, pp. 107-121.
- Moore, D. A., Fuller, B., Hazzan, M., and Jones, J. W. (2007). "Development of a Security Vulnerability Assessment for the RAMCAP Chemical Sector." *Journal of Hazardous Materials*, Vol. 142, pp. 689-694.
- Morgeson, J. D., Utgoff, V. A., Fainberg, M. A., and Keleher, M. (2006). *National Comparative Risk Assessment Pilot Project. Volume I: Main Text with Appendixes A and B*, IDA Document D-3309, Institute for Defense Analyses, Alexandria, VA.
- Mosleh, A., and Chang, Y. H. (2004). "Model-Based Human Reliability Analysis: Prospects and Requirements." *Reliability Engineering & System Safety*, Vol. 83, pp. 241-253.
- Moteff, J. (2005). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. Congressional Research Service Report to Congress, Order Code RL32561.
- National Infrastructure Institute (2007). "CARVER2®: Critical Infrastructure Assessment Tool." National Infrastructure Institute Center for Infrastructure Expertise. Available at: <http://www.ni2ciel.org/CARVER2.asp>.
- National Research Council (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, Washington, DC.

- National Rural Water Association (2002). *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*. Association of State Drinking Water Administrators.
- Neale, D. (2008). Personal Communication.
- Nerud, B. (2008). "Terrorist Attack Analysis: A Systems Approach to Developing Proactive Antiterrorism Programs." *Presented at the Second National Conference on Security Analysis and Risk Management*, 13-15 May 2008, George Mason University, Arlington, VA.
- Newland, D. E., and Cebon, D. (2002). "Could the World Trade Center Have Been Modified to Prevent its Collapse?" *Journal of Engineering Mechanics*, Vol. 128, No. 7, pp. 795-800.
- Oxford University Press (2004). *The Oxford Dictionary of Proverbs*. Oxford University Press.
- Parfenov, Y., Zdoukhov, L. N., and Radasky, W. A. (2004). "Conducted IEMI Threats for Commercial Buildings." *IEEE Transactions on Electromagnetic Compatibility*, Vol. 46, No. 3, pp. 404-411.
- Passino, K. M., and Yurkovich, S. (1998). *Fuzzy Control*. Addison-Wesley: Menlo Park, CA.
- Pate-Cornell, M. E. (1986). "Warning Systems in Risk Management." *Risk Analysis*, Vol. 6, No. 2, pp. 223-234.
- Pate-Cornell, E. (2007). "Probabilistic Risk Analysis versus Decision Analysis: Similarities, Differences and Illustrations." in *Uncertainty & Risk*, pp. 232-242.

- Pate-Cornell, E., and Guikema, S. (2002). "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures." *Military Operations Research*, Vol. 7, No. 4, pp. 5-23.
- Pluchinsky, D. (2002). "The Heard it All Here, and That's the Trouble." *Washington Post*, 16 June 2002, pp. B03.
- Poptanich, K. (2008). "Strategic Homeland Security Risk Assessment." Presented at the *Critical Infrastructure Protection: Metrics and Tools Workshop*, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA, 5-7 June 2008.
- Powers, M. R. (2008). "The Mathematics of Terrorism Risk: Equilibrium Force Allocations and Attack Probabilities." Presented at the *Critical Infrastructure Protection: Metrics and Tools Workshop*, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA, 5-7 June 2008.
- President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations: Protecting America's Infrastructures*. Washington, DC, White House.
- Purpura, P. P. (2008). *Security and Loss Prevention*. 5th Ed. Elsevier Butterworth-Heinemann, Amsterdam.
- Rakar, A., and Juricic, D. (2002). "Diagnostic Reasoning Under Conflicting Data: The Application of the Transferable Belief Model." *Journal of Process Control*, Vol. 12, No. 1, pp. 55-67.

- Rakar, A., Juricic, D., and Balle, P. (1999). "Transferable Belief Model in Fault Diagnosis." *Engineering Applications of Artificial Intelligence*, Vol. 12, No. 5, pp. 555-567.
- Ray, J. C. (2007). "Risk-Based Prioritization of Terrorist Threat Mitigation Measures on Bridges." *Journal of Bridge Engineering*, Vol. 12, No. 2, pp. 140-146.
- Ren, L. C. (1999). "Advance in Risk Analysis for Natural Disasters." *Advances in Earth Science*, Vol. 14, No. 3.
- Resnyansky, L. (2006). "Conceptualisation of Terrorism in Modeling Tools: Critical Reflexive Approach." *Prometheus*, Vol. 24, No. 4, pp. 441-447.
- Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001), "Complex Networks: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001.
- Rosoff, H., and von Winterfeldt, D. (2007). "A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach." *Risk Analysis*, Vol. 27, No. 3, pp. 533-546.
- Sagan, S. D. (2004). "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security." *Risk Analysis*, Vol. 24, No. 4, pp. 935-946.
- Sandler, T., and Lapan, H. E. (1988). "The Calculus of Dissent: An Analysis of Terrorists' Choice of Targets." *Synthese*, Vol. 76, pp. 245-261.
- Sandman, P. M. (1989). "Hazard versus Outrage in the Public Perception of Risk." in Covello, V. T., McCallum, D. B., and Pavlova, M. T. eds., *Effective Risk*

Communication: The Role and Responsibility of Government and Nongovernment Organizations, Springer.

- Science Applications International Corporation (2002). *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. Transportation Policy and Analysis Center, SAIC, Vienna, VA.
- Sentz, K., and Ferson, S. (2002). *Combination of Evidence in Dempster-Shafer Theory*, SANDIA Technical Report, SAND2002-0835.
- Shackle, G. L. S. (1969). *Decision, Order, and Time in Human Affairs*. 2nd Ed. Oxford University Press.
- Shafer, G. (1976). *A Mathematical Theory of Evidence*. Princeton University Press, NJ.
- Skidmore, M., and Toya, H. (2002). "Do Natural Disasters Promote Long-Run Growth." *Economic Inquiry*, Vol. 40, No. 4, pp. 664-687.
- Slovic, P. (2002). "Terrorism as Hazard: A New Species of Trouble." *Risk Analysis*, Vol. 22, No. 3, pp. 425-426.
- Smets, P. (1988). "Belief Functions." in Smets, P., Mamdani, A., Dubois, D., and Prade, H. *Non-Standard Logics for Automated Reasoning*, pp. 253-286.
- Smets, P. (1992). "The Concept of Distinct Evidence." *Proceedings of the 4th Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems, IPMU 92*, Palma de Mallorca, 6-10 July 92, pp. 789-794.
- Smets, P. (2005a). "Belief Functions on Real Numbers." *International Journal of Approximate Reasoning*, Vol. 40, No. 3, pp. 181-223.

- Smets, P. (2005b). "Decision Making in the TBM: The Necessity of the Pignistic Transformation." *International Journal of Approximate Reasoning*, Vol. 38, No. 2, pp. 133-147.
- Smets, P., Kennes, R. (1994). "The Transferable Belief Model." *Artificial Intelligence*, Vol. 66, No. 2, pp. 191-234.
- Smidts, C., Shen, S. H., and Mosleh, A. (1997). "The IDA Cognitive Model for the Analysis of Nuclear Power Plant Operator Response Under Accident Conditions. Part I. Problem Solving and Decision Making Model." *Reliability Engineering & System Safety*, Vol. 55, pp. 51-71.
- Society for Risk Analysis (2008). Home Page. Available at <http://www.sra.org>.
- Stewart, M. G., and Netherton, M. D. (2007). "Security Risks and Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading." *Reliability Engineering & System Safety*, Vol. 93, No. 4, pp. 627-638.
- Swaminathan, S., and Smidts, C. (1999a). "The Event Sequence Diagram Framework for Dynamic Probabilistic Risk Assessment." *Reliability Engineering & System Safety*, Vol. 63, pp. 73-90.
- Swaminathan, S., and Smidts, C. (1999b). "The Mathematical Formulation for the Event Sequence Diagram Framework." *Reliability Engineering & System Safety*, Vol. 65, pp. 103-118.
- Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House.
- Taylor, M. (2002). "Identifying Vulnerability: Enhancing Organizational Security in the Post 9-11 World." American International Security Corporation, Boston, MA.

- US Department of Defense (2005). "Defense Critical Infrastructure Program (DCIP)." Department of Defense Directive Number 3020.40, 19 Aug 2005.
- US Department of Energy (2002). *Vulnerability Assessment Methodology: Electric Power Infrastructure*. Office of Energy Assurance.
- US Department of Homeland Security (2006a). "DHS Introduces Risk-Based Formula for Urban Areas Security Initiative Grants." URL: https://www.dhs.gov/xnews/releases/press_release_0824.shtm.
- US Department of Homeland Security (2006b). *National Infrastructure Protection Plan*. Washington, DC.
- US Department of Homeland Security (2006c). *Target Capabilities List version 2.0*.
- US Department of Justice (2000). "Department of Justice Assessment of the Increased Risk of Terrorist or Other Criminal Activity Associated with Posting Off-Site Consequence Analysis Information on the Internet." Via Lexis-Nexis.
- US Department of the Army (1994). *Security Engineering Project Development*. TM-5-853-1.
- US Department of the Army (1998). *Intelligence Officer's Handbook*. FM 34-8-2.
- US Federal Emergency Management Agency (2003). *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. FEMA 426.
- US Federal Highway Administration (2003). *Recommendations for Bridge and Tunnel Security*. Blue Ribbon Panel n Bridge and Tunnel Security.
- US Food and Drug Administration (2007). *An Overview of the CARVER Plus Shock Method for Food Sector Vulnerability Assessments*.

- Van Keuren, E., Wilkenfeld, J., and Knighten, J. (1991). "Utilization of High-Power Microwave Sources in Electronic Sabotage and Terrorism." *Proceedings of IEEE Security Technology Conference* 1991, pp. 16-20.
- Veatch, J. D., James, J. W., May, T. T., and Trolan, W. L. (2002). "An Airport Vulnerability Assessment Methodology." Science Applications International Corporation, Vienna, VA.
- Vellani, K. H. (2007). *Strategic Security Management: A Risk Assessment Guide for Decision Makers*. Elsevier Butterworth-Heinemann, Amsterdam.
- Viscusi, W. K., and Aldy, J. E. (2003). "The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World." *Journal of Risk and Uncertainty*, Vol. 27, No. 1, pp. 5-76.
- Walley, P. (1990). *Statistical Reasoning with Imprecise Probabilities*. Chapman & Hall.
- Wallsten, T. S., and Budescu, D. V. (1994). "A Review of Human Linguistic Probability Processing: General Principles and Empirical Evidence." *The Knowledge Engineering Review*, 10(1): 43-62.
- Wang, Z., and Liu, M. (2006). "Application of Quantitative Risk Assessment on Terrorist Attack." *China Public Security*, Vol. 12, No. 4, pp. 18-22.
- Washburn, A. R. (2002). "Notes on Firing Theory." Naval Postgraduate School.
- Westrum, R. (2004). "Increasing the Number of Guards at Nuclear Power Plants." *Risk Analysis*, Vol. 24, No. 4, pp. 959-961.
- White House (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC.

- Williamson, R. C., and Downs, T. (1990). "Probabilistic Arithmetic I: Numerical Methods for Calculating Convolutions and Dependency Bounds." *International Journal of Approximate Reasoning*, Vol. 4, pp. 89-158.
- Willis, H. H., Morral, A. R., Kelly, T. K., and Medby, J. J. (2005). *Estimating Terrorism Risk*. Center for Terrorism Risk Management Policy, RAND Corporation, Pittsburgh, PA.
- Wolfers, A. (1952). "'National Security' as an Ambiguous Symbol." *Political Science Quarterly*, Vol. 67, No. 4, pp. 481-502.
- Woo, G. (1999). *The Mathematics of Natural Catastrophes*. Imperial College Press.
- Woo, G. (2002). "Quantitative Terrorism Risk Assessment." *Journal of Risk Finance*, Fall 2002, pp. 7-14.
- Wu, Z. Z., Zhang, Z. (2005). "Progress of Risk Assessment for Terror Attacks on Industrial Facilities." *Journal of Safety Science and Technology*, Vol. 1, No. 4, pp. 3-7.
- Yager, R. R. (1986). "Arithmetic and Other Operations on Dempster-Shafer Structures." *International Journal of Man-Machine Studies*, Vol. 25, pp. 357-366.
- Yager, R. R. (1987). "On the Dempster-Shafer Framework and New Combination Rules." *Information Sciences*, Vol. 41, No. 2, pp. 93-137.
- Yager, R. R. (2006). "OWA Trees and their Role in Security Modeling Using Attack Trees." *Information Sciences*, Vol. 176, pp. 2933-2959.
- Zadeh, L. A. (1965). "Fuzzy Sets." *Information and Control*, Vol. 8, pp. 338-353.
- Zadeh, L. A. (1975). "The Concept of a Linguistic Variable and its Application to Approximate Reasoning, Part I." *Information Sciences*, 8(3): 199-249.

- Zadeh, L. A. (1984). "Precision of Meaning via Translation Into PRUF." in Vaina, L., and Hintikka, J. *Cognitive Constraints on Communication*. Kluwer.
- Zadeh, L. A. (1999). "Fuzzy Sets as a Basis for a Theory of Possibility." *Fuzzy Sets and Systems*, Vol. 100 Supplement, pp. 9-34.
- Zadeh, L. A. (2005). "Toward a Generalized Theory of Uncertainty (GTU) – An Outline." *Information Sciences*, Vol. 172, pp. 1-40.
- Zhang, Z., Wu, Z. Z., and Liu, M. (2004). "A Case Study on Mitigating the Risk of Terror Attack." *China Safety Science Journal*, Vol. 14. No. 2, pp. 95-97.
- Zhang, S. B., Tian, D. F., and Wu, J. (2006). "Simple Probabilistic Method for Relative Risk Evaluation of Nuclear Terrorism Events." *Nuclear Power Engineering*, Vol. 27, No. 6, pp. 74-81.
- Zhao, G. M., M. Liu, Zhang, Q. S., Yang, Y., and Wang, L. (2006). "Terror Attack Risk Assessment of Subway Station Based on Game Theory." *Journal of Safety and Environment*, Vol. 6, No. 3, pp. 47-50.