SANDIA REPORT

SAND2006-5777

Unlimited Release

Printed September 2006

Evaluation of Risk from Acts of Terrorism: The Adversary/Defender Model Using Belief and Fuzzy Sets

John L. Darby

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.osti.gov/bridge>

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>

SAND2006-5777
Unlimited Release
Printed September 2006

Evaluation of Risk from Acts of Terrorism: The Adversary/Defender Model Using Belief and Fuzzy Sets

John L. Darby
Department 6442
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Abstract

Risk from an act of terrorism is a combination of the likelihood of an attack, the likelihood of success of the attack, and the consequences of the attack. The considerable epistemic uncertainty in each of these three factors can be addressed using the belief/plausibility measure of uncertainty from the Dempster/Shافر theory of evidence. The adversary determines the likelihood of the attack. The success of the attack and the consequences of the attack are determined by the security system and mitigation measures put in place by the defender. This report documents a process for evaluating risk of terrorist acts using an adversary/defender model with belief/plausibility as the measure of uncertainty. Also, the adversary model is a linguistic model that applies belief/plausibility to fuzzy sets used in an approximate reasoning rule base.

Acknowledgements

The use of a linguistic rule base for modeling the adversary is based on concepts from the Logic Evolved Decision (LED) methodology developed at Los Alamos National Laboratory (LANL) by Terry Bott and Steve Eisenhower, extended in this work to include belief/plausibility as the measure of uncertainty. The numerical model for the defender benefited from the work and suggestions of Jon Helton at Arizona State University.

The evaluation of belief/plausibility for fuzzy sets is based on the development of Ronald Yager at Iona College.

Scott Ferson of Applied Biomathematics provided suggestions and helpful reference material during the formulation of the concepts. The RAMAS RiskCalc software (version 4.0) developed by Ferson, et al., was used to check test case results of the BeliefConvolution code written by the author.

The author appreciates the careful review of this report by Jon Helton of Arizona State University and Mark Snell of Sandia National Laboratories as well as the preparation of the report for publication by Diane Ross of Sandia National Laboratories.

Contents

1	Introduction.....	11
1.1	Summary of Adversary/Defender Model.....	11
1.2	Report Organization.....	14
1.3	Summary of Belief/Plausibility and Fuzzy Sets	14
2	Nature of the Problem	16
2.1	The Adversary Perspective	16
2.2	The Defender Perspective	17
2.3	Optimization of the Design Basis Threat.....	18
2.4	Framework for Evaluating Adversary/Defender Objectives	20
2.4.1	The Adversary Model.....	20
2.4.2	The Defender Model	21
2.4.3	Benefits and Challenges of the Adversary/Defender Model.....	21
3	Belief and Fuzzy Sets	22
3.1	Simple Examples	22
3.1.1	Example of Total Ignorance	23
3.1.2	Example of Vagueness	25
3.1.3	Example Contrasting Aleatory and Epistemic Uncertainty	26
3.2	Belief and Numerical Convolution	27
3.3	Fuzzy Sets and Linguistic Convolution.....	32
4	Evaluation of a Scenario with the Defender Model	40
5	Evaluation of a Scenario with the Adversary Model.....	48
6	Assumptions, Areas for Future Work, and Conclusions	54
6.1	Assumptions.....	54
6.2	Areas for Future Work	54
6.3	Conclusions.....	56
	Appendix A. The Belief Measure of Uncertainty.....	57
	Appendix B. Probability and Uncertainty	83
	Appendix C. Evaluation of P_E with Belief/Plausibility	93
	Appendix D. Java Tools: Belief Convolution and Linguistic Belief.....	103
	Appendix E. Risk as Exceedance Frequency of Consequence.....	119
	Glossary	135
	References.....	137

Figures

Figure 1-1. Example Fuzzy Sets for Number of Deaths.....	15
Figure 2-1. Differences between Risk for Safety and Terrorist Problems.....	16
Figure 2-2. Optimization of Defender Resources.....	19
Figure 3-1. Likelihood Based on Information Available.....	24
Figure 3-2. Probability and Belief/Plausibility for Total Ignorance.....	24
Figure 3-3. Example of Vagueness.....	26
Figure 3-4. Intervals for Simple Example.....	30
Figure 3-5. Belief/Plausibility for Variable Z.....	32
Figure 3-6. Fuzzy Sets for Consequence (Deaths).....	33
Figure 3-7. Example Degrees of Evidence For Fear in the Populace.....	35
Figure 3-8. Quality of Life for John.....	38
Figure 3-9. Happiness for John.....	39
Figure 4-1. Degrees of Evidence (Probabilities) for P_E and C.....	41
Figure 4-2. Degrees of Evidence (Nested) for f_A	41
Figure 4-3. Exceedance Probability for Conditional Risk (Expected Consequence).....	42
Figure 4-4. Risk Exceedance Results using Belief/Plausibility and Probability.....	44
Figure 4-5. Expected Values with Belief and Probability.....	45
Figure 4-6. Ranking of Scenarios.....	45
Figure 4-7. Summary of Scenarios by Expected Values for Likelihood and Expected Consequence.....	46
Figure 4-8. Risk in Exceedance Frequency of Consequence Format for Example Problem.....	47
Figure 5-1. Results for Probability Of Success.....	51
Figure 5-2. Results for Consequence.....	52
Figure 5-3. Results for Expected Consequence.....	52

Tables

Table 3-1. Example Rule Base for <i>Overall Consequence (OC)</i>	35
Table 3-2. Rule Base for Quality of Life (QL).....	36
Table 3-3. Rule Base for Happiness (H).....	38
Table 5-1. Rule #1: Rule base for Expected Consequence (EC).....	49
Table 5-2. Rule #2: Rule base for Consequence (C).....	49
Table 5-3. Rule #3: Rule base for <i>Probability Of Success (PS)</i> with Varying Degrees of Probability that the Physical Security System can be Defeated.....	50

Acronyms

CCDF	complementary cumulative distribution function
CDP	Critical Detection Point
CR	conditional risk
DBT	design basis threat
DHS	Department of Homeland Security
DOE	Department of Energy
EC	expected consequences
LANL	Los Alamos National Laboratory
LDRD	Laboratory Directed Research and Development
LED	Logic Evolved Decision
NNSA	National Nuclear Security Administration
SNL	Sandia National Laboratories

This page intentionally left blank.

Executive Summary

This report documents an approach for evaluating the risk from acts of terrorism using an Adversary/Defender model developed in the Security Systems and Technology Center at Sandia National Laboratories in Albuquerque, NM. This work was developed and applied to support an evaluation of the security of nuclear materials storage sites for the National Nuclear Security Administration (NNSA) in the Department of Energy (DOE). Also, this work was incorporated into an evaluation of the effectiveness of cyber security systems for a Laboratory Directed Research and Development (LDRD) project. The work was performed between July 2005 and June 2006.

The purpose of this work was to apply innovative, non-probabilistic techniques to an overall evaluation of risk from acts of terrorism, including the likelihood of an attack. A terrorist attack is not a random event; it involves a specific scenario that is selected, planned, and implemented by the adversary. There is significant epistemic (state of knowledge) uncertainty for the defender as to the scenarios that the adversary will select. Conversely, the adversary has epistemic uncertainty as to the effectiveness of protective measures employed by the defender, including intelligence-gathering efforts to prevent scenarios from being implemented, security systems in place to defeat an attack, and the effectiveness of measures to mitigate consequences.

Traditional probabilistic risk analysis techniques — as applied to the evaluation of random, “dumb” events such as an earthquake — have difficulty modeling the risk from intentional acts by a malevolent, thinking adversary due to the inherently large epistemic uncertainty associated with intentional acts. The methodology developed in this report uses a more general measure of uncertainty than probability, specifically belief/plausibility from the Dempster/Shافر theory of evidence, to capture epistemic as well as aleatory (random) uncertainty. Probability is a special case of belief/plausibility. Also, fuzzy sets and approximate reasoning are used for a linguistic evaluation of the selection of scenarios by the adversary. In both the adversary and the defender models, uncertainty is captured and propagated using belief/plausibility.

The process of selecting scenarios from the perspective of the adversary involves a complicated consideration of many dependent factors. Unless all the factors of importance to the adversary are “good,” the adversary will discard a scenario and consider other scenarios. Instead of a detailed numerical evaluation, the adversary uses more of a “yes/no” decision process for such factors as:

1. Are the consequences of the type desired?
2. Are the potential consequences highly likely to be of sufficient magnitude?
3. Given the perceived magnitude of the consequences and the perceived level of protection, is it worth gathering the resources needed to have a high assurance of success?
4. What other scenarios require fewer resources and have acceptable consequences?

That is, the adversary selects scenarios that are highly likely to succeed and maximize consequences while making effective use of resources within the constraint of the pool of resources available. The adversary spends more effort in designing the scenario for a high likelihood of success rather than estimating a precise numerical value for the likelihood of success.

The use of a *linguistic model* for the adversary focuses the evaluation on developing the appropriate rule base for how the adversary thinks, rather than forcing a detailed numerical evaluation of variables where there is insufficient information to do so. The model also captures the significant epistemic uncertainty inherent in attempting to think like the adversary.

The *defender model* evaluates risk numerically as the product of three terms: frequency of an attack, probability that the attack (if implemented) is successful, and consequences of the attack if successful. The estimate for the frequency of an attack uses the results of the *adversary model*. The uncertainty in the frequency of an attack is best captured using belief/plausibility due to the large epistemic uncertainty associated with this term. If enough information is available, the uncertainty in the probability that the attack is successful and/or the uncertainty in the consequence of the attack can be modeled using a probability measure, although in general belief/plausibility can be used to capture uncertainty for these factors also.

Overall consequence, from the perspective of both the adversary and defender, can be a combination of several types of consequences, some difficult to evaluate numerically, such as: deaths, economic damage, fear in the populace, damage to national security, morale, and others. The linguistic model for the adversary is a natural language for considering the different consequences. In the rule base, all specific consequences can be assigned fuzzy sets and the rule base can be configured as desired to combine the specific consequences into fuzzy sets defined for Overall Consequence. For example, “Lots” of Fear in the Populace and “Minor” Number of Deaths can be mapped to “Moderate” Overall Consequence, and “Some” Fear in the Populace and “Major” Number of Deaths can be mapped to “Major” Overall Consequence. Again, it is the rule base that is important, not the detailed numerical values.

To compare different consequences numerically for the defender, a common measure for consequence can be used, Willingness to Pay, which is the dollar amount the defender is willing to pay to prevent a specific consequence from occurring.

Two Java codes were written by the author to automate convolution of numeric or linguistic variables using the belief/plausibility measure. The BeliefConvolution code performs convolution of random variables with evidence assigned to intervals of real numbers. The LinguisticBelief code performs convolution of linguistic variables using approximate reasoning with evidence assigned to fuzzy sets. BeliefConvolution implements evaluation for the defender model and LinguisticBelief implements evaluation for the adversary model.

In conclusion, this work documents an adversary/defender process for evaluating overall risk from acts of terrorism, including the considerable epistemic uncertainty in the evaluation.

1 Introduction

This report documents an approach for evaluating the risk from acts of terrorism using an Adversary/Defender model developed in the Security Systems and Technology Center at Sandia National Laboratories in Albuquerque, NM. This work (performed between July 2005 and June 2006) was developed and applied to support an evaluation of the security of nuclear materials storage sites for the National Nuclear Security Administration (NNSA) in the Department of Energy (DOE). Also, this work was incorporated into an evaluation of the effectiveness of cyber security systems for a Laboratory Directed Research and Development (LDRD) project.

The purpose of this work was to apply innovative, non-probabilistic techniques to an overall evaluation of risk from acts of terrorism, including the likelihood of an attack. A terrorist attack is not a random event; it involves a specific scenario that is selected, planned, and implemented by the adversary. There is significant epistemic (state of knowledge) uncertainty for the defender as to the scenarios that the adversary will select. Conversely, the adversary has epistemic uncertainty as to the effectiveness of protective measures employed by the defender, including intelligence-gathering efforts to prevent scenarios from being implemented, security systems in place to defeat an attack, and the effectiveness of measures to mitigate consequences.

The concept of using separate models for the adversary and defender has been suggested by a number of analysts, including Merkle at Sandia National Laboratories (SNL) and Darby, et al. at Los Alamos National Laboratory. [Merkle] [Darby, Bush, et al.]

A glossary at the end of this report provides practical definitions of terms such as “belief” and “fuzzy sets.” These terms have specific mathematical meanings provided in the main body and Appendix A of this report.

1.1 *Summary of Adversary/Defender Model*

The goal of the adversary in this model is to maximize the expected consequence while constrained by available resources, and the goal of the defender is to minimize risk while constrained by available resources. Expected consequence is defined as “consequence weighted by the likelihood that the scenario (if implemented) is successful.” Risk is the product of three terms: (1) the likelihood of an attack, (2) the probability that the attack is successful, and (3) the consequence(s) of the attack. The results of the adversary model provide information to the defender model as to the likelihood of an attack.

A scenario is defined as consisting of a specific target, adversary resources, and attack plan. Adversary resources include both attributes (equipment, weapons, numbers of attackers, etc.) and knowledge (details of target characteristics and protective measures, if any, for the target, etc.)

A terrorist attack is not a random event; it involves a specific scenario that is selected, planned, and implemented by the adversary. An intentional terrorist attack is significantly different from a random event. Consider the failure of a specific building in response to an earthquake, a random event. The risk from the earthquake considers the likelihood of the earthquake, the

response of the building to the earthquake, and the number of people likely to be killed if the building fails. The magnitude of the earthquake is independent of the fragility of the building. However, for an intentional terrorist attack against the building, the adversary estimates the resources required to destroy the building based on an evaluation of the fragility of the building, and decides if the potential consequences are worth the effort to bring the resources to bear necessary to destroy the building. The adversary has a choice as to which building to attack, the earthquake does not.

There is significant epistemic (state of knowledge) uncertainty for the defender as to the scenario(s) that the adversary will select. The adversary has epistemic uncertainty as to the effectiveness of protective measures employed by the defender, including intelligence-gathering efforts to prevent scenarios from being implemented, security systems in place to defeat an attack, and the effectiveness of measures to mitigate consequences.

Therefore, terrorist acts are intentional and an evaluation of them involves considerable epistemic uncertainty. Traditional probabilistic risk analysis techniques have difficulty modeling the risk from these acts due to the inherently large epistemic uncertainty. The methodology discussed in this report uses a more general measure of uncertainty than probability, specifically belief/plausibility from the Dempster/Shافر theory of evidence, to capture epistemic as well as aleatory (random) uncertainty.¹

The process of selecting scenarios from the perspective of the adversary involves a complicated consideration of many dependent factors. Unless all the factors of importance to the adversary are “good,” the adversary will discard a scenario and consider other scenarios. Instead of a detailed numerical evaluation, the adversary uses more of a “yes/no” decision process for such factors as:

1. Are the consequences of the type desired?
2. Are the potential consequences highly likely to be of sufficient magnitude?
3. Given the perceived magnitude of the consequences and the perceived level of protection, is it worth gathering the resources needed to have a high assurance of success?
4. What other scenarios require fewer resources and have acceptable consequences?

That is, the adversary selects scenarios that are highly likely to succeed and maximize consequences while making effective use of resources within the constraint of the pool of resources available. The adversary spends more effort in designing the scenario for a high likelihood of success rather than estimating a precise numerical value for the likelihood of success.²

¹ Probability is a special case of belief/plausibility, so for portions of the model dominated by aleatory uncertainty, such as consequence from a specific scenario, the belief/plausibility measure reduces to a probability measure.

² That is, the adversary is not concerned with the precise likelihood of each variable of concern, such as the probability of being detected being less than 0.01. They focus on “we believe we are not likely to be detected” where “not likely” is ill-defined (a fuzzy set) but is understood to

For example, a threat scenario that includes recruitment of an insider may be rejected by the adversary due to concern of discovery if the insider is not already a proven member of the adversary organization. Or, the adversary may discard a scenario that requires a large number of attackers and/or significant logistical support.

For these reasons, the *adversary model* uses an approximate reasoning rule base with linguistic variables. For example, a linguistic variable may be “Ease of Gathering Information on Target.” To allow for uncertainty, fuzzy sets are defined for each linguistic variable. For example, for the variable Ease of Gathering Information on Target, possible fuzzy sets could be: “Very Easy,” “Easy,” “Moderate,” and “Difficult.” To capture uncertainty, degrees of evidence are assigned to families of fuzzy sets. To combine linguistic variables a rule base is used; the rule base serves a function for convoluting the linguistic variables of concern. Uncertainty is propagated through the rule base using the mathematics of the belief/plausibility measure.

The use of a *linguistic model* for the adversary focuses the efforts of the modeler on developing the appropriate rule base for how the adversary thinks, rather than forcing a detailed numerical evaluation of variables where there is insufficient information to do so.

The *defender model* evaluates risk as the product of three terms: frequency of an attack, probability that the attack (if implemented) is successful, and consequences of the attack if successful. The uncertainty in the frequency of an attack is best captured using belief/plausibility due to the large epistemic uncertainty for the defender. If enough information is available, the uncertainty in the probability that the attack is successful and/or the uncertainty in the consequence of the attack can be modeled using a probability measure, although in general belief/plausibility can be used to capture uncertainty for these factors also.³

Overall consequence, from the perspective of both the adversary and defender, can be a combination of several types of consequences, some difficult to evaluate numerically, such as: deaths, economic damage, fear in the populace, damage to national security, morale, and others. The linguistic model for the adversary is a natural language for considering the different consequences. In the rule base all specific consequences can be assigned fuzzy sets and the rule base can be configured as desired to combine the specific consequences into fuzzy sets defined for Overall Consequence. For example, “Lots” of Fear in the Populace and “Minor” Number of Deaths can be mapped to “Moderate” Overall Consequence, and “Some” Fear in the Populace and “Major” Number of Deaths can be mapped to “Major” Overall Consequence. Again, it is the rule base that is important, not the detailed numerical values, and the focus of the adversary model is on a rule base that allows the defender to think like the adversary.

mean a low value (below on the order of 0.01). The decision is based on all variables of concern being acceptable to the adversary. The emphasis is on the variables of concern and how they interact rather than a precise numerical evaluation of these variables. Since the adversary has a choice, if all variables of concern are not acceptable for a particular scenario, the adversary will select another scenario.

³ Probability of success of the attack is a term in the risk equation. Probability is also a measure of uncertainty, and we can have a probability distribution that reflects uncertainty in the probability of success of the attack. These two meanings of probability are discussed in Appendix B.

To compare different consequences numerically for the defender, a common measure for consequence can be used, Willingness to Pay, which is the dollar amount the defender is willing to pay to prevent a specific consequence from occurring.

The problem of evaluating risk from acts of terrorism is too complex to be addressed purely academically. A proposed methodology must be applied to the real world and improved by experience gained in the application. To that end, to implement the model described in this report, simplifying assumptions have been made and software has been developed to implement the adversary and defender evaluations using these assumptions.

1.2 Report Organization

The organization of this report is as follows:

- Section 2 discusses the problem from the viewpoint of both the adversary and defender, and provides the framework for evaluating the objectives of each.
- Section 3 summarizes the concepts of belief and fuzzy sets.
- Section 4 discusses the numerical model for the defender.
- Section 5 discusses the linguistic model for the adversary. Note: The defender model is discussed before the adversary model because it is easier to first explain the use of belief for a numeric variable and then expand the explanation to belief for a linguistic variable.
- Section 6 discusses the major assumptions used in the models and areas for future work, and provides conclusions.
- Appendices provide supplementary information.

Sections 1, 2, and 5 make assumptions about the adversary behavior that are reasonable but not all of them may be true. These are “working” assumptions for starting the development of the adversary model and need to be checked and perhaps generalized in the future.

1.3 Summary of Belief/Plausibility and Fuzzy Sets

To consistently capture the epistemic (state of knowledge) uncertainty associated with the defender evaluating intentional acts by an adversary, the belief/plausibility measure of uncertainty from the Dempster/Shafer theory of evidence is used. This measure is discussed qualitatively in Section 3 and quantitatively in Appendix A. For a sample space S , degrees of evidence, m , are assigned to subsets (events) of S . The subsets with nonzero degrees of evidence are called focal elements. The belief and plausibility for any subset (event) in S is:

$$\begin{aligned} Bel(A) &= \sum_{B|B \subseteq A} m(B) \\ Pl(A) &= \sum_{B|A \cap B \neq \emptyset} m(B) \end{aligned} \quad (\text{Eqn. 1-1})$$

where A is any subset of S and B is a focal element of S .

If the focal elements are singletons (events containing only one element of the sample space), both belief and plausibility reduce to the standard probability measure of uncertainty. A belief/plausibility interval can be interpreted as a lower/upper bound on a probability. The utility of the belief/plausibility measure is that it provides a consistent treatment of epistemic uncertainty without additional assumptions when the available information is nonspecific.

A fuzzy set is a set whose elements can have partial membership. Fuzzy sets are discussed qualitatively in Section 3 and quantitatively in Appendix A. Figure 1-1 shows example fuzzy sets for the random variable “Number of Deaths.” We use fuzzy sets for categorizing events such as a “Moderate” Number of Deaths as linguistically meaning “Between about 50 and about 500 deaths,” with the numerical meaning given in Figure 1-1.

Figure 1-1. Example Fuzzy Sets for Number of Deaths

We also deal with fuzzy sets that are purely linguistic, such as the consequence “Fear in the Populace” with fuzzy sets “Little,” “Some,” and “Lots” for which no numerical definition in terms of degrees of membership is used.

Belief/plausibility can be applied to fuzzy sets as well as crisp sets [Yager 1986].

We use fuzzy sets for evaluating the selection of scenarios by the adversary. The fuzzy sets are chosen based on our need to make decisions (e.g., the degree to which we need to segregate a variable such as consequence or adversary intent), and a rule base is used to linguistically combine fuzzy sets for the variables of concern. Since we as a defender have to act as a surrogate adversary, there is considerable epistemic uncertainty in our model for the adversary, and we capture this uncertainty using belief/plausibility.

2 Nature of the Problem

This section discusses the nature of the problem of intentional acts of terrorism from the viewpoints of the adversary and the defender. Based on these viewpoints, objectives of both the adversary and defender are developed; specifically, the adversary strives to maximize expected consequence and the defender strives to minimize risk.

2.1 The Adversary Perspective

For safety-related problems that deal with random failures, the evaluation of risk must consider low-consequence but high-likelihood accidents since numerically these may dominate risk. However, the adversary will select scenarios that maximize the likelihood of achieving a selected high consequence constrained by the resources available to the adversary. That is, low-consequence scenarios are not likely since they will not be attempted by the adversary. Figure 2-1 illustrates this difference.

Figure 2-1. Differences between Risk for Safety and Terrorist Problems

The adversary chooses scenarios that require the minimum level of resources to achieve the desired consequence; however, as required, the adversary will spend the time and effort to gather the resources necessary to successfully attack a target of special interest. Therefore, once the adversary has decided on the desired consequences, the adversary will select the target for which the resources optimize the likelihood of successfully accomplishing those consequences. Once the “softest” target is selected that offers the potential for achieving those consequences, if the adversary decides that more resources are required to have a high likelihood of success, the

adversary will spend the time and effort necessary to gather the required resources rather than select a “softer” target that does not meet the criteria for consequences.

The adversary will initially consider a large number of potential scenarios, but will ultimately select a limited number of scenarios for detailed evaluation. In this report, the author assumes that the adversary attempts to maximize the expected consequence, defined as consequence weighted by the likelihood that the scenario (if implemented) is successful.

Selection of a scenario by the adversary depends on an assessment of the difficulty in gathering the minimum resources perceived as necessary for success. The gathering of the required resources by the adversary is constrained by organization (membership, funding, etc.) and by concern that the more complex the required resources and the longer the time required to gather them, the higher the likelihood that the adversary will be discovered by intelligence-gathering efforts before an attack can be attempted.

The adversary attacks specific targets, such as buildings, but the targets are chosen such that the consequences are far greater than those due to loss of the specific targets. That is, the targets are “local,” but the consequences are “global.”

2.2 *The Defender Perspective*

The defender minimizes the risk from acts of terrorism by optimizing the allocation of available resources over all possible scenarios of concern. The defender does not know which scenarios the adversary may select. Therefore, for the defender, all scenarios must be considered.

Both the adversary and defender are constrained by available resources, but their use of resources is different. The adversary focuses resources on a few precisely known scenarios while the defender must allocate resources to address all scenarios.

The defender can minimize risk by minimizing the likelihood of attack and/or success given an attack. In the past, much of the protection of high-consequence targets, such as nuclear weapons sites, has focused on minimizing adversary success, by defining a design basis threat (DBT) and designing a security system to stop success, given an attack within the confines of that threat. However, the resources used by the adversary are escalating and it is difficult to justify ever-increasing expenditures on security systems to counter an increasing DBT without also addressing the effectiveness of techniques to minimize the likelihood of an attack. Also, many infrastructure targets in the commercial sector of interest to the adversary have no DBT and little physical security in place. Since the adversary has a choice of scenarios, they may select a target with lower consequence that is less protected.

Much of the effort in the United States since 9-11 has focused on minimizing the likelihood of an attack by using stricter laws and intelligence-gathering efforts to stop the planning and resource-gathering phases of scenarios before they are implemented. The defender model for risk should consider the effectiveness of such intelligence-gathering efforts. Given the large epistemic uncertainty inherent in evaluating the effectiveness of these measures, a probability measure of

uncertainty is not the best choice; a belief/plausibility measure is a good choice for capturing the uncertainty.

For targets with a high level of security, the presence of the security increases the amount of resources required by the adversary to succeed, thereby affording the defender more time to detect the gathering of such resources.

The defender can also minimize risk by reducing consequence. Measures to reduce consequence are measures taken if the adversary is successful and include emergency response, contingency, or mitigative measures. The mitigative measures must be developed before the consequence occurs in order to be implemented in a timely fashion given the consequence.

To better estimate risk, the defender should consider the effectiveness of measures to reduce the likelihood of an attack and the effectiveness of measures to mitigate the consequences of a successful attack as well as the effectiveness of security systems to defeat an attack. Although more difficult to evaluate due to uncertainty, the effectiveness of measures for reducing the likelihood of an attack may be less sensitive to changes in the resources available to an adversary than physical security system elements.

2.3 Optimization of the Design Basis Threat

For targets where the concept of a DBT is used, consideration of the likelihood of an attack can be used to optimize the specification of the DBT.

Regulatory bodies establish the DBT for a set of facilities of concern, such as nuclear weapons sites or nuclear reactors. The details of the DBT are classified. The DBT specifies the adversary resources to be countered by the security system. The facility is expected to prevent success of a terrorist act given an attack where the adversary has resources within the DBT. With the level of threat that exists, escalating the DBT to require that all facilities prevent the adversary's success may not be cost effective, given an attack by an adversary with extensive yet credible resources.

The cost of protecting all facilities to prevent the success of such a threat may be prohibitive in terms of dollars and the effect on facility operations. The effectiveness of measures for preventing an attack with such "high resources" should be considered; that is, measures to prevent an attack where the adversary has resources beyond the DBT should be considered.

The likelihood of an attack is influenced by the resources perceived by the adversary necessary for a high likelihood of success. The greater the required resources, the less the likelihood of an attack for two reasons:

1. The adversary may determine that it is too costly and/or time consuming to gather the required resources.
2. The defender has a higher likelihood of detecting the gathering of the required resources as they increase in complexity and/or require more time to gather.

An evaluation of the probability of success of an attack must consider the adversary resources. An attack made with resources within the DBT may not succeed. Since the DBT specifies the adversary resources that the facility is designed to defeat, the adversary needs to have resources in excess of those commensurate with the DBT to have a very high likelihood of success. So, the DBT sets a threshold for where the defender should direct efforts for detecting the gathering of adversary resources. For adversary resources below those commensurate with the DBT, the defender should focus efforts on providing protection at the facilities to prevent adversary success given an attack; this is the current strategy. For adversary resources above the DBT, the defender should focus resources on detecting the adversary attempting to gather those resources. Figure 2-2 shows conceptually how the adversary resources specified by the DBT can be used to segregate the application of defender resources between preventing success and preventing attack.

Figure 2-2. Optimization of Defender Resources

For a fixed set of defender resources, there is an optimum specification of the DBT for which the defender can optimize the reduction in risk. The optimum DBT meets the following requirements:

- Set sufficiently high such that the resources required by the adversary for success have a high likelihood of being detected before an attack can be made.

- Set sufficiently low such that it is not prohibitive to provide protection at the facilities of concern to prevent success given an attack by an adversary using resources within the DBT.

2.4 *Framework for Evaluating Adversary/Defender Objectives*

The goal of the adversary is to maximize the expected consequence while constrained by available resources. The goal of the defender is to minimize risk while constrained by available resources.

2.4.1 *The Adversary Model*

A scenario was defined in Section 1 as follows; a specific target, adversary resources, and attack plan. Adversary resources include both attributes (equipment, weapons, numbers of attackers etc.) and knowledge (details of target characteristics and protective measures, if any, for the target, etc.).

It is assumed that the goal of the adversary is to select a set of scenarios that maximize expected consequence subject to the constraint of the resources available to the adversary.

For a scenario, effective consequence is defined as the consequence perceived by the adversary weighted by the adversary estimate of the likelihood that the security system can be defeated using the scenario (the adversary estimate of the likelihood that the consequence can be achieved). For a single scenario, the (overall) consequence can be a combination of a variety of specific consequences, such as deaths, economic damage, fear in the populace, damage to national security, etc. The adversary model must combine the different specific consequences into an overall consequence.

Conceptually, the adversary model is:

$$\max(\overset{\leftrightarrow}{EC}_A) | \text{Adversary Resources} \quad (\text{Eqn. 2-1})$$

where $\overset{\leftrightarrow}{EC}_A$ is a complex combination of expected consequences (EC) estimated by the adversary (A) for each possible scenario. For the adversary, maximizing expected consequence is constrained by the adversary resources. We as a defender think like the adversary in order to estimate expected consequences, and our evaluation must consider the large epistemic uncertainty inherent in this process.

Section 5 presents the adversary model for a specific scenario. The process for considering all scenarios in the context of Equation 2-1 is an area of current investigation, and such a process will involve binning and screening of the huge number of potential scenarios.

2.4.2 The Defender Model

The goal of the defender is to minimize risk over the set of all scenarios, given the resources available to the defender. Conceptually, the defender model is:

$$\min(\overset{\leftrightarrow}{R}_D) | \text{Defender Resources} \quad (\text{Eqn. 2-2})$$

where $\overset{\leftrightarrow}{R}_D$ is a complex combination of risk (R) estimated by the defender (D) for each possible scenario. For the defender, minimizing risk is constrained by the defender resources.

Risk for each scenario is the product of three terms: (1) the likelihood that the scenario is selected by the adversary, (2) the probability that the attack is successful, and (3) the consequence(s) of the attack. Each term has uncertainty that must be considered. The likelihood of the scenario has considerable epistemic uncertainty, since it is estimated using information from the adversary model in which the defender attempts to think like the adversary.

Section 4 presents the defender model for a specific scenario. The process for considering all scenarios in the context of Equation 2-2 is an area of current investigation, and such a process will involve binning and screening of the huge number of potential scenarios.

2.4.3 Benefits and Challenges of the Adversary/Defender Model

By segregating the evaluation into two players, adversary and defender, the approach allows the different objectives of each to be explicitly considered. Also, the segregation allows for explicit consideration of the different states of knowledge of the adversary and the defender. Finally, this model allows different evaluation criteria to be used for the adversary and the defender; specifically, a linguistic evaluation for the adversary for maximizing expected consequence, and a numerical evaluation for the defender for minimizing risk.

Since the adversary has a choice of scenarios, the number of scenarios in Equations 2-1 and 2-2 is very large. Due to the significant uncertainty present for both adversary and defender, each variable for each scenario should be modeled as a range of values and the equations should be solved by convoluting measures of uncertainty for each variable. The belief measure has been selected as the measure of uncertainty to consistently include epistemic uncertainty. Solving Equations 2-1 and 2-2 for all the scenarios using a belief/plausibility measure for all the variables for each scenario is a formidable task. Due to this complexity, in application it will be necessary to lump scenarios into classes of scenarios and use screening criteria during the evaluation. The process for creating classes of scenarios and the development of screening criteria will be developed during application of the method to real-world problems.

The remainder of this report focuses on evaluating expected consequence and risk for a specific scenario (or a specific class of scenarios) from the viewpoint of the adversary and defender, respectively.

3 Belief and Fuzzy Sets

This section provides a practical explanation of: (1) belief/plausibility as a measure of a type of uncertainty called ambiguity, and (2) fuzzy sets as a measure of a type of uncertainty called vagueness. Belief/plausibility can be extended to address fuzzy sets. Appendix A provides a summary discussion of the mathematics of belief/plausibility and fuzzy sets. The glossary contains practical definitions of terms that are defined mathematically in the report.

3.1 Simple Examples

The use of belief/plausibility and fuzzy sets in this report is based on developments – mostly since the 1960s – in the understanding of uncertainty and in the mathematical models that implement this understanding. When first encountering these concepts, the reader is left with somewhat of an understanding of the mathematics of the techniques, but with little physical insight into the applicability of the techniques. The situation is analogous to reading a book on the theory of probability without having the experience of applying probability measures to real-world problems. To assist in the physical understanding of these concepts, the following discussion is provided.

The belief measure of uncertainty is a generalization of the probability measure of uncertainty. When the uncertainty is of a certain type called strife (which is related to aleatory or stochastic uncertainty), belief becomes probability. However many real-world problems have uncertainty of the type called nonspecificity (which is related to epistemic or state-of-knowledge uncertainty) for which the fidelity of the information available is insufficient to justify a probability metric for uncertainty.

For a variable of interest, the sample space, sometimes called the universe of discourse, is the set of all unique outcomes for the variable. A subset of the sample space is called an event, and an element of the sample space is called an elementary event. Elementary events, being unique, are mutually exclusive or disjoint. Events, in general, are not mutually exclusive. Both probability theory and belief theory assign likelihood to events in the sample space. [Helton et al. 2004]

Probability theory has certain restrictive properties that are not required in belief theory. Probability has the “additive property,” which states that the probability of any sequence of disjoint events is the sum of the probability of the events. Thus, for a discrete sample space, the probability of an event is the sum of the probability of the elementary events that comprise that event. For a continuous sample space (some interval of all real numbers) the probability of an event is the integral of the probability density function over the interval corresponding to the event. Probability theory has the property that the sum of the probability of an event and the probability of the complement of the event is 1.0, where the complement of an event is the set of all elementary events in the sample space that are not part of the event.

In many applications of probability, the likelihood of each element of the sample space is provided or assumed; that is, a probability density is used and using the probability density, the probability of any event can be calculated. If the information available is not specific enough to provide a probability density, then an assumption must be made as to the probability density to be

able to calculate the probability of any event. However, the assumption for generating the probability density may not be warranted by the “fidelity” of the information available.⁴ Thus, for nonspecific information the use of probability is not fully justified. With its less restrictive properties, belief/plausibility can be used to estimate the likelihood of events when the information is not specific enough to provide a probability density.

3.1.1 Example of Total Ignorance

Consider a problem where a missing report is known to be in one of a set of 35 boxes in an office. The sample space for this problem is $S = \{b_1, b_2, \dots, b_{35}\}$ where b represents a box. This is an example of “total ignorance” since all we know is that the event of interest – the box containing the report – is somewhere within the sample space.

Both probability and belief measures assign a likelihood of 1.0 to the event consisting of the entire sample space since it is known that the report is in a box in S . However, to estimate the probability that the report is in a particular box, an assumption about the probability density must be made. With no more information, there is total ignorance as to how to assign the probability measure to each box; an assumption must be made about the probability of the report being in each box and the sum of the probability over all boxes must be 1.0; a typical assumption is that the report is equally likely to be in any box so each box is assigned a probability of $1/35$, or 0.0286. But this approach requires an assumption beyond that provided by the evidence.

A more general measure of likelihood is based solely on the information that the report is somewhere in the entire set of 35 boxes; a dual measure of likelihood, plausibility/belief, is appropriate.⁵ It is plausible that the report is in any box, but we have no belief that the report is in any box. With the belief/plausibility metric, the likelihood that the report is in any box is specified by a belief of 0 and a plausibility of 1.0; that is, the belief that the report is in any box is 0 (since we have no information other than the report is in some box) and the plausibility of the report being in any box is 1.0 since it could be in any box.

Figures 3-1 and 3-2 illustrate this example of total ignorance.

⁴ To be more precise, the information available has uncertainty of the type called nonspecificity which cannot easily be addressed using a probability measure. Refer to Appendix A.

⁵ For this example, belief/plausibility reduce to necessity/possibility, respectively, because there is only one focal element. Refer to Appendix A.

Figure 3-1. Likelihood Based on Information Available

Probability for each Box

Belief / Plausibility for each Box

Figure 3-2. Probability and Belief/Plausibility for Total Ignorance

The type of uncertainty discussed in this example is called ambiguity. Ambiguity is the uncertainty associated with the likelihood that a particular event will occur.

3.1.2 Example of Vagueness

Vagueness is a type of uncertainty not addressed by probability. Vagueness addresses uncertainty as to how we categorize a known outcome. The example in Section 3.1.1 dealt with a type of uncertainty called ambiguity, which is uncertainty about the value of a random variable. Ambiguity allows us to consider the uncertainty associated with the likelihood of an event in the future. Once the event has occurred, we may have uncertainty as to how to categorize the event and this type of uncertainty is called vagueness. [Klir and Yuan]

For example, assume we know with certainty which box the report is in and we are asked whether or not that box is toward the center of the room. “Boxes toward the center of the room” is a subset (event) of the sample space for all boxes, but there is uncertainty (vagueness) as to the degree of membership of some of the boxes in the subset of interest. Boxes in the corners of the room are not members of the subset “Boxes toward the center of the room,” and boxes in the center of the room are members of the subset “Boxes toward the center of the room.” But boxes neither in the corners nor in the center are “sort of in the center of the room” and thus have partial membership in the subset “Boxes toward the center of the room,” where the membership increases from 0 to 1 as the box location progresses from a corner toward the center. Sets containing members with partial membership are called fuzzy sets, and the mathematics of fuzzy sets can be used to model uncertainty due to vagueness. If the box known to contain the report is not in the corners or in the middle, it is vague as to whether or not that box is toward the center of the room, and that vagueness is indicated by the assignment of partial membership of that box in the fuzzy subset “Boxes toward the center of the room.”

For example, suppose the report is known to be in box #6 where the location of box #6 in the room is indicated in Figure 3-3. Assume that a degree of membership of 0.8 can be assigned to box #6 in the fuzzy set “Boxes toward the center of the room”. That fuzzy set can be expressed as $\{0/\text{box}\#1, \dots, 0.8/\text{box}\#6, \dots, 1/\text{box}\#34, \dots\}$ where $\mu_F(s)/s$ indicates that element s in sample space S has a degree of membership $\mu_F(s)$ in a fuzzy set F defined on S .

Figure 3-3. Example of Vagueness

It is possible to combine measures of ambiguity and vagueness to develop belief/plausibility measures for fuzzy sets, as discussed in Appendix A.

3.1.3 Example Contrasting Aleatory and Epistemic Uncertainty

Consider drawing a marble from a bag, using probability to represent uncertainty. Assume we know that the bag has two marbles, one red and one blue. Let the random variable of interest, X , be the number of red marbles selected when one marble is pulled from the bag. The sample space for the random variable X is $\{0, 1\}$. For this situation, the uncertainty of selecting a red marble is purely aleatory, and $P(X = 0)$ is $1/2$ and $P(X = 1)$ is $1/2$ where P denotes probability. The uncertainty cannot be reduced by having more information; this is characteristic of a problem with purely aleatory uncertainty.

Now consider a different situation for which we have less information. Assume the bag may have either two red marbles, or both a red and blue marble, but the bag does not contain two blue marbles. As before the random variable of interest, X , is the number of red marbles selected when one marble is pulled from the bag. This situation involves epistemic uncertainty as well as aleatory uncertainty. With no more information, we **assume** equal probabilities for the two cases; the probability the bag contains two red marbles is $1/2$, and the probability the bag contains a red and a blue marble is $1/2$. So, $P(X = 0) = 1/2 * 1/2 = 1/4$. $P(X = 1) = 1/2 * 1 + 1/2 * 1/2 = 3/4$.

Epistemic uncertainty can be reduced with more information. Assume we do two trials, **with replacement**, and draw a red marble both times; this indicates the bag may have two red marbles but two trials is not much information. We choose to assign $P(X = 1) = 5/8$ and $P(X = 0) = 3/8$.⁶

Assume we do two trials, **with replacement**, and draw a blue marble at least once; our epistemic uncertainty as to the contents of the bag is eliminated since we know that the bag must contain both a red and a blue marble. We assign a $P(X = 1) = 1/2$ and $P(X = 0) = 1/2$.

Suppose we are unable to reduce the epistemic uncertainty; that is, we cannot perform any trials. All we know is that the bag may have either two red marbles, or both a red and blue marble, but not two blue marbles. The sample space for X is $\{0, 1\}$ and we assign evidence of 1.0 to $\{0, 1\}$. Using the properties of belief/plausibility, $\text{Bel}(X = 1) = 0$ and $\text{Pl}(X = 1) = 1$ where Bel and Pl denote belief and plausibility, respectively. We have insufficient information to know the probability that $X = 1$; based on the evidence all we can say is that the probability that $X = 1$ is somewhere between 0 and 1. The belief/plausibility interval contains the forced probability point estimate of $3/4$ that we made earlier by assuming equal likelihood for (red, red) and (red, blue). We have insufficient information to know the true probability, all we can say is that the probability is somewhere within the belief/plausibility interval.

Assume we do two trials, **with replacement**, and draw a red marble both times; this indicates the bag may have two red marbles. Based on this information, for X we chose to assign evidence of 0.5 to $\{0, 1\}$ and 0.5 to $\{1\}$.⁷ This results in a Bel/Pl interval of 0/0.5 for the value 0 (no red marble selected) and a Bel/Pl interval of 0.5/1.0 for the value 1 (one red marble selected). The belief/plausibility measure has more uncertainty than the probability measure since the result is a belief/plausibility interval for the likelihood of a value for X instead of a point estimate probability. The belief/plausibility intervals contain the probability point estimates that we made earlier: $P(X = 0) = 3/8$ and $P(X = 1) = 5/8$.

3.2 *Belief and Numerical Convolution*

Consider a random variable X that has uncertainty. The uncertainty in the random variable X can be represented by a probability measure which in practice requires an estimate of the likelihood (probability) for each possible value x in X (if X is discrete) or the assignment of a probability density function if X is continuous. The state of knowledge may be insufficient to allow a probability to be specified over the values of X as indicated in the examples of Section 3.1.

For the evaluation of terrorist risk, our state of knowledge is insufficient to justify the use of probability as a measure of uncertainty. For example, we need to evaluate the frequency of an attack for a specific scenario, which is highly uncertain. Consider the random variable X to be the frequency of an attack (number of attacks per year) for the scenario.⁸ For the purposes of

⁶ A Bayesian update could be performed to update an assumed prior probability distribution with the evidence from the trials.

⁷ A mechanistic process for updating the assignment of degrees of evidence given more information is a subject of current research.

⁸ Section 4 discusses why the “initiating event”, defined here as an attack by the adversary against a specific target, is modeled as a frequency.

this discussion, the range for the frequency of attack for a specific scenario is taken to be $[0, 10]$ per year since 10 per year is a reasonable upper limit that has a low likelihood of occurrence.^{9,10} As a defender, we have considerable epistemic uncertainty as to the likelihood the adversary will select a specific scenario; we consider that uncertainty by assigning a likelihood measure over the values of X .

For terrorists' targets in the United States, the evidence is that approximately one attack occurs per year and there are on the order of a million potential targets, so without additional information, using probability as our measure of uncertainty, our expected value for X is on the order of 10^{-6} per year. However, a point estimate is insufficient as our knowledge about X is highly uncertain, so we wish to develop a probability distribution function over the range of X , $[0, 10]$ with a mean of 10^{-6} . We chose to assume a uniform distribution for X over the interval $[0, 2 \times 10^{-6}]$, for which the probability density is 5×10^5 and the mean is 10^{-6} . However, we have made an assumption (the probability density function) not warranted by the evidence, and that assumption results in failure to retain the uncertainty inherent in the information we have. For example, with our assumed probability density, we calculate a probability of 0.5 that X is between $[0, 10^{-6}]$. We could just as well have assumed another probability density, a triangular distribution for example, and we would obtain a different probability that X is between $[0, 10^{-6}]$. We could select a number of specific probability density functions, and therefore, an infinite number of estimates exist for the probability that X is between $[0, 10^{-6}]$. The problem is that we have failed to account for all our uncertainty by forcing the selection of a probability density function; but, using probability as our measure of uncertainty we are forced to do.

The information we have is too nonspecific to justify the use of probability as the measure of uncertainty.

With the more general measure of belief/plausibility, our treatment of uncertainty can be true to the nonspecificity of the information we have. We assign a degree of evidence of 1.0 to the interval $[0, 2 \times 10^{-6}]$ per year, which produces a belief/plausibility distribution as follows:

- a belief/plausibility of 1.0/1.0 to $[0, 2 \times 10^{-6}]$ or any interval containing $[0, 2 \times 10^{-6}]$, such as $[0, 10^{-5}]$,
- a belief/plausibility of 0/1.0 to any interval within $[0, 2 \times 10^{-6}]$, such as $[0, 10^{-6}]$, and
- a belief/plausibility of 0/0 to any interval that is disjoint with $[0, 2 \times 10^{-6}]$, such as $[3 \times 10^{-6}, 10^{-5}]$.

For the interval $[0, 10^{-6}]$ we have a belief/plausibility interval of 0/1.0; we have little belief (zero) that the frequency of attack will be in this interval but a high plausibility (one) that the frequency of attack could be in this interval. This belief/plausibility uncertainty interval reflects the large uncertainty inherent in the information available to us.

⁹ Using standard interval symbols, “[” means include and “(” means exclude. For example, $[a, b]$ denotes all real numbers between a and b including a and b . $(a, b]$ denotes all real numbers between a and b excluding a and including b .

¹⁰ For some scenarios, such as attacks against the U.S. military in Iraq, the upper limit may be greater than 10 attacks per year, and in such cases the upper limit is increased.

If more information for our target of concern becomes available, we can refine our assignment of degrees of evidence. For example, if intelligence information indicates that our target is more attractive than a “generic” target we may assign evidence to the frequency of attack as follows: evidence of 0.3 to $[0, 2 \times 10^{-6}]$ per year and evidence of 0.7 to $[0, 10^{-3}]$ per year. The broad intervals to which evidence is assigned reflect our uncertainty, but as more information becomes available we can refine our estimates by generating more evidence for more intervals. However, we will never have information specific enough to assign a probability distribution to the frequency of attack.

Consider a combination of random variables. For example, consider the combination of two random variables X and Y represented as $X \times Y$.¹¹ The $\times$ symbol used here is not multiplication but represents the sample space formed by the Cartesian product of two variables. $X \times Y$ represents the combination of the variables.¹² A combination of random variables is called a random vector. We are interested in propagating measures of uncertainty for each constituent random variable into a measure of uncertainty of the resulting random vector for a mathematical combination on the variables, usually an algebraic combination such as addition or multiplication. This process of propagating uncertainty is called convolution.

For our application, the defender model is concerned with estimating risk, which involves convoluting the likelihood of attack with the likelihood of adversary success with the magnitude of consequence for each threat scenario. Each of these factors may in turn be a convolution of other factors, such a consequence being a combination of a number of types of consequence, as previously discussed, or the effectiveness of the security system being a combination of different elements of the security system. (See Appendix C.)

To perform the convolution for random variables (real numbers) we must define the function of interest $f(X, Y)$ representing how we wish to combine specific values for X and Y ; for example, we may wish to add X and Y , $X + Y$, or multiply X and Y , $X \cdot Y$. For example, for risk the function is multiplication of the three random variables in the risk equation, and for consequence (in terms of constituent-specific consequences) the function is addition.

Just as there is a mathematical process for convoluting probability measures of uncertainty there is a mathematical process for convoluting belief/plausibility measures of uncertainty.

A simple example of convolution with belief/plausibility follows. Consider two independent random variables X and Y to be added to form $Z = X + Y$. For any given specific values of X and Y , x and y , Z has a specific value $z = x + y$.

If X and Y have no uncertainty, then both X and Y have one value, x_1 and y_1 , and Z has the one value $z_1 = x_1 + y_1$, and there is no uncertainty for Z .

¹¹ To be precise, X is the range for its corresponding random variable, as discussed in Section B.4.

¹² For example, if x is an element of X and y is an element of Y , $X \times Y = \{ \langle x, y \rangle \mid x \text{ in } X \text{ and } y \text{ in } Y \}$ where $\langle \rangle$ denotes a tuple.

If X and Y have uncertainty and the information about X and Y is specific enough to use probability as the measure of uncertainty, then the uncertainty in Z resulting from addition of all the possible values of X and Y is a probability calculated by convoluting the probability distributions for X and Y under addition to produce a probability distribution for Z.

If the information about X and Y is too nonspecific to use probability as the measure of uncertainty, then the more general measure of uncertainty called belief can be used. Instead of assigning a measure of uncertainty to values of X and Y (as done with probability), belief allows a measure of uncertainty to be assigned to intervals over X and Y. For example, let X range from 0 to 100 and let the degrees of evidence be as follows:

0.20 for the interval [0, 10]
 0.35 for the interval [2, 25]
 0.45 for the interval [82, 100]

The belief/plausibility for exceeding a given value can be easily evaluated using Equation 1-1. Let x be the value to be exceeded. The plausibility for exceeding x is the sum of all degrees of evidence for which the associated interval has *any* overlap with the interval (x, 100]. The belief for exceeding x is the sum of all degrees of evidence for which the associated interval lies (completely) within (x, 100]. For example, let x be 15; the interval of interest is (15, 100]. Figure 3-4 illustrates the situation.

Figure 3-4. Intervals for Simple Example

Both [2, 25] and [82, 100] overlap (15, 100] so the plausibility for (15, 100] is $0.35 + 0.45 = 0.8$. [82, 100] is the only interval that lies within (15, 100] so the belief for (15, 100] is 0.45.

The interval calculation is more complex for convolution, but is straightforward for convolution involving simple functions such as addition or multiplication of two constituent variables. The degrees of evidence for the result are calculated by forming the relation consisting of all 2-tuples with the first element of the tuple an interval with a non-zero degree of evidence from the first variable and the second element of the tuple an interval with a non-zero degree of evidence from the second variable. The degree of evidence for each tuple is the product of the two degrees of evidence for each element in the tuple assuming noninteraction.¹³ An interval for the convoluted

¹³ Noninteraction, as used here, is a generalization of probabilistic independence as discussed in Appendix A.

result is obtained by applying the appropriate function (e.g., addition or multiplication) to the intervals in the tuple. This convolution process is illustrated in the following example.

For example let X range from 1 to 20 with the following degrees of evidence and intervals:

0.8 for [2, 15]
0.2 for [1, 10]

Let Y range from 0 to 30 with the following degrees of evidence and intervals:

0.7 for [5, 25]
0.3 for [0, 4]

The random vector $X \times Y$ has the following degrees of evidence for the indicated tuples:

$0.8 \cdot 0.7$ for $\langle [2, 15], [5, 25] \rangle$
 $0.8 \cdot 0.3$ for $\langle [2, 15], [0, 4] \rangle$
 $0.2 \cdot 0.7$ for $\langle [1, 10], [5, 25] \rangle$
 $0.2 \cdot 0.3$ for $\langle [1, 10], [0, 4] \rangle$

Let $Z = X + Y$; Z ranges from 1 to 50. Since the function is addition, Z has the following degrees of evidence for the indicated intervals, using interval addition:

0.56 for [7, 40]
0.24 for [2, 19]
0.14 for [6, 35]
0.06 for [1, 14]

The likelihood of exceedance for Z is shown in Figure 3-5. Also, Figure 3-5 shows the expected value interval for Z.¹⁴

(Had X and Y been modeled using probability, belief and plausibility both become probability and the expected value interval is a point value, the mean. For this case, Figure 3-5 would have one curve, probability, and a point estimate expected value, the mean of the probability distribution.)

¹⁴ The expected value interval is a generalization of the probabilistic mean as discussed in Appendix A.

Figure 3-5. Belief/Plausibility for Variable Z

The author automated the numerical convolution of non-interacting random variables for algebraic functions in a Java computer code called BeliefConvolution. This code is discussed in Appendix D of this report.

A commercially available code, RAMAS Risk Calc, performs convolution of algebraic functions using probability, fuzzy arithmetic, and probability boxes [RAMAS Risk Calc]. The RAMAS RiskCalc software with user's manual is available at low cost; see <http://www.ramas.com/riskcalc.htm>. This is an excellent tool and is highly recommended.

Probability boxes can be used to model belief. [Ferson, Probability Boxes] RAMAS RiskCalc was used to check the results of BeliefConvolution.

3.3 Fuzzy Sets and Linguistic Convolution

The rule-based approach described here is the rule-based approach developed as part of the Logic Evolved Decision (LED) methodology at Los Alamos National Laboratory (LANL), extended in this work to use belief/plausibility as the measure of uncertainty. This rule-based approach is used for the adversary model as discussed later in Section 5. The rationale for using a linguistic approach for the adversary was discussed in Section 1.

Consider a random variable “the number of deaths from a terrorist attack on Albuquerque.” which has the domain $[0, 6 \times 10^5]$ since the population of Albuquerque is about 600,000. For estimating the consequences from a particular scenario we reason at a higher level than the specific number of deaths for two reasons: (1) there is too much uncertainty to distinguish between say 1000 and 2000 deaths, and (2) when comparing scenarios with widely different

consequences, such as blowing up a building to detonating a nuclear device, we have orders of magnitude differences in the consequences. We chose a partition over the range as follows: $[0, 50)$, $[50, 500)$, $[500, 5000)$, $[>= 5000]$. We have defined sets, subsets of the range, at the fidelity to which we wish to reason. We also assign names to these sets: “Minor” for $[0, 50)$, “Moderate” for $[50, 500)$, “Major” for $[500, 5000)$, and “Catastrophic” for $[>= 5000]$. We have assigned a linguistic (name) to the sets of interest commensurate with the level to which we wish to consider consequences. These sets of interest are crisp sets. However, there is a problem with our crisp sets. If 4999 people die, the consequence is “Major” but if 5000 people die, the consequence is “Catastrophic”; although the crisp sets solve the problem of reasoning at too fine a level they suffer from the problem of sharp boundaries. We really want to consider 4999 deaths as some of both major and catastrophic to a certain degree, and we can do so by making our sets fuzzy; specifically we define “Minor” as “up to *about* 50,” “moderate” as “between *about* 50 and *about* 500,” “Major” for “between *about* 500 and *about* 5000,” and “Catastrophic” for “greater than *about* 5000.” Degrees of membership can be assigned to these fuzzy sets as indicated in Figure 3-6.

Figure 3-6. Fuzzy Sets for Consequence (Deaths)

Given degrees of evidence assigned to crisp intervals in the range for deaths, such as 0.7 for $[10, 1000]$ and 0.3 assigned to $[1, 50,000]$, we can calculate the belief/plausibility for any fuzzy set given the fuzzy set defined in terms of degree of membership as in Figure 3-6. Section D.1.2 of Appendix D summarizes how the BeliefConvolution code implements calculation of belief/plausibility for fuzzy sets given crisp evidence.

We can also calculate belief/plausibility for any fuzzy set given evidence assigned to other fuzzy sets if we have the fuzzy sets defined in terms of degree of membership. Sections A.2.7 and A.3.5 summarize the details.

We are also concerned with consequences other than deaths, since we must think like the adversary and we know that the adversary considers many types of consequences in the process of selecting scenarios. We are concerned with economic loss in dollars (\$), so we can assign fuzzy sets to consequence in \$ and give a definition of the fuzzy sets in terms of degree of membership similar to the example in Figure 3-6. However, we are also concerned with consequences that are not easy to quantify as a number, such as Damage to National Security, and Fear in the Populace. For these consequences we can define fuzzy sets purely linguistically, such as “Insignificant,” “Significant,” and “Very Significant” for Damage to National Security, and “Little,” “Some,” and “Lots” for Fear in the Populace.

In concept, we could force a numerical definition of all fuzzy sets for all consequences. For example we could force a numerical definition for Damage to National Security over an interval $[0, x]$ where “ x ” is a real number, and we could develop degrees of evidence for each fuzzy set “Insignificant,” “Significant,” and “Very Significant” similar to the example in Figure 3-6. However, we have the problem of defining “ x ” to be consistent with the upper value of **all** the other consequences, such as Deaths and Fear in the Populace. Also, the subject matter experts do not always think numerically; for example, they may consider a “Significant” Damage to National Security as equivalent to a “Major” number of Deaths regardless of any forced numerical definition of “Significant.” For these reasons, we need a technique that does not require a numerical definition for the fuzzy sets.

To consider likelihood that an adversary will choose selected scenarios, we need to combine the different types of consequences (Deaths, \$, Damage to National Security, Fear in the Populace, etc.) into an overall consequence. Since in general the consequence types are not numerically defined, we cannot perform the combination with numerical convolution. We chose to perform a linguistic convolution and that can be done by developing an approximate reasoning rule base. We consider Overall Consequence linguistically using the fuzzy sets “Low,” “Medium, or “High.” We chose to not numerically define these fuzzy sets using degrees of membership but rather define them in the context of a rule base for the combination of the constituent consequences.

For example, consider two specific consequences (Deaths and Fear in the Populace) combined into overall Consequence as indicated by the rule base of Table 3-1.

The rule base incorporates approximate reasoning because the inputs for the rules (Minor, Little, etc.) are approximate (fuzzy sets). The rules are a linguistic equivalent of a numerical convolution.

Table 3-1. Example Rule Base for Overall Consequence (OC)

Deaths	Fear in the Populace		
	Little	Some	Lots
Minor	<i>Low OC</i>	<i>Medium OC</i>	<i>Medium OC</i>
Moderate	<i>Medium OC</i>	<i>Medium OC</i>	<i>Medium OC</i>
Major	<i>High OC</i>	<i>High OC</i>	<i>High OC</i>
Catastrophic	<i>High OC</i>	<i>High OC</i>	<i>High OC</i>

When evaluating the rules we have considerable uncertainty that can be expressed as the assignment of degrees of evidence to families of fuzzy sets. For example, for a specific scenario our evidence for Fear in the Populace may be as indicated in Figure 3-7.

Figure 3-7. Example Degrees of Evidence For Fear in the Populace

We assign evidence at the fuzzy set level. The fuzziness of the set affects our assignment of evidence; for example, the evidence in Figure 3-7 depends on our common understanding of the fuzzy meanings of “Little,” “Some,” and “Lots.” Section A.3.6 discusses the details of the convolution calculation using the rule base. Since both the evidence and the rules are at the fuzzy set level, and we do not have the fuzzy sets defined in terms of degrees of membership, the convolution is as if the fuzzy sets were crisp. The fuzziness of the sets is considered in the assignment of evidence, not in the convolution process.

A simple example of the linguistic convolution process is as follows.

Consider a simple purely linguistic example where we wish to reason on Quality of Life based on Health and Wealth. For “Health” we will use the fuzzy sets “Bad,” “Moderate,” “Excellent.”

Uncertainty is reflected by the assignment of degrees of evidence to appropriate combinations of these fuzzy sets. For example, based on the information available for a specific individual named “John” we may assign the following evidence for the “Health” of “John”:

0.8 to {"Bad," "Moderate"}, and
0.2 to {"Moderate," "Excellent"}.

Assume we model "Wealth" with the fuzzy sets "Poor," "Middle Class," and "Rich." Based on the evidence available we assign evidence for the "Wealth" of "John" as:

0.3 to {"Middle Class"}, and
0.7 to {"Poor," "Middle Class"}.

We wish to reason on the linguistic "Quality of Life" based on combining "Health" and "Wealth" using the rule base for "Quality of Life" is provided in Table 3-2.

Table 3-2. Rule Base for Quality of Life (QL)

Wealth	Health		
	Bad	Moderate	Excellent
Poor	<i>Not So Good (QL)</i>	<i>Not So Good (QL)</i>	<i>Good (QL)</i>
Middle Class	<i>Not So Good (QL)</i>	<i>Not So Good (QL)</i>	<i>Good (QL)</i>
Rich	<i>Not So Good (QL)</i>	<i>Good (QL)</i>	<i>Good (QL)</i>

The rule base implies that "Quality of Life" "Not So Good" is formed from:

{<"Bad," "Poor">, <"Bad," "Middle Class">, <"Bad," "Rich">, <"Moderate," "Poor">, <"Moderate," "Middle Class">},

and that "Quality Of Life" "Good" is formed from:

{<"Moderate," "Rich">, <"Excellent," "Poor">, <"Excellent," "Middle Class">, <"Excellent," "Rich">}.

Using the evidence provided for "Health" and "Wealth" for "John" and the rule base for "Quality of Life," and assuming that "Health" and "Wealth" are non-interactive, we obtain the following focal elements (here focal elements are evidence for combinations of fuzzy sets) for "John":

{<"Bad," "Middle Class">, <"Moderate," "Middle Class">} with evidence 0.24

{<"Bad," "Poor">, <"Moderate," "Poor">, <"Bad," "Middle Class">, <"Moderate," "Middle Class">} with evidence 0.56

{<"Moderate," "Middle Class">, <"Excellent," "Middle Class">} with evidence 0.06

{<"Moderate," "Poor">, <"Excellent," "Poor">, <"Moderate," "Middle Class">, <"Excellent," "Middle Class">} with evidence 0.14.

The combinatorics involved in evaluating a rule base are straightforward but tedious; the author wrote a Java computer code called LinguisticBelief to perform convolution of linguistic variables with fuzzy sets using belief/plausibility. This code is described in Appendix D.

For the single simple rule base for “Quality Of Life” for “John” a manual evaluation is instructive.

The belief/plausibility for Not So Good is calculated using Equation 1-1 (refer to Appendix A.) The following two focal elements of Health x Wealth¹⁵ are a subset of Not So Good:

{<Bad, Middle Class>, <Moderate, Middle Class>}, and
{< Bad, Poor>, <Moderate, Poor >, < Bad, Middle Class >, <Moderate, Middle Class >},

so $\text{Bel}(\text{Not So Good}) = 0.24 + 0.56 = 0.80$.

All the focal elements of Health x Wealth have non-null intersection with Not So Good, so $\text{Pl}(\text{Not So Good}) = 1.0$.

Similarly for Good, $\text{Bel}(\text{Good}) = 0$ and $\text{Pl}(\text{Good}) = 0.06 + 0.14 = 0.20$.

In summary, using the mathematics of belief/plausibility, we obtain the following results for “Quality of Life” for “John”:

“Not So Good” has a belief/plausibility interval of 0.8/1.0
“Good” has a belief/plausibility interval of 0/0.2.

Figure 3-8 shows these results.

¹⁵ For linguistic reasoning, “x” represents convolution per the rule base.

Figure 3-8. Quality of Life for John

The rule base can be extensive. For example, we can combine “Quality of Life” with “Outlook On Life” to evaluate “Happiness.” Let the fuzzy sets for “Outlook on Life” be “Pessimist” and “Optimist” and let the fuzzy sets for “Happiness” be “Depressed,” “Accepting,” and “Very Happy.” Form “Happiness” using the following rule base:

Table 3-3. Rule Base for Happiness (H)

Quality Of Life	Outlook On Life	
	Pessimist	Optimist
Not So Good	<i>Depressed (H)</i>	<i>Accepting (H)</i>
Good	<i>Accepting (H)</i>	<i>Very Happy (H)</i>

Assume the following evidence for “Outlook on Life” for “John”:

{“Pessimist”} with evidence 0.02, and
 {“Pessimist,” “Optimist”} with evidence 0.98.

Using the LinguisticBelief code, the results for “Happiness” for “John” are:

“Very Happy” has a belief/plausibility interval of 0/0.196
 “Accepting” has a belief/plausibility interval of 0/0.984
 “Depressed” has a belief/plausibility interval of 0.016/1.0.

Figure 3-9 illustrates the results.

Figure 3-9. Happiness for John

The utility of the linguistic technique using belief/plausibility is that it focuses the argument on the rules for how we evaluate the result of a combination of many very different variables each with considerable epistemic uncertainty, rather than focusing on a precise numerical estimate of the result, given little information.

The ability to reason with linguistic variables and also propagate epistemic uncertainty for the values of the variables is a powerful tool. Many of our current evaluations related to terrorist risk are linguistic. For example, the “red,” “orange,” yellow,” “blue,” “green” threat advisory ranking employed by the Department of Homeland Security (DHS) is linguistic.

Some existing simple evaluations of terrorist risk use linguistics for such variables as likelihood and consequence, but assign numerical point estimates such as 5 for high and 3 for low. These techniques have problems. For example, there is little basis for assigning a value of “5” for a high consequence (e.g., why not the square root of 13?). There is little basis for combining the numbers as variables (Does a “3” likelihood and a “5” consequence have a result of $3 + 5 = 8$ or $3 \cdot 5 = 15$ or $3^{1/4} \cdot 5^2 = 32.9$ or something else?). There is no consideration of uncertainty; we have insufficient information to assign a “5”: all we know is that the interval $[3, 5]$ is more likely than the interval $[0, 3]$ but either can occur.

A better process for performing linguistic evaluations can propagate uncertainty, such as the one just discussed using fuzzy sets and belief/plausibility. Section 5 provides a simple example of this process for evaluating a terrorist scenario.

4 Evaluation of a Scenario with the Defender Model

The risk for a particular scenario can be evaluated as:

$$Risk = f_A * (1.0 - P_E) * C \quad (\text{Eqn. 4-1})$$

where f_A is the defender estimate for the frequency that the scenario is implemented by the adversary, P_E is the probability that the protection system prevents the scenario from being successful, and C is the consequence if the attack is not neutralized.^{16, 17} *Note:* $(1 - P_E)$ is the probability that the adversaries defeat the security system. In Equation 4-1, Risk has the units of consequence per unit time. Equation 4-1 is similar in form to the risk equation for a random event modeled in a safety analysis.¹⁸ However, the risk equation for a terrorist act considers intentional rather than random acts.

f_A , P_E , and C are treated as random variables with a belief measure and Equation 4-1 is evaluated by convoluting the random variables.

In practice for our application, the evidence is from expert elicitation and is typically over intervals of real numbers; when the evidence supports the use of probability, the intervals degenerate into points and the evidence is over a discrete set of points.

A simple example of the process follows. The results for this example were calculated with the BeliefConvolution Java code.

Let the sample spaces for f_A , P_E , and C be:

$$\begin{aligned} f_A &= [0, 10] \text{ with units of per year} \\ P_E &= [0, 1] \text{ dimensionless} \\ C &= [0, 10^7] \text{ with units of number of deaths} \end{aligned}$$

¹⁶ Sometimes Equation 4-1 is written $Risk = P_A * (1 - P_E) * C$ where P_A is the probability that the scenario is implemented by the adversary. Use of P_A can cause problems if f_A is not small. P_A depends on the time of interest. Usually, the time of interest is a year. P_A can be calculated from f_A , assuming that f_A is the parameter for an exponential distribution. The probability that the scenario occurs *one or more times* within time T is $P_A(T) = 1 - \exp(-f_A T)$ which approaches 1 for large $f_A T$. It is sometimes erroneously stated that f_A in units per year is the probability over a time period of one year; if $f_A T$ is small this is valid since a series expansion for $P_A(T)$ is $1 - (1 - f_A T + \dots)$ which is $f_A T$ for small $f_A T$, and for T equal to 1 year, $P(1)$ is numerically equal to f_A . If f_A is not small, say 10 per year, the probability of the event occurring *one or more times* over a time period of a year is $P_A(1) = 1 - \exp(-10 * 1)$ which is 0.99995 (approximately 1). Typically we want the likelihood of the consequence, which for large f_A is not P_A ; therefore, the initiating event should be quantified as a frequency. Note that f_A is treated as a random variable, not a constant value, to capture the uncertainty in its value; the defender has more uncertainty (mostly epistemic) in f_A than in either P_E or C .

¹⁷ f_A includes the effectiveness of intelligence efforts to prevent implementation of the scenario. P_E considers the effectiveness of security system elements to defeat an attack given implementation of the scenario.

¹⁸ For example, the risk from an earthquake for a facility can be evaluated as $f_E * P_F * C$ where f_E is the frequency of the earthquake, P_F is the conditional probability that the facility fails given the earthquake (fragility), and C is the consequence. Note that the initiating event, the earthquake, is modeled as a frequency, f_E , consistent with the use of a frequency f_A for the initiating event in our defender model.

Assume that the scenario is sufficiently well-specified such that P_E and C can be modeled probabilistically with the degrees of evidence (probabilities) given in Figure 4-1.¹⁹ (In Figure 4-1 “m” denotes a degree of evidence that reduces to a probability “p” if the focal elements are singletons. Refer to Appendix A.)

Figure 4-1. Degrees of Evidence (Probabilities) for P_E and C

Assume f_A is modeled with the degrees of evidence given in Figure 4-2. The evidence is over intervals; specifically, 0.7 is evidence for the interval $[0, 10^{-5}]$, 0.15 is evidence for the interval $[0, 10^{-3}]$, and 0.15 is evidence for the interval $[0, 10^{-2}]$.

Figure 4-2. Degrees of Evidence (Nested) for f_A

¹⁹ It is not required that P_E and C be modeled using probability as the measure of uncertainty; for this example, they are modeled probabilistically to illustrate that variables with a probability measure can be convoluted with variables with a belief/plausibility measure, since probability is a special case of belief/plausibility. In this example, the scenario is well-defined so that the uncertainties in the performance of the security system and in the consequence are purely aleatory. For example, uncertainty in P_E is dominated by the time for the guard force to respond given detection, which depends on the random distribution of guards during the day. Uncertainty in C is dominated by the weather for a consequence being release of a toxic chemical from the target.

Since the degrees of evidence are nested, the uncertainty in f_A is a special case of belief/plausibility called necessity/possibility, as discussed in Appendix A.

In common usage, “Conditional Risk” is the risk given an attack: $(1-P_E)*C$. Conditional Risk is sometimes called Expected Consequence, meaning the consequence, C , weighted by the probability that an attack (if attempted) is successful in causing the consequence, $(1-P_E)$. For this example, conditional risk has a probability distribution with an expected value (mean) of 3881 deaths. Figure 4-3 shows the probability of exceedance for conditional risk.

Figure 4-3. Exceedance Probability for Conditional Risk (Expected Consequence)

Figure 4-4 provides the belief/plausibility for risk exceedance. This result is the uncertainty distribution for the random variable Risk for our scenario. For any event A , $\text{Bel}(A) + \text{Pl}(A^C) = 1$ where A^C is the complement of event A . For example, the belief/plausibility of greater than 100 deaths per year is 0/0.00374; the belief/plausibility of less than or equal to 100 deaths per year is 0.99625/1.0. The expected value interval for Risk is $[0, 6.4]$ deaths per year.

As indicated in Figure 4-2, the information for f_A is not specific enough to justify the use of a probability distribution. If we *force* f_A to be modeled probabilistically we will lose much of the uncertainty inherent in the evidence. To illustrate this, a probability distribution can be generated for f_A assuming a uniform probability distribution over focal elements.

For example, approximate the sample space as the discrete set $f_A = \{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 1, 10\}$. For the focal element $\{0, 10^{-5}\}$ the degree of evidence is 0.7 and the probabilities are 0.7/2 for both 0 and 10^{-5} . For the focal element $\{0, 10^{-5}, 10^{-4}, 10^{-3}\}$ the degree of evidence is 0.15 and the probabilities are 0.15/4 for 0, 10^{-5} , 10^{-4} , and 10^{-3} . For the focal element $\{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}\}$ the degree of evidence is 0.15 and the probabilities are 0.15/5 for 0, 10^{-5} , 10^{-4} , 10^{-3} , and 10^{-2} . Summing, the probability distribution for $\{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}\}$ is $\{0.4175, 0.4175, 0.0675, 0.0675, 0.03\}$.

Figure 4-4 also shows the probability for risk exceedance using this *assumed* probability distribution for f_A . The mean of the probability distribution is 1.5 deaths per year. Figure 4-5 shows the expected values for deaths per year using both the belief measure and the forced probability measure. The loss of uncertainty is evident in both Figures 4-4 and 4-5 when the results from the probability model are compared to the results from the belief/plausibility model.

Figure 4-4. Risk Exceedance Results using Belief/Plausibility and Probability.

Figure 4-5. Expected Values with Belief and Probability

In application, many scenarios are of concern. The goal is to rank scenarios by decreasing risk. One approach is to rank scenarios based on the upper value of the expected value interval for risk, sub-ranked by the lower value of the expected value. Figure 4-6 shows a graphical summary of this process.

Figure 4-6. Ranking of Scenarios

Most risk assessments summarize risk by segregating likelihood and consequence. For our situation, likelihood could be taken as $f_A * (1 - P_E)$ and consequence as C , or likelihood could be taken as f_A and consequence as $(1 - P_E) * C$, the expected consequence. Since P_E and C are affected by actions on the part of the defender and f_A is determined by the adversary, we chose to consider likelihood as f_A and consequence as expected consequence, $(1 - P_E) * C$. We can calculate an expected value for both f_A and $(1 - P_E) * C$. For the example previously discussed, the expected value interval for f_A is $[0, 1.7 \times 10^{-3}]$ per year and the expected value (a point estimate since P_E and C were modeled using probability for this example) for the expected consequence, $(1 - P_E) * C$, is 3.9×10^3 deaths.

For each of the scenarios ranked as indicated in Figure 4-6, a segregation of likelihood and expected consequence can be provided as indicated in Figure 4-7, where in general expected consequence will have an interval for its expected value. The actual belief/plausibility distributions for f_A , $(1 - P_E) * C$, and $f_A * (1 - P_E) * C$ are available for more detailed evaluations of scenarios.

Figure 4-7. Summary of Scenarios by Expected Values for Likelihood and Expected Consequence

We can define overall risk as the addition of risk for each scenario. It is possible mathematically to evaluate overall risk by convoluting the belief/plausibility distributions for each scenario. However, the large number of scenarios may preclude this, and it is not clear what this result would add to the decision process.

Safety-based assessments of risk frequently summarize risk for all initiating events of concern as an “exceedance frequency of consequence” based on the “risk triplet approach” [Kaplan, Garrick]. Considering uncertainty measured with probability, the result is a family of curves,

each representing a specific percentile of probability. As discussed in Appendix E, this approach can be extended and used when belief/plausibility is the measure of uncertainty. Figure 4-8 summarizes risk for the earlier example as an exceedance frequency of consequence. With 0.95 belief the frequency of exceeding 1×10^5 deaths is not greater than 2×10^{-5} per year; with 0.70 belief the frequency of exceeding 1×10^5 deaths is not greater than 4×10^{-8} per year.

Figure 4-8. Risk in Exceedance Frequency of Consequence Format for Example Problem

The assignment of evidence to f_A is based on the defender evaluation of the scenario from the viewpoint of the adversary. Section 5 discusses the adversary model. The results of the adversary model provide information that is part of the defender state of knowledge for assigning evidence to f_A .

This section has presented an example of the evaluation of risk for one scenario from the viewpoint of the defender. As discussed in Section 2.4.2, the defender should evaluate all scenarios and minimize overall risk by allocating resources over all scenarios, and the process for considering many scenarios is under development.

5 Evaluation of a Scenario with the Adversary Model

The expected consequence for a particular scenario can be evaluated as:

$$\text{Expected Consequence} = (1 - P_E) * C \quad (\text{Eqn. 5-1})$$

where P_E is the adversary estimate of the probability that the security system prevents success of the scenario, and C is the adversary estimate of the consequence if the attack is successful. In Equation 5-1, Expected Consequence has the units of consequence.

Let P_A be the adversary estimate for the probability of success of the scenario. That is, $P_A = (1 - P_E)$ and Expected Consequence = $P_A * C$.

P_A and C are treated as linguistic variables with fuzzy sets, and a belief/plausibility measure is used to capture uncertainty. Equation 5-1 is evaluated by linguistic convolution using a rule base. Sections 1 and 3.3 discussed the rationale for the linguistic model for the adversary.

The rule base is developed based on the expertise available to construct the rules to “think like the adversary.” The point is that the adversary model focuses on the rules by which the adversary makes a decision as to the attractiveness of scenarios, and uncertainty is captured and propagated up the rule base. In actual application, the defender must play the role of the adversary, or perhaps use a red team to play the role of the adversary. Due to the uncertainty on the part of the defender/red team as to how the adversary actually thinks, there is considerable uncertainty in the adversary model as developed by the defender/red team. The adversary model uses belief/plausibility to capture this uncertainty.

A simple example of the process follows. The rule base is an example rule base and is not meant to be the final rule base actually used in an evaluation. The results for this example were calculated with the LinguisticBelief Java code.

Assume the following approximate reasoning process where “x” indicates convolution as defined in the rule base:

Expected Consequence = Probability Of (Adversary) Success x Consequence

Probability Of Success = Probability Resources Required Gathered Without
Detection x Probability Information Required Can Be Obtained x
Probability Physical Security System can be Defeated

Consequence = Deaths x Damage to National Security

Assume the following fuzzy sets for each linguistic variable:

Expected Consequence = {No, Maybe, Yes}

Probability Of Success = {Low, Medium, High}

Consequence = {Small, Medium, Large}

Probability That Resources Required Were Gathered Without Detection = {Low, Medium, High}

Probability That Information Required Can Be Obtained = {Low, Medium, High}

Probability That Physical Security System Can Be Defeated = {Low, Medium, High}

Deaths = {Minor, Moderate, Major, Catastrophic}

Damage To National Security = {Insignificant, Significant, Very Significant}

This example has three rules, as shown in the next three tables. Table 5-1 assumes a rule base for *Expected Consequence (EC)*:

Table 5-1. Rule #1: Rule base for Expected Consequence (EC)

Consequence	Probability Of Success		
	Low	Medium	High
Small	No (EC)	No (EC)	No (EC)
Medium	No (EC)	No (EC)	Maybe (EC)
Large	No (EC)	Maybe (EC)	Yes (EC)

Table 5-2 assumes a rule base for *Consequence (C)*.

Table 5-2. Rule #2: Rule base for Consequence (C)

Deaths	Damage To National Security		
	Insignificant	Significant	Very Significant
Minor	Small (C)	Medium (C)	Large (C)
Moderate	Medium (C)	Medium (C)	Large (C)
Major	Large (C)	Large (C)	Large (C)
Catastrophic	Large (C)	Large (C)	Large (C)

The last rule, Table 5-3, has three dimensions, based on the value assumed for the Probability that the Physical Security System can be Defeated, which may be “High”, “Medium”, or “Low”.

Table 5-3. Rule #3: Rule base for *Probability Of Success (PS)* with Varying Degrees of Probability that the Physical Security System can be Defeated

Probability that the Physical Security System can be Defeated = High			
Probability Information Required can Be Obtained	Probability Resources Required Gathered Without Detection		
	Low	Medium	High
Low	<i>Low (PS)</i>	<i>Low (PS)</i>	<i>Low (PS)</i>
Medium	<i>Low (PS)</i>	<i>Medium (PS)</i>	<i>Medium (PS)</i>
High	<i>Low (PS)</i>	<i>Medium (PS)</i>	<i>High (PS)</i>
Probability that the Physical Security System can be Defeated = Medium			
Probability Information Required can Be Obtained	Probability Resources Required Gathered Without Detection		
	Low	Medium	High
Low	<i>Low (PS)</i>	<i>Low (PS)</i>	<i>Low (PS)</i>
Medium	<i>Low (PS)</i>	<i>Medium (PS)</i>	<i>Medium (PS)</i>
High	<i>Low (PS)</i>	<i>Medium (PS)</i>	<i>Medium (PS)</i>
Probability that the Physical Security System can be Defeated = Low			
Probability Information Required can Be Obtained	Probability Resources Required Gathered Without Detection		
	Low	Medium	High
Low	<i>Low (PS)</i>	<i>Low (PS)</i>	<i>Low (PS)</i>
Medium	<i>Low (PS)</i>	<i>Low (PS)</i>	<i>Low (PS)</i>
High	<i>Low (PS)</i>	<i>Low (PS)</i>	<i>Low (PS)</i>

Assume the following evidence for a particular scenario:

Deaths:

0.8 for {Major, Catastrophic}

0.2 for {Moderate, Major}

Damage to National Security:

0.1 to {Insignificant, Significant}

0.9 to {Significant, Very Significant}

Probability Resources Required Obtained Without Detection:

0.7 to {Medium}

0.3 to {Medium, High}

Probability Information Required Can Be Obtained:

0.15 to {Medium}
0.85 to {Medium, High}

Probability Physical Security System Can Be Defeated:
1.0 to {Medium, High}

The rule base reflects the following:

- Expected Consequence “Yes” indicates an attractive scenario for the adversary and requires that Probability Of Success (for the adversary) be “High” and Consequence be “Large.”
- Probability of Success “High” requires a “High” value for each of the three constituent probabilities.
- Consequence “Large” is from Deaths and/or Damage To National Security being severe enough from the viewpoint of the adversary.

Using the LinguisticBelief code, the results in Figures 5-1 to 5-3 were obtained.

Figure 5-1. Results for Probability Of Success

Figure 5-2. Results for Consequence

Figure 5-3. Results for Expected Consequence

The results for this scenario indicate that although the adversary estimates a “Large” consequence to be likely (belief/plausibility of 0.8/1.0), the adversary expects Probability of Success to be only “Medium” (belief/plausibility of 0.7/1.0), resulting in an overall estimate that

Expected Consequence will be “Maybe” (belief/plausibility of 0.6/1.0). Since the adversary has a choice of scenarios, the adversary will continue examining other scenarios until ones with a high likelihood of “Yes” for Expected Consequence are identified.

In application, there will be many scenarios of concern. The goal is to rank scenarios by decreasing expected consequence. One approach is to rank scenarios based on the plausibility for the worst fuzzy set for expected consequence, “Yes” in the prior example, sub-ranked by plausibility of the next-worst fuzzy sets, “Maybe” and “No” in the prior example.²⁰

This section has presented an example of the evaluation of risk for one scenario from the viewpoint of the adversary. As discussed in Section 2.4.1, the model to date assumes that the adversary will maximize expected consequence by allocating resources over selected scenarios, and the process for considering many scenarios is under development.

²⁰ As the defender thinking like the adversary, we rank by plausibility. If the actual adversary used this linguistic evaluation tool to assist in the selection of scenarios, the adversary would rank by belief. This is evident in exercises conducted by special forces acting as a surrogate adversary; unless they believe that a scenario has high certainty for success, they will discard this scenario and choose another one with less uncertainty.

6 Assumptions, Areas for Future Work, and Conclusions

Sections 4 and 5 discussed the defender and adversary models, respectively, and provided example applications of each. To automate these evaluations, Java codes have been developed as discussed in Appendix D.

6.1 Assumptions

The adversary model is based on the assumption that the adversary goal is to maximize expected consequence.

A great deal of dependence is built implicitly into the model. Expected consequence, on the part of the adversary, and risk, on the part of the defender, depend on a scenario. Thus, the evaluations must be done for each scenario of concern.

Many of the variables in the model are conditional. For example, in the defender model, the effectiveness of the security system is conditional on implementation of the scenario by the adversary, and consequence is conditional on success of the scenario.

The evaluation of the models assume that the variables to be convoluted are non-interactive in the sense of belief, which allows for multiplication of evidence for focal elements during convolution. For the case where the focal elements are singletons, belief reduces to probability and this assumption is equivalent to assuming that the variables are probabilistically independent. A report by Ferson discusses the problem of dependence among variables. [Ferson] Helton is developing Monte-Carlo sampling techniques for the belief/plausibility measure; such techniques would eliminate the dependence problem associated with repeated variables that cannot be factored. [Helton et al. 2006] Also, as is the case for large-scale probabilistic evaluations, Monte-Carlo sampling would greatly improve the automation of the calculation of belief/plausibility.

The “combinatorics” issue associated with the use of belief/plausibility as a measure of uncertainty is considerable. Belief/plausibility requires consideration of evidence over the power set of the universe of discourse, and the number of focal elements from convolution of a large number of variables can be too large to maintain even using computer codes. To address this problem, the codes discussed in Appendix D implement “aggregation” of evidence.

6.2 Areas for Future Work

Using a probability measure, new information can be mechanistically incorporated to generate an updated probability distribution using a Bayesian update technique. A similar process for belief/plausibility that updates evidence assigned to focal elements given new information is being investigated.

The complex issue of dependence requires further research. The problem with dependence is that “it depends”. An example from probabilistic risk analysis applications to nuclear power plants is illustrative. Suppose an event of concern is a flood from an internal pipe break

followed by failure of a motor-operated valve to open on demand. There is dependence because the flood can short out the motor if the flood is high enough to cover the motor. The likelihood that the flood shorts the motor depends on: location of the break, amount of water that exits the break, where the water collects, and where the motor is located relative to where the water collects. Also the valve motor can fail by flooding of the supply of power to the motor, which depends on where the motor control center, circuit breakers, and electrical switchgear are located that power the motor. Also, if the electrical power supply is flooded then more than one motor is lost as the same power train powers many motors. The only way to address such dependence is by individual case, based on the details of the scenario.

For terrorist acts, the dependence is much more complicated than for random “dumb” acts. For example, consider two scenarios “a” and “b” involving attacks against targets in the U.S., quantified with frequencies f_a and f_b . If “a” is attempted and succeeds in causing large consequences, then f_b may increase as success encourages more attacks; if “a” is attempted and fails, then f_b may decrease. Also, both f_a and f_b can change, based on world events outside the U.S. With a war between Israel and Hezbollah, terrorist groups may decide to attempt “a”, “b”, or both with higher likelihood to punish the U.S., a supporter of Israel.

So dependence is of concern and needs to be addressed in the context of specific applications.

The adversary model may need to be extended to use a more complex measure than “maximize expected consequence.” Section 2 discussed the metrics to be used for the adversary and defender: expected consequence and risk. These metrics are based on evaluating individual scenarios and the number of scenarios can be immense. Furthermore, each scenario is to be evaluated from the perspective of both the adversary and the defender including propagation of uncertainty using the belief/plausibility measure. Scenarios must be combined into classes of scenarios and screening criteria must be developed to reduce the number of scenarios to a manageable number.

A test application of the models is expected to provide insight for improvements to and more effective automation of the methodology. To date, the methodology is being used in two areas:

- Evaluation of cyber security as part of an SNL LDRD program. The BeliefConvolution code is being used within a larger Java evaluation tool for this project. The belief/plausibility measures were selected for this cyber security project because computer security experts were not comfortable with assigning probability distributions for the effectiveness of cyber security protection elements, but they were comfortable with assigning evidence to intervals.
- Consideration of the effectiveness of intelligence-gathering activities to detect adversaries gathering resources beyond those specified in the DBT for attacks on DOE nuclear materials processing/handling sites.

It is expected that the adversary model will soon be applied to the evaluation of intelligence information for a classified project.

6.3 Conclusions

A terrorist attack is not a random event, yet there is considerable epistemic uncertainty as to which scenarios a terrorist will chose to implement. The belief/plausibility measure of uncertainty is proposed to capture this uncertainty in the evaluation of risk from intentional terrorist acts when we, the defender, attempt to think like them, the adversary.

The adversary and defender each have different goals and different knowledge. The goal of the adversary is to maximize expected consequence for a select number of scenarios restrained by the resources available to the adversary. The goal of the defender is to minimize risk considering all scenarios. This report proposes the use of an adversary/defender model to address these differences in objectives. The use of a separate model for adversary and defender allows the different epistemic uncertainty for each to be explicitly considered. The use of separate models allows the evaluation of scenarios on the part of the adversary to be performed linguistically, an appropriate approach considering the choices available to the adversary. The defender model is a numerical model.

Software has been developed in Java to implement the evaluation of scenarios for both the adversary and defender.

Appendix A. The Belief Measure of Uncertainty

This appendix discusses the mathematics for the belief measure of uncertainty. The references provide more detailed information.

The axioms for belief require that the number of focal elements for a universe of discourse be countable. Sections A.2 and A.3 of this report address discrete sets. Section A.4 discusses intervals of real numbers.

A.1 Value and Uncertainty

A random variable is a real-valued function defined on a sample space. [Dougherty] The values for a random variable can be represented as a set of all possible numerical values; for example, $X = \{x \mid x \text{ an element of } [0,1]\}$.²¹ The uncertainty for a random variable can be expressed by assigning a “likelihood” to events in its set. Therefore, a complete description of the random variable consists of two parts: (1) the set of all possible values and (2) an uncertainty measure on that set. A random vector is a combination of random variables and the random vector has a set of values (tuples). The name convolution is used to denote the combination of uncertainties of random variables into an uncertainty for a function defined on the random vector.

Consider two discrete random variables with ranges defined as follows:²²

$$\begin{aligned} X &= \{x_i \mid i = 1, 2, \dots, n\} \\ Y &= \{y_j \mid j = 1, 2, \dots, m\} \\ X \times Y &= \{ \langle x, y \rangle \mid x \in X, y \in Y \} \end{aligned} \tag{Eqn. A-1}$$

where x and y are real numbers. The random vector is the Cartesian product $X \times Y$. A subset of the Cartesian product $X \times Y$ is called a relation. In the remainder of this discussion, reference to the random variable X means the range for X .

We are interested in a function defined on a random vector that maps to the set of real numbers, $f: X \times Y \rightarrow \text{Reals}$. For example we may wish to perform addition, $X + Y$, or multiplication $X * Y$.²³ Let $f(x, y) = z$. The mapping f produces the solution:

$$Z = \{z \mid f(x, y) = z, x \in X, y \in Y\} \tag{Eqn. A-2}$$

²¹ To be precise, X is the range for its corresponding random variable; see Section B.4. The set contains all possible unique outcomes for the random variable. The elements of the set are mutually exclusive.

²² $\langle \rangle$ denotes a tuple whereas $\{ \}$ denotes a set; a tuple is an ordered collection and elements can be repeated, a set is an unordered collection and elements cannot be repeated. Uppercase is used for a random variable and lowercase is used for a value of the random variable; for example, X is a random variable and x is a specific value for X .

²³ If the random variables X and Y are probabilities (Kaplan frequencies in the sense of Appendix B), probabilistic combinations of these variables use the mathematics of a probability measure. For example, $X \cup Y = X + Y - X \cap Y$. If X and Y are mutually exclusive $X \cap Y = 0$; if X and Y are independent $X \cap Y = X * Y$.

Note that more than one $\langle x, y \rangle$ can have the same z . For example, if f is $X + Y$ then $\langle 2, 3 \rangle$ and $\langle 1, 4 \rangle$ both have $z = x + y = 5$.

Equation A-2 provides the values for the function of interest. We also need to generate a measure of uncertainty for each of these values by convoluting the uncertainties for X and Y . As subsequently discussed, there are measures of uncertainty besides probability, and we will use the name uncertainty to denote a general measure of which probability is one special case.²⁴ The mathematics for the convolution depend on the measure selected for uncertainty.

An uncertainty distribution is associated with each random variable; the uncertainty distribution specifies a “likelihood” for each value of the random variable.

Denote the power set of X as $Pow(X)$. $Pow(X)$ is defined as the set of all subsets X including the null set. For example, the power set of $X = \{a, b, c\}$ is $Pow(X) = \{\text{null}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. For a finite set with n elements the power set has 2^n elements. A general measure of uncertainty, U , is a mapping on the power set: $U: Pow(X) \rightarrow [0, 1]$. Using the mathematics for the uncertainty measure, a likelihood can be calculated for each event in X .

A.2 Types of Uncertainty and Measures of Uncertainty

A.2.1 Ambiguity and Belief/Plausibility

Let A be a subset of X . A is also called an event for the random variable. The elements of X are unique values (mutually exclusive). In general, events are not mutually exclusive since subsets of X can have common elements.²⁵

Since the sample space has unique elements, and the random variable is a mapping of the sample space to the reals, the value of a random variable will be unique, but there is uncertainty as to this value. This type of uncertainty is called Ambiguity. A measure of ambiguity is called a fuzzy measure in the literature. Ambiguity is the uncertainty in predicting the outcome of a future occurrence, such as the ultimate intensity and point of landfall for a hurricane forming in the Gulf of Mexico.

The most general fuzzy measure of interest for our evaluation of risk is Belief, which can be explained by considering degrees of evidence assigned to the elements of $Pow(X)$. Let m denote a degree of evidence. “ m ” is a function defined as follows:

$$\begin{aligned} m : Pow(X) &\rightarrow [0,1] \\ m(\text{null}) &= 0 \\ \sum_{A \in Pow(X)} m(A) &= 1 \end{aligned} \tag{Eqn. A-3}$$

²⁴ To be technically correct, what we call uncertainty here is a fuzzy measure. See Section A.2.1.

²⁵ For example let $X = \{a, b, c\}$ and let event $A = \{a, b\}$ and event $B = \{b, c\}$. A and B are not mutually exclusive since both contain b . A subset with only one element is called a singleton. Singleton events are mutually exclusive.

The elements of $\text{Pow}(X)$ for which m is greater than 0 are called the focal elements of X . The focal elements of X are the subsets (events) of X on which the evidence focuses.

In terms of degrees of evidence, Belief (Bel) and its dual fuzzy measure Plausibility (Pl) are defined as follows for any A and B in $\text{Pow}(X)$:

$$\begin{aligned} \text{Bel}(A) &= \sum_{B|B \subseteq A} m(B) \\ \text{Pl}(A) &= \sum_{B|A \cap B \neq \emptyset} m(B) \end{aligned} \quad (\text{Eqn. A-4})$$

$m(A)$ represents the evidence that the value of the random variable is *exactly* in A (in A only). $\text{Bel}(A)$ represents the evidence that the value of the random variable is in A or any subset of A . $\text{Pl}(A)$ represents the evidence that the value of the random variable is in A , in any subset of A , or any set that overlaps (is not disjoint) with A .

$\text{Bel}(A)$ is a measure of the amount of information that implies A^C is false, where A^C is the complement of A . $\text{Pl}(A)$ is a measure of the amount of information that implies A is true (i.e., does not negate “ A is true”).

One useful interpretation is that $\text{Bel}(A)$ is a measure of the degree to which A *will* happen, and $\text{Pl}(A)$ is a measure of the degree to which A *could* happen.

The collection of all the focal elements with non-zero degrees of evidence form the body of evidence.

The ambiguity type of uncertainty is completely specified by the body of evidence.

Two types of ambiguity are of interest. Strife (or Discord) is present if there is more than one focal element. Nonspecificity is present if a focal element is not a singleton.

With a belief/plausibility distribution, a random variable X has an expected value interval $[E_*(X), E^*(X)]$ given by:

$$\begin{aligned} E_*(X) &= \sum_{\text{all } A_i \subseteq X} \inf(A_i) * m(A_i) \\ E^*(X) &= \sum_{\text{all } A_i \subseteq X} \sup(A_i) * m(A_i) \end{aligned} \quad (\text{Eqn. A-5})$$

where A_i is an element of $\text{Pow}(X)$ and m is a degree of evidence.²⁶

As an example of Belief and Plausibility consider $X = \{a, b, c\}$ with the body of evidence given in Figure A-1.

²⁶ For a finite set $\sup$ (supremum, or least upper bound) is $\max$, and $\inf$ (infimum, or greatest lower bound) is $\min$.

Figure A-1. Example Body of Evidence for Belief and Plausibility

The body of evidence for Figure A-1 is: $\{a\}$ with $m = 0.2$, $\{a, b\}$ with $m = 0.7$, and $\{b, c\}$ with $m = 0.1$. This body of evidence exhibits both Strife and Nonspecificity.

Using Equation A-4, Bel and Pl can be evaluated for any element in $\text{Pow}(X)$. Of specific interest to us are these fuzzy measures for the singletons: $\text{Bel}(\{a\}) = 0.2$, $\text{Bel}(\{b\}) = 0$, $\text{Bel}(\{c\}) = 0$, $\text{Pl}(\{a\}) = 0.9$, $\text{Pl}(\{b\}) = 0.8$, and $\text{Pl}(\{c\}) = 0.1$. Figure A-2 shows the uncertainty distribution for this case.

Let $a = 8$, $b = 1$, and $c = 6$. Using Equation A-5, the expected value interval $[E^*(X), E^*(X)]$ is $[2.4, 7.8]$.

Figure A-2. Uncertainty Distribution for Body of Evidence in Figure A-1

A.2.2 Strife and Probability

Probability is a special case of Belief. If the focal elements are singletons, then both Belief and Plausibility reduce to a common fuzzy measure, Probability. For a discrete sample space, a probability measure assigns a degree of evidence to the elements of X (the singletons of $\text{Pow}(X)$), and the degree of evidence for an element, m , is called the probability, p , of the element. The degrees of evidence (probabilities) sum to 1.0.²⁷

The expected value, called the mean, of X is:

$$\bar{X} = \sum_{all\ x} x * p(x) \quad (\text{Eqn. A-6})$$

Equation A-6 is a special case of Equation A-5 where $E_*(X) = E^*(X)$; that is, the expected value interval is a point value.

Figure A-3 is an example body of evidence where probability is the appropriate metric for uncertainty for $X = \{a, b, c\}$.

Figure A-3. Example Body of Evidence for Probability

Using either Equations A-4 or A-5 where Bel and Pl are both denoted as Prob: $\text{Prob}(a) = 0.5$, $\text{Prob}(b) = 0.3$, and $\text{Prob}(c) = 0.2$. Figure A-4 shows the uncertainty distribution for this case.

Let $a=4$, $b=13$, and $c = 7$. Using either Equations A-5 or A-6, the expected value of the random variable is 7.3.

²⁷ As discussed earlier, here we are dealing with discrete sets. A probability measure requires that the probability of two disjoint events be the sum of the probabilities of each event. Since the elements of the set are mutually exclusive outcomes, the probability of any event defined on the set is the sum of the probabilities of its constituent outcomes. Events are in general not mutually exclusive since they can share outcomes and are therefore not disjoint.

Figure A-4. Uncertainty Distribution for Body of Evidence in Figure A-3

Probability is a special case of Belief/Plausibility where there is no Nonspecificity. Probability considers Strife but does not consider nonspecificity, so it is an inappropriate measure of uncertainty where there is significant nonspecificity.

Probability is well suited to problems where the uncertainty is aleatory (random) such as tossing a cubical die known to have 1 to 6 dots on each side. Probability is not well suited to problems where the uncertainty is epistemic (state of knowledge) such as a case where we do not know how many dots are on each face of the die or even that the die is a cube. Examples of situations where probability is not the best measure of uncertainty are provided in Section 3.

A.2.3 Coherent Evidence and Possibility

Belief/Plausibility becomes Necessity/Possibility, respectively, if the focal elements are nested. The nested requirement means that for any two focal elements A and B, either A is a subset of B or B is a subset of A. Possibility is applicable to situations where the body of evidence is coherent; that is, where nonspecificity dominates over strife. This is in contrast to a situation where a probability metric is applicable: the evidence is precise but contradictory. It is important to note that necessity/possibility never reduce to probability, but belief/plausibility both reduce to probability for specific evidence.

A possibility distribution can be produced based on the degrees of evidence, and the Possibility and Necessity for any element of the power set can be calculated from the possibility

distribution. The possibility distribution π is a mapping on the sample space X : $\pi: X \rightarrow [0,1]$.²⁸ Let x denote an element of X . Let Π denote the Possibility of any event A , a subset of X and let N denote the Necessity:

$$\begin{aligned}\Pi(A) &= \max_{x \in A} \pi(x) \\ N(A) &= \min_{x \notin A} (1 - \pi(x)) = 1 - \max_{x \in A^c} \pi(x) = 1 - \Pi(A^c)\end{aligned}\quad (\text{Eqn. A-7})$$

where A^c denotes the complement of A .

A simple way to generate the possibility distribution from the degrees of evidence is to order the focal elements by increasing level of nesting; that is, if the focal elements are $\{A_i \mid i = 1, 2, \dots, n\}$ reorder and renumber the focal elements such that $A_1 \subset A_2 \subset \dots \subset A_n$. With this rearrangement:

$$\pi(x_i) = \sum_{k=i}^n m(A_k) \quad (\text{Eqn. A-8})$$

where i denotes a focal element and x_i is any x that is a member of A_i . [Klir and Yuan]

For any function $f: X \rightarrow \text{Reals}$, using the Lebesgue-Stieltjes integrals, the expected interval for f is:

$$\begin{aligned}E_*(f) &= \sum_i f(x_i) [\Pi(\{x_j \mid f(x_j) \leq x_i\}) - \Pi(\{x_j \mid f(x_j) \leq x_{i-1}\})] \\ E^*(f) &= \sum_i f(x_i) [\Pi(\{x_j \mid f(x_j) > x_{i-1}\}) - \Pi(\{x_j \mid f(x_j) > x_i\})]\end{aligned}\quad (\text{Eqn. A-9})$$

$[E_*(X), E^*(X)]$ is obtained using $f(x) = x$ in Equation A-9.

For a probability distribution, the expected value is a point estimate given in Equation A-6. A necessity/possibility distribution (and a belief/plausibility distribution) has an expected value interval, $[E_*(X), E^*(X)]$ instead of a point estimate expected value. This is not surprising since the probability distribution over a random variable represented as a discrete set is a set of points as indicated in Figure A-4 while a necessity/possibility distribution (and a belief/plausibility distribution) over a random variable is a set of intervals as subsequently indicated in Figure A-6 for a possibility distribution (and previously indicated in Figure A-2 for a belief distribution).

As an example of Possibility and Necessity consider the body of evidence in Figure A-5 on $X = \{a, b, c\}$.

²⁸ If we have defined a random variable on the sample space, the random variable can be viewed as transforming the sample space to the reals, and the range of the random variable can serve as a surrogate sample space. [Dougherty, Probability] Therefore, X can be a random variable (a sample space on the reals) for which π specifies a possibility distribution for the values of the range of the random variable.

Figure A-5. Example Body of Evidence for Possibility and Necessity

Using Equations A-7 and A-8: $\Pi(a) = 1.0$, $\Pi(b) = 0.6$, $\Pi(c) = 1.0$, $N(a) = 0$, $N(b) = 0$, $N(c) = 0$. Figure A-6 shows the uncertainty distribution for this case.

Figure A-6. Uncertainty Distribution for Body of Evidence in Figure A-5

Let $a = 3$, $b = 8$, and $c = 2$. Using either Equations A-5 or A-9, the expected value interval $[E_*(X), E^*(X)]$ is $[2, 6]$.

Consider the assignment of uncertainty for the frequency of an attack using a possibility metric where $F_A = \{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 1\}$ per year. Since there are on the order of a million targets and approximately one attack per year, for a generic target the body of evidence justifies assignment of a degree of evidence of 1.0 to the subset $\{0, 10^{-5}\}$. (A generic target is one for which specific evidence of adversary intent is not available.) If there is evidence based on intelligence that a specific target is more likely to be attacked, then a body of evidence such as

that given in Figure A-7 can be produced, where the possibilities are calculated using Equation A-8.

Figure A-7. Example Possibilistic Model for Threat Frequency

A.2.4 Vagueness and Fuzzy Sets

Sections A.2.1 through A.2.3 discussed various measures of uncertainty that address ambiguity; such measures are called fuzzy measures. This section addresses another type of uncertainty, Vagueness.

Whereas ambiguity deals with the uncertainty related to which value of a random variable is likely to occur, Vagueness deals with the uncertainty of how to categorize a *known* value of a random variable. Vagueness can be modeled using the concept of fuzzy sets. Note that a fuzzy measure is a different concept from a fuzzy set; a fuzzy measure addresses ambiguity while a fuzzy set addresses vagueness.

A fuzzy set extends the concept of a traditional set, called a crisp set, to include partial membership. For example for the variable $X = \{a, b, c\}$ a crisp subset is $A = \{a, b\}$. Each element in X is either completely in A or not; a and b are in A and c is not in A . A fuzzy set can have members with partial membership, for example $F = \{1/a, 0.3/b\}$ is a fuzzy subset of X for which element a has total membership and element b has partial membership of degree 0.3. Fuzzy sets are useful for modeling linguistic concepts. For example consider the random variable for the frequency of an attack $F_A = \{0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}, 1\}$ and consider the following fuzzy sets for F_A : “unlikely,” “credible,” and “likely.”²⁹ Figure A-8 provides a possible definition of these fuzzy sets.

²⁹ “unlikely” is a set since it is a subset of F_A and it is a fuzzy set since not every element in “unlikely” has degree of membership of 1.0; for example 10^{-4} has degree of membership of 0.5 in “unlikely.” Similarly, “credible” and “likely” are fuzzy sets of F_A .

Figure A-8. Fuzzy Sets for Frequency of Attack

A.2.5 Probability of a Fuzzy Set

As developed in Section A.2.2, probability is a fuzzy measure that addresses a special type of ambiguity called strife. Probability can be extended to address vagueness and such an extension will be called “fuzzified” probability.

For a set X let $p(x)$ be the probability of element x in a discrete set X . Let F be a fuzzy set defined on X by the degree of membership $\mu_F(x)$. The probability of the fuzzy event F is:

$$P(F) = \sum_{x \in X} p(x) * \mu_F(x) \quad (\text{Eqn. A-10})$$

Equation A-10 weights the probability of x by the degree of membership of x in the fuzzy set of interest, F .

A.2.6 Possibility of a Fuzzy Set

As developed in Section A.2.3 possibility is a fuzzy measure that addresses ambiguity when the body of evidence is coherent. Possibility can be extended to address vagueness and such an extension will be called fuzzified possibility.

For a set X let $\pi(x)$ be the possibility for element x in X . Let F be a fuzzy set defined on X by the degree of membership $\mu_F(x)$. The possibility of the fuzzy event F is: [Dubois and Prade]

$$\Pi(F) = \sup_{x \in X} \min[\pi(x), \mu_F(x)] \quad (\text{Eqn. A-11})$$

Equation A-11 is an extension of Equation A-7 to fuzzy sets; it weights the possibility for x by the degree of membership of x in the fuzzy set of interest, F .

A.2.7 Belief for a Fuzzy Set

The development in this section summarizes the approach developed by Yager. [Yager 1986] Given fuzzy sets A and B for a universe of discourse X , the possibility for fuzzy set B given fuzzy set A is:³⁰

$$\Pi(B | A) = \max_{x \in X} \{ \min[\mu_A(x), \mu_B(x)] \} \quad (\text{Eqn. A-12})$$

where $\mu_A(x)$ is the degree of membership of the element x in the fuzzy set A .

The necessity for B given A is $1 - \Pi(B^c | A)$ where B^c is the fuzzy complement of B ; that is, $B^c \equiv 1 - B$. This necessity can be expressed as:

$$N(B | A) = 1 - \max_{x \in X} \{ \min[\mu_A(x), 1 - \mu_B(x)] \} \quad (\text{Eqn. A-13})$$

where $\mu_{B^c}(x)$ has been taken as $1 - \mu_B(x)$.

For “fuzzy focal elements” (fuzzy sets with evidence) A_i over X and for any fuzzy set B in X :

$$\begin{aligned} Pl(B) &= \sum_i [m(A_i) \cdot \Pi(B | A_i)] \\ Bel(B) &= \sum_i [m(A_i) \cdot N(B | A_i)] \end{aligned} \quad (\text{Eqn. A-14})$$

Equation A-14 reduces to Equation A-4 if the focal elements A_i and B are crisp sets.

If the focal elements A_i are crisp and B is fuzzy, Equation A-14 reduces to:

$$\begin{aligned} Pl(B) &= \sum_i [m(A_i) \cdot (\max \{ \mu_B(x) | x \in A_i \})] \\ Bel(B) &= \sum_i [m(A_i) \cdot (1 - \max \{ 1 - \mu_B(x) | x \in A_i \})] \end{aligned} \quad (\text{Eqn. A-15})$$

³⁰ If A and B are crisp, “given A ” means event A occurs, so $\Pi(A) = 1$ and $N(A) = 1$. $\Pi(B|A) = 1$ if A and B are not disjoint, otherwise $\Pi(B|A) = 0$. $N(B|A) = 1$ if B is a subset of A , otherwise $N(B|A) = 0$.

If A and B are fuzzy, “given A ” means that the possibility distribution is determined by the degrees of membership of A ; specifically, $\pi(x) = \mu_A(x)$ for all x in the universe of discourse X and: $\Pi(A) = \max_{x \in X} \mu_A(x)$, and $N(A) = \min_{x \in X} (1 - \mu_A(x))$. For a normalized fuzzy set (one with at least one element with a degree of membership of 1), $\Pi(A) = 1$ and $N(A) = 1$ since the fuzzy event A is the sure event. $\Pi(B|A)$ is evaluated as the overlap between fuzzy event B and the sure fuzzy event A using Equation A-12. [Dubois and Prade, Sections 1.4 and 1.7]

A.3 Convolution

Section A.2 summarized various metrics for uncertainty, specifically: Belief/Plausibility, Necessity/Possibility, Probability, Fuzzy Sets, “Fuzzified” Probability, “Fuzzified” Possibility, and “Fuzzified” Belief.

As discussed in Section A.1, it is necessary to convolute the uncertainty measures for random variables to produce an uncertainty measure for a function defined on a random vector. Sections A.3.1 through A.3.4 assume crisp sets; Sections A.3.5 and A.3.6 address fuzzy sets.

A.3.1 Probabilistic Convolution

As presented in Section A.2, the values for a function $f: X \times Y \rightarrow \text{Reals}$ defined on the random vector $X \times Y$ are given in Equation A-2 repeated here:

$$Z = \{z \mid f(x, y) = z, x \in X, y \in Y\} \quad (\text{Eqn. A-2, repeated})$$

Where $f(x, y) = z$. Let $p(x)$ and $p(y)$ be probability distributions over X and Y , respectively. The probability distribution $p(z)$ is:³¹

$$p(z) = \sum_{\text{all } x \in X, y \in Y} p(x, y) \mid f(x, y) = z \quad (\text{Eqn. A-16})$$

where $p(x, y)$ is the joint probability distribution over X and Y . If X and Y are independent random variables then $p(x, y) = p(x) * p(y)$.

A.3.2 Possibilistic Convolution

As presented in Section A-2, the values for a function $f: X \times Y \rightarrow \text{Reals}$ defined on the random vector $X \times Y$ are given in Equation A-2 repeated here:

$$Z = \{z \mid f(x, y) = z, x \in X, y \in Y\} \quad (\text{Eqn. A-2, repeated})$$

where $f(x, y) = z$. Let $\pi(x)$ and $\pi(y)$ be possibility distributions over X and Y , respectively. The possibility distribution $\pi(z)$ is:

$$\pi(z) = \sup_{\text{all } x \in X, y \in Y} \{\pi(x, y) \mid f(x, y) = z\} \quad (\text{Eqn. A-17})$$

where $\pi(x, y)$ is the joint possibility distribution over X and Y . If X and Y are non-interactive random variables (in the possibilistic sense) then $\pi(x, y) = \min[\pi(x), \pi(y)]$. This is the “min” definition of noninteraction.

³¹ Since the x elements are mutually exclusive and the y elements are mutually exclusive the $\langle x, y \rangle$ tuples are mutually exclusive and the probabilistic sum is an algebraic sum as indicated in the equation. As previously stated, this section deals with sets of discrete elements.

A.3.3 Convolution for Belief

As presented in Section A.2, the values for a function $f: X \times Y \rightarrow \text{Reals}$ defined on the random vector $X \times Y$ are given in Equation A-2 repeated here:

$$Z = \{z \mid f(x, y) = z, x \in X, y \in Y\} \quad (\text{Eqn. A-2, repeated})$$

For the random vector $X \times Y$ each degree of evidence can be considered a binary relation R .³² That is, R is a subset of $X \times Y$ with non-zero m .

Using Equation 2-4 the belief and plausibility for $z = f(x, y)$ are:

$$\begin{aligned} Bel(z) &= \sum_{R \subseteq X \times Y \mid z = f(x, y) \text{ and } R \subseteq \{<x, y>\}} m(R) \\ Pl(z) &= \sum_{R \subseteq X \times Y \mid z = f(x, y) \text{ and } \{<x, y>\} \cap R \neq \text{null}} m(R) \end{aligned} \quad (\text{Eqn. A-18})$$

Following Equation A-5, the expected value interval for f is:

$$\begin{aligned} E_*(f : X \times Y) &= \sum_{all \ R \subseteq X \times Y} \inf[f(R)] * m(R) \\ E^*(f : X \times Y) &= \sum_{all \ R \subseteq X \times Y} \sup[f(R)] * m(R) \\ \text{where } f(R) &= \{f(x, y) \mid <x, y> \in R\} \end{aligned} \quad (\text{Eqn. A-19})$$

Let C denote any subset of $X \times Y$. Using Equation A-4:

$$\begin{aligned} Bel(C) &= \sum_{R \subseteq X \times Y \mid R \subseteq C} m(R) \\ Pl(C) &= \sum_{R \subseteq X \times Y \mid R \cap C \neq \text{null}} m(R) \end{aligned} \quad (\text{Eqn. A-20})$$

For each R , let R_X denote the projection of R on X and let R_Y denote the projection of R on Y .

$$\begin{aligned} R_X &= \{x \in X \mid <x, y> \in R \text{ for some } y \in Y\} \\ R_Y &= \{y \in Y \mid <x, y> \in R \text{ for some } x \in X\} \end{aligned} \quad (\text{Eqn. A-21})$$

Define the marginal degrees of evidence m_x , the projection of m on X , and m_y , the projection of m on Y as:

³² A binary relation is defined as a subset of the Cartesian product $X \times Y$. For example, if $X = \{a, b\}$ and $Y = \{p, q\}$ then $X \times Y = \{<a, p>, <a, q>, <b, p>, <b, q>\}$ and $R = \{<a, p>, <a, q>, <b, q>\}$ is a binary relation on $X \times Y$.

$$\begin{aligned}
m_X(A) &= \sum_{R|A=R_X} m(R) \text{ for all } A \in \text{Pow}(X) \\
m_Y(B) &= \sum_{R|B=R_Y} m(R) \text{ for all } B \in \text{Pow}(Y)
\end{aligned}
\tag{Eqn. A-22}$$

where $R|A=R_X$ means all relations R such that the projection of R onto X (R_X) is equal to A .

For any focal elements A and B in X and Y , respectively, the marginal bodies of evidence are said to be noninteractive if and only if:

1. $m(A \times B) = m_X(A) * m_Y(B)$, and
2. $m(R) = 0$ for all $R \neq A \times B$.³³

This is the “product” definition of noninteraction.

The “min” definition of possibilistic noninteraction discussed in Section A.3.2 is **not** a special case of the “product” definition of noninteraction. Even if the focal elements of X and Y are nested, if X and Y are noninteractive using the product definition, the focal elements of $X \times Y$ may not be nested. That is, the product definition of noninteraction does not preserve nesting of focal elements. [Klir and Yuan, Section 7.3]

Probabilistic independence is a special case of the product definition of noninteraction. For a probability measure, a degree of evidence is a probability for an element of the sample space, so any focal elements A and B are singletons of X and Y (call them a and b) and $A \times B$ has one element $\{<a, b>\}$ with a probability $P(a)*P(b)$.

In this report, unless stated otherwise, noninteraction means the product definition of noninteraction.

Independence and noninteraction are discussed at length in a report by Ferson, et al. [Ferson 2004]

As an example of convolution for belief/plausibility let $X = \{x_1, x_2\}$ and $Y = \{y_1, y_2, y_3\}$. Assume the bodies of evidence for X and Y given in Figure A-9.

³³ The requirement that $m(A \times B) = m_X(A) * m_Y(B)$ means that for any focal elements A in X and B in Y , there is a focal element in $X \times Y$ formed by $A \times B$ with degree of evidence equal to $m_X(A) * m_Y(B)$. The requirement that $m(R) = 0$ for all $R \neq A \times B$ means that any focal element in $X \times Y$ is a Cartesian product of focal elements in X and Y .

Figure A-9. Bodies of Evidence for X and Y

The random vector $X \times Y = \{<x_1, y_1>, <x_1, y_2>, <x_1, y_3>, <x_2, y_1>, <x_2, y_2>, <x_2, y_3>\}$. The binary relations and the projections of those relations for the focal elements of $X \times Y$ are given in Table A-1.

Table A-1. Binary Relations and Projections for $X \times Y$ for Figure A-9

R	R_X	R_Y
$R_1 = \{<x_1, y_1>, <x_1, y_2>\}$	$R_{1X} = \{x_1\}$	$R_{1Y} = \{y_1, y_2\}$
$R_2 = \{<x_1, y_2>, <x_1, y_3>\}$	$R_{2X} = \{x_1\}$	$R_{2Y} = \{y_2, y_3\}$
$R_3 = \{<x_2, y_1>, <x_2, y_2>\}$	$R_{3X} = \{x_2\}$	$R_{3Y} = \{y_1, y_2\}$
$R_4 = \{<x_2, y_2>, <x_2, y_3>\}$	$R_{4X} = \{x_2\}$	$R_{4Y} = \{y_2, y_3\}$

The marginal degrees of evidence are given in Table A-2.

Table A-2. Marginal Degrees of Evidence

A an element of Pow(X)	$m_X(A)$	B an element of Pow(Y)	$m_Y(B)$
null	0		
$\{x_1\}$	$m(R_1) + m(R_2)$		
$\{x_2\}$	$m(R_3) + m(R_4)$		
$\{x_1, x_2\}$	0		
		null	0
		$\{y_1\}$	0
		$\{y_2\}$	0
		$\{y_3\}$	0
		$\{y_1, y_2\}$	$m(R_1) + m(R_3)$
		$\{y_1, y_3\}$	0
		$\{y_2, y_3\}$	$m(R_2) + m(R_4)$
		$\{y_1, y_2, y_3\}$	0

Assuming the bodies of evidence for X and Y are noninteractive:

$$m(R_1) = m(\{x_1\}) * m(\{y_1, y_2\}) = 0.12$$

$$m(R_2) = m(\{x_1\}) * m(\{y_2, y_3\}) = 0.48$$

$$m(R_3) = m(\{x_2\}) * m(\{y_1, y_2\}) = 0.08$$

$$m(R_4) = m(\{x_2\}) * m(\{y_2, y_3\}) = 0.32$$

and the body of evidence for $X \times Y$ is:

$$m(\{ \langle x_1, y_1 \rangle, \langle x_1, y_2 \rangle \}) = 0.12$$

$$m(\{ \langle x_1, y_2 \rangle, \langle x_1, y_3 \rangle \}) = 0.48$$

$$m(\{ \langle x_2, y_1 \rangle, \langle x_2, y_2 \rangle \}) = 0.08$$

$$m(\{ \langle x_2, y_2 \rangle, \langle x_2, y_3 \rangle \}) = 0.32$$

Using this body of evidence with Equation A-4, the belief and plausibility distributions for each element of $X \times Y$ can be calculated as summarized in Table A-3.

Table A-3. Belief and Plausibility for Elements of $X \times Y$

Element	Belief	Plausibility
$\langle x_1, y_1 \rangle$	0	0.12
$\langle x_1, y_2 \rangle$	0	0.60
$\langle x_1, y_3 \rangle$	0	0.48
$\langle x_2, y_1 \rangle$	0	0.08
$\langle x_2, y_2 \rangle$	0	0.40
$\langle x_2, y_3 \rangle$	0	0.32

Note that unlike degrees of evidence or probability, Plausibility and Belief over the elements do not have to sum to 1.0.

Assume that $x_1 = 1$, $x_2 = 2$, $y_1 = 4$, $y_2 = 3$, and $y_3 = 2$. Let the function of interest on the random vector $X \times Y$ be $z = f(x, y) = x + y$. Table A-4 lists the $\langle x, y \rangle$ tuples and $f(x, y)$ for each tuple.

Table A-4. Tuples and Functional Values

$\langle x, y \rangle$	$z = x + y$
$\langle x_1, y_1 \rangle = \langle 1, 4 \rangle$	5
$\langle x_1, y_2 \rangle = \langle 1, 3 \rangle$	4
$\langle x_1, y_3 \rangle = \langle 1, 2 \rangle$	3
$\langle x_2, y_1 \rangle = \langle 2, 4 \rangle$	6
$\langle x_2, y_2 \rangle = \langle 2, 3 \rangle$	5
$\langle x_2, y_3 \rangle = \langle 2, 2 \rangle$	4

The belief and plausibility for each element of f (each unique z in Table A-4) can be calculated using equation A-14 with the body of evidence previously calculated. Since none of the R is a subset of any $\langle x, y \rangle$ tuple, $\text{Bel}(z) = 0$ for all z . For $z = 5$, the pertinent tuples are $\langle x_1, y_1 \rangle$ and $\langle x_2, y_2 \rangle$. $\langle x_1, y_1 \rangle$ has non-null intersection with R_1 and $\langle x_2, y_2 \rangle$ has non-null intersection with R_3 and R_4 . So from Equation 2-14 $\text{Pl}(x + y = 5) = m(R_1) + m(R_3) + m(R_4) = 0.12 + 0.08 + 0.32 = 0.52$. Similarly, $\text{Pl}(x + y = 3) = m(R_2) = 0.48$, $\text{Pl}(x + y = 4) = m(R_1) + m(R_2) + m(R_4) = 0.92$, $\text{Pl}(x + y = 6) = m(R_3) = 0.08$.

Table A-5 summarizes the functional values, and the belief and plausibility for each value of the function f .

Table A-5. Values, Belief, and Plausibility

$f(x, y) = x + y$	Belief	Plausibility
3	0	0.48
4	0	0.92
5	0	0.52
6	0	0.08

The uncertainty distribution for the function of interest is summarized in Figure A-10.

The body of evidence for $f: X \times Y$ is:

$$\begin{aligned}
 m(\{f(x_1, y_1), f(x_1, y_2)\}) &= m(5, 4) = 0.12 \\
 m(\{f(x_1, y_2), f(x_1, y_3)\}) &= m(4, 3) = 0.48 \\
 m(\{f(x_2, y_1), f(x_2, y_2)\}) &= m(6, 5) = 0.08 \\
 m(\{f(x_2, y_2), f(x_2, y_3)\}) &= m(5, 4) = 0.32
 \end{aligned}$$

so,

$$m(5, 4) = 0.12 + 0.32 = 0.44$$

$$m(4, 3) = 0.48$$

$$m(6, 5) = 0.08$$

Using Equation A-5, the expected value interval for $f:X \times Y$ can be calculated.

$$E^*(f(x, y)) = 4(0.44) + 3(0.48) + 5(0.08) = 3.6, \text{ and}$$

$$E^*(f(x, y)) = 5(0.44) + 4(0.48) + 6(0.08) = 4.6.$$

Figure A-10. Uncertainty Distribution for Example Problem

Belief and Plausibility can be calculated for subsets on the functional values. Consider the subset “values of the function $f:X \times Y$ greater than 3” for the example problem. The tuples of $X \times Y$ that form this subset are: $\langle x_1, y_1 \rangle$, $\langle x_1, y_2 \rangle$, $\langle x_2, y_1 \rangle$, $\langle x_2, y_2 \rangle$, and $\langle x_2, y_3 \rangle$. Using Equation A-20, $C = \{\langle x_1, y_1 \rangle, \langle x_1, y_2 \rangle, \langle x_2, y_1 \rangle, \langle x_2, y_2 \rangle, \langle x_2, y_3 \rangle\}$, and:

$$\text{Bel}(A) = m(R_1) + m(R_3) + m(R_4) = 0.52$$

$$\text{Pl}(A) = m(R_1) + m(R_2) + m(R_3) + m(R_4) = 1.0.$$

For the subset “all values of $f:X \times Y$ ” belief and plausibility are both 1.0 as expected.

A.3.4 Expectation Value for a Function of a Random Vector

The previous sections discussed the convolution process for generating the uncertainty distribution for the values of a function on a random vector, $f: X \times Y \rightarrow \text{Reals}$, for different metrics for uncertainty.

The process for calculating the expected interval of a random variable was also summarized, and for a probability metric the expected value interval simplifies to a point value, the mean.

This section discusses some conditions for which the expected value for the values of the function can be directly calculated from the expected values for the constituent random variables.

For a probability measure with $f(x, y) = x + y$ it can be shown that the expected value for $X + Y$ is the sum of the expected values for X and Y , even if X and Y are not independent. That is, $E[X + Y] = E[X] + E[Y]$ in all cases.

For a probability measure with $f(x, y) = x \cdot y$ it can be shown that the expected value for $X \cdot Y$ is the product of the expected values for X and Y , if X and Y are independent. That is, $E[X \cdot Y] = E[X] \cdot E[Y]$ if X and Y are independent.

As proven in section A.3.4.1, using a belief measure for noninteractive X and Y , $E^*[X + Y] = E^*[X] + E^*[Y]$, and $E^*[X \cdot Y] = E^*[X] \cdot E^*[Y]$. Furthermore, if the domain of X and Y are the *non-negative* reals, then $E^*[X + Y] = E^*[X] + E^*[Y]$, and $E^*[X \cdot Y] = E^*[X] \cdot E^*[Y]$.

A.3.4.1 Expectation Value for Noninteractive X and Y

A.3.4.1.1 $E(X+Y)$, X and Y Noninteractive, X and Y real numbers

Consider random variables X and Y whose values are real numbers, with X and Y noninteractive as defined in Section A.3.3. Under these conditions, it is asserted that:

$$E_*(X + Y) = E_*(X) + E_*(Y) \text{ and } E^*(X + Y) = E^*(X) + E^*(Y).$$

The proof of this assertion follows.

Consider $f(x, y) = x + y$. Following the development in Section A.3.3:

$$\begin{aligned} E_*(X + Y) &= \sum_{\text{all } A_i \times B_j \subseteq X \times Y} \inf \{a + b \mid \langle a, b \rangle \in A_i \times B_j\} * m_X(A_i) * m_Y(B_j) \\ E^*(X + Y) &= \sum_{\text{all } A_i \times B_j \subseteq X \times Y} \sup \{a + b \mid \langle a, b \rangle \in A_i \times B_j\} * m_X(A_i) * m_Y(B_j) \end{aligned} \quad (\text{Eqn. A-23})$$

where A_i and B_j are the focal elements of X and Y , respectively; that is, A_i and B_j are elements of the power set of X and Y with non-zero degrees of evidence. $A_i \times B_j$ is a relation on $X \times Y$.

“sup” is supremum, least upper bound, and “inf” is infimum, greatest lower bound.³⁴ $m_X(A_i)$ and $m_Y(B_j)$ are the projections of $m(A_i \times B_j)$ onto X and Y , respectively. Noninteraction means that $m(A_i \times B_j) = m_X(A_i) \cdot m_Y(B_j)$.

Let $a_{i \inf}$, $b_{j \inf}$, $a_{i \sup}$, and $b_{j \sup}$ be defined as follows:

$$\begin{aligned} a_{i \inf} &\equiv \inf\{a \mid a \in A_i\} \\ b_{j \inf} &\equiv \inf\{b \mid b \in B_j\} \\ a_{i \sup} &\equiv \sup\{a \mid a \in A_i\} \\ b_{j \sup} &\equiv \sup\{b \mid b \in B_j\} \end{aligned} \quad (\text{Eqn. A-24})$$

For any real numbers, positive or negative:

$$\begin{aligned} \inf\{a+b \mid a, b \in A_i \times B_j\} &= a_{i \inf} + b_{j \inf} \\ \sup\{a+b \mid a, b \in A_i \times B_j\} &= a_{i \sup} + b_{j \sup} \end{aligned} \quad (\text{Eqn. A-25})$$

and Equation A-23 can be written as:

$$\begin{aligned} E_*(X+Y) &= \sum_{all A_i \times B_j \subseteq X \times Y} (a_{i \inf} + b_{j \inf}) * m_X(A_i) * m_Y(B_j) \\ E^*(X+Y) &= \sum_{all A_i \times B_j \subseteq X \times Y} (a_{i \sup} + b_{j \sup}) * m_X(A_i) * m_Y(B_j) \end{aligned} \quad (\text{Eqn. A-26})$$

Equation A-26 can be written:

$$\begin{aligned} E_*(X+Y) &= \sum_{all A_i} \sum_{all B_j} (a_{i \inf} + b_{j \inf}) * m_X(A_i) * m_Y(B_j) \\ E^*(X+Y) &= \sum_{all A_i} \sum_{all B_j} (a_{i \sup} + b_{j \sup}) * m_X(A_i) * m_Y(B_j) \end{aligned} \quad (\text{Eqn. A-27})$$

Equation A-27 can be written:

$$\begin{aligned} E_*(X+Y) &= \sum_{all A_i} a_{i \inf} * m_X(A_i) \sum_{all B_j} m_Y(B_j) + \sum_{all B_j} b_{j \inf} * m_Y(B_j) \sum_{all A_i} m_X(A_i) \\ E^*(X+Y) &= \sum_{all A_i} a_{i \sup} * m_X(A_i) \sum_{all B_j} m_Y(B_j) + \sum_{all B_j} b_{j \sup} * m_Y(B_j) \sum_{all A_i} m_X(A_i) \end{aligned} \quad (\text{Eqn. A-28})$$

Since it is required that:

³⁴ Since this section is dealing with discrete sets, inf is equivalent to min and sup is equivalent to max. The conclusions in section A.3.4.1 are valid for focal element that are intervals of real numbers as well as for focal elements that are sets of discrete numbers.

$$\begin{aligned}\sum_{all A_i} m_X(A_i) &= 1 \\ \sum_{all B_j} m_Y(B_j) &= 1\end{aligned}\tag{Eqn. A-29}$$

Equation A-28 simplifies to:

$$\begin{aligned}E_*(X+Y) &= \sum_{all A_i} a_{i \inf} * m_X(A_i) + \sum_{all B_j} b_{j \inf} * m_Y(B_j) \\ E^*(X+Y) &= \sum_{all A_i} a_{i \sup} * m_X(A_i) + \sum_{all B_j} b_{j \sup} * m_Y(B_j)\end{aligned}\tag{Eqn. A-30}$$

Equation A-30 shows that $E_*(X+Y) = E_*(X) + E_*(Y)$ and $E^*(X+Y) = E^*(X) + E^*(Y)$.

Therefore, if the domain of X and Y are the reals and X and Y are noninteractive, $E_*(X+Y) = E_*(X) + E_*(Y)$ and $E^*(X+Y) = E^*(X) + E^*(Y)$.

A.3.4.1.2 $E(X \cdot Y)$, X and Y Noninteractive, X and Y Non-negative Real Numbers

Consider random variables X and Y whose values are *non-negative* real numbers, with X and Y noninteractive as defined in Section A.2.3. Under these conditions, it is asserted that:

$$E_*(X \cdot Y) = E_*(X) \cdot E_*(Y) \text{ and } E^*(X \cdot Y) = E^*(X) \cdot E^*(Y).$$

The proof of this assertion follows.

Consider $f(x, y) = x \cdot y$. Following Section A.3.3:

$$\begin{aligned}E_*(X * Y) &= \sum_{all A_i x B_j \subseteq X \times Y} \inf \{a * b | <a, b> \in A_i x B_j\} * m_X(A_i) * m_Y(B_j) \\ E^*(X * Y) &= \sum_{all A_i x B_j \subseteq X \times Y} \sup \{a * b | <a, b> \in A_i x B_j\} * m_X(A_i) * m_Y(B_j)\end{aligned}\tag{Eqn. A-31}$$

Let $a_{i \inf}$, $b_{j \inf}$, $a_{i \sup}$, and $b_{j \sup}$ be as defined in Equation A-24.

Since we are dealing with non-negative real numbers,³⁵

$$\begin{aligned}\inf \{a * b | <a, b> \in A_i x B_j\} &= a_{i \inf} * b_{j \inf} \\ \sup \{a * b | <a, b> \in A_i x B_j\} &= a_{i \sup} * b_{j \sup}\end{aligned}\tag{Eqn. A-32}$$

and Equation A-31 can be written as:

³⁵ Equation A-32 is not valid if we allow negative numbers in the domain for X or Y.

$$\begin{aligned}
E_*(X * Y) &= \sum_{all A_i x B_j \subseteq X \times Y} (a_{i \inf} * b_{j \inf}) * m_X(A_i) * m_Y(B_j) \\
E^*(X * Y) &= \sum_{all A_i x B_j \subseteq X \times Y} (a_{i \sup} * b_{j \sup}) * m_X(A_i) * m_Y(B_j)
\end{aligned} \tag{Eqn. A-33}$$

Equation A-33 can be written:

$$\begin{aligned}
E_*(X * Y) &= \sum_{all A_i} \sum_{all B_j} a_{i \inf} * b_{j \inf} * m_X(A_i) * m_Y(B_j) \\
E^*(X * Y) &= \sum_{all A_i} \sum_{all B_j} a_{i \sup} * b_{j \sup} * m_X(A_i) * m_Y(B_j)
\end{aligned} \tag{Eqn. A-34}$$

Equation A-34 can be re-written as:

$$\begin{aligned}
E_*(X * Y) &= \sum_{all A_i} a_{i \inf} * m_X(A_i) \sum_{all B_j} b_{j \inf} * m_Y(B_j) \\
E^*(X * Y) &= \sum_{all A_i} a_{i \sup} * m_X(A_i) \sum_{all B_j} b_{j \sup} * m_Y(B_j)
\end{aligned} \tag{Eqn. A-35}$$

Equation A-35 shows that $E_*(X \cdot Y) = E_*(X) \cdot E_*(Y)$ and $E^*(X \cdot Y) = E^*(X) \cdot E^*(Y)$.

Therefore, if the domain of X and Y are the *non-negative* reals and X and Y are noninteractive, $E_*(X \cdot Y) = E_*(X) \cdot E_*(Y)$ and $E^*(X \cdot Y) = E^*(X) \cdot E^*(Y)$.

A.3.4.1.2 Examples

A.3.4.1.2.1 Examples with X and Y Non-Negative

For the example in Section A.3.3, the expected value interval $[E_*(X + Y), E^*(X + Y)]$ was calculated to be $[3.6, 4.6]$. Since X and Y satisfy the requirements for the assertions, the expected value interval can be calculated as $[E_*(X) + E_*(Y), E^*(X) + E^*(Y)]$. Specifically,

$$\begin{aligned}
E_*(X) &= 1 \cdot 0.6 + 2 \cdot 0.4 = 1.4 \\
E^*(X) &= 1 \cdot 0.6 + 2 \cdot 0.4 = 1.4 \\
E_*(Y) &= \min(4, 3) \cdot 0.2 + \min(3, 2) \cdot 0.8 = 2.2 \\
E^*(Y) &= \max(4, 3) \cdot 0.2 + \max(3, 2) \cdot 0.8 = 3.2 \\
\text{and } [E_*(X) + E_*(Y), E^*(X) + E^*(Y)] &= [3.6, 4.6].
\end{aligned}$$

Similarly, for the example in Section 4, the expected value for $(1 - P_E)$ is a probabilistic mean: $0.02 \cdot 0.3 + 0.03 \cdot 0.2 + 0.90 \cdot 0.1 + 0.05 \cdot 0 = 0.102$ and the expected value for C is a probabilistic mean: $0.03 \cdot 10^2 + 0.05 \cdot 10^3 + 0.80 \cdot 10^4 + 0.10 \cdot 10^5 + 0.02 \cdot 10^6 = 3.80 \times 10^4$. The expected value interval for f_A is:

$$\begin{aligned}
E_*(f_A) &= \min(0, 10^{-5}) \cdot 0.70 + \min(0, 10^{-5}, 10^{-4}, 10^{-3}) \cdot 0.15 + \\
&\quad \min(0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}) \cdot 0.15 = 0 \\
E^*(f_A) &= \max(0, 10^{-5}) \cdot 0.70 + \max(0, 10^{-5}, 10^{-4}, 10^{-3}) \cdot 0.15 + \\
&\quad \max(0, 10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}) \cdot 0.15 = 1.657 \times 10^{-3}.
\end{aligned}$$

$$[E_*(1 - P_E) * E_*(C) * E_*(f_A), E^*(1 - P_E) * E^*(C) * E^*(f_A)] = [0, 6.4].$$

By convolution, as summarized in Section A.3.3

$$[E_*(f_A * (1 - P_E) * C), E^*(f_A * (1 - P_E) * C)] = [0, 6.4].$$

A.3.4.1.2.1 Example with X and Y having Negative Values

Consider $X = \{-2, 1, 4\}$ and $Y = \{-6, 0, 5\}$. Let the focal elements of X be:

$\{-2, 1\}$ with $m = 0.6$

$\{1, 4\}$ with $m = 0.4$

Let the focal elements of Y be:

$\{-6, 0\}$ with $m = 0.8$

$\{-6, 0, 5\}$ with $m = 0.2$.

$$E_*(X) = 0.6(-2) + 0.4(1) = -0.8$$

$$E^*(X) = 0.6(1) + 0.4(4) = 2.2$$

$$E_*(Y) = 0.8(-6) + 0.2(-6) = -6.0$$

$$E^*(Y) = 0.8(0) + 0.2(5) = 1.0.$$

Consider $X + Y$.

$$E_*(X) + E_*(Y) = -6.8$$

$$E^*(X) + E^*(Y) = 3.2$$

Using the BeliefConvolution code, $E_*(X+Y) = -6.8$ and

$E^*(X+Y) = 3.2$, so $E_*(X+Y) = E_*(X) + E_*(Y)$ and $E^*(X+Y) = E^*(X) + E^*(Y)$.

Consider $X \cdot Y$.

$$E_*(X) \cdot E_*(Y) = 4.8$$

$$E_*(X) \cdot E^*(Y) = -0.8$$

$$E^*(X) \cdot E_*(Y) = -13.2$$

$$E^*(X) \cdot E^*(Y) = 2.2.$$

Using the BeliefConvolution code,

$$E_*(X \cdot Y) = -13.68 \text{ and } E^*(X \cdot Y) = 8.8, \text{ so}$$

$E_*(X \cdot Y) \neq E_*(X) \cdot E_*(Y)$ and $E^*(X \cdot Y) \neq E^*(X) \cdot E^*(Y)$ where E^* denotes either E_* or E^* to account for the product of two negative numbers being positive.

A.3.5 Convolution with Fuzzy Sets

The discussion of convolution in Sections A.3.1 through A.3.4 assumed crisp sets. Convolution can also be performed with fuzzy sets. The following discussion is from Yager, for convolution using the belief/plausibility measure given evidence on fuzzy sets defined by degrees of membership on the reals. [Yager 1986]

Let OP denote any arithmetic operation on real numbers (addition, subtraction, multiplication, division, exponentiation). Let $Z = X \text{ OP } Y$ and let S be a subset of Z. Let A_i and B_j denote the i^{th} and j^{th} focal elements of X and Y, respectively, and assume the focal elements are noninteractive:

$$m(S) = \sum_{\substack{i,j \\ A_i \text{ OP } B_j = S}} m(A_i) \bullet m(B_j) \quad (\text{Eqn. A-36})$$

If A_i and B_j are fuzzy sets, OP is defined as

$$Z = A_i \text{ OP } B_j \quad (\text{Eqn. A-37})$$

where for any real number z

$$Z(z) = \max_{\substack{\text{all } x,y \\ \text{such that} \\ x \text{ OP } y = z}} \{\min[\mu_{A_i}(x), \mu_{B_j}(y)]\} \quad (\text{Eqn. A-38})$$

For the special case of A_i and B_j crisp:

$$Z = \{x \text{ OP } y \mid \text{for } x \in A_i \text{ and } y \in B_j\} \quad (\text{Eqn. A-39})$$

The paper by Yager also addresses operations that are not arithmetic. [Yager 1986]

A.3.6 Linguistic Convolution

This section summarizes a technique for the evaluation of purely linguistic information using a belief measure.

In this approach, X and Y are modeled to a level of detail consistent with the fidelity of the information available. For example if X is the number of deaths from a terrorist attack, we may chose to bin X into subsets such as “Minor,” “Moderate,” “Major,” and “Catastrophic.” Also, we may not have a precise definition of each set; for example, “Major” may be defined as “between about 500 and about 5000 deaths.” Given fuzzy sets defined with degrees of membership over the reals, the techniques of Section A.2.7 can be used to evaluate belief/plausibility for any fuzzy set of concern, and the techniques of Section A.3.5 can be used to evaluate belief/plausibility for arithmetic operations on fuzzy sets defined over the reals.

However, as discussed in Section 1, for our application we have variables whose fuzzy sets are purely linguistic, such as the variable Y being “Damage to National Security” modeled with, for example, the fuzzy sets “Not Much,” “Of Concern,” and “Yes.” These fuzzy sets are purely linguistic and do not have degrees of membership defined over the reals.

In the linguistic model, X and Y do not have to be expressed using numbers, and the fuzzy sets for X and Y are purely linguistic, not defined by degrees of membership over numerical values of X and Y . That is, the fidelity of the model is at the fuzzy set level. A random vector $Z = X \times Y$ is also described by purely linguistic fuzzy sets, and a function for Z is defined by an approximate reasoning rule base.

Evidence is over the fuzzy sets in X and Y. A focal element for X is of the form $[A_i, m(A_i)]$ where A_i is an element of the fuzzy power set of X,³⁶ $m(A_i)$ is the evidence assigned to A_i , and i ranges over all the focal elements for X. Similarly, a focal element for Y is of the form $[B_j, m(B_j)]$ where B_j is subset of the set of all fuzzy sets of Y, $m(B_j)$ is the evidence assigned to B_j , and j is over all the focal elements for Y. Assuming noninteraction, $m(A_i \times B_j) = m_X(A_i) \cdot m_Y(B_j)$.

From the rule base, a given fuzzy set for Z, call it C_m , is of the form $C_m = \bigcup_{i,j \text{ per rules}} \{ \langle F_i, G_j \rangle \}$

where F_i and G_j are fuzzy sets of X and Y, respectively, and $\langle \rangle$ denotes a tuple. Both the evidence and the rules are at the fuzzy set level; all the A_i , B_j , and C_m are comprised of fuzzy sets from the fuzzy sets of X and Y. Since we are reasoning at the fuzzy set level without definitions for degrees of membership for the fuzzy sets, the mathematics of Section A.2.7 cannot be used in the evaluation of rules. The standard Equation A-4 for belief/plausibility is used; that is, the fuzzy sets are fuzzy in the assignment of evidence, but are treated as crisp in the evaluation of the rule base.

Section 3.3 provides a simple example of linguistic convolution.

A.4 Belief for Focal Elements as Intervals of Real Numbers

The previous sections of this appendix focused on evaluation of uncertainty for a variable that has a discrete number of values. A similar approach can be used for a variable whose value is any real number over an interval, if degrees of evidence are assigned to a finite number of intervals within the domain of the variable. [Oberkampf and Helton]

If the intervals to which degrees of evidence are assigned are point values (degenerate intervals) then both belief and plausibility reduce to probability.

Section 3.2 provides a simple example of belief where evidence is assigned to intervals.

A.5 Summary

This appendix discussed the modeling of uncertainty using a set of values and an uncertainty distribution over that set. Two types of uncertainty were discussed: ambiguity and vagueness. A general measure for ambiguity was presented: belief/plausibility. For ambiguity involving strife with no nonspecificity, belief/plausibility both become probability. For a consonant body of evidence, belief/plausibility become necessity/possibility, respectively.

Convolution of random variables using the following measures was discussed: probability, possibility, and belief. Linguistic convolution using an approximate reasoning rule base was also discussed.

The concept of fuzzy sets for vagueness was discussed. Extension (“fuzzification”) of probability, possibility, and belief to also include vagueness were summarized.

³⁶ For example if the fuzzy sets for X are “bad” and “good,” the fuzzy power set for X is $\{ \{ \text{null} \}, \{ \text{“bad”} \}, \{ \text{“good”} \}, \{ \text{“bad,” “good”} \} \}$, and one possible A_i is $\{ \text{“bad,” “good”} \}$.

This page intentionally left blank.

Appendix B. Probability and Uncertainty

This appendix discusses the two uses of the term “Probability.” Consider a variable that is itself a probability, such as the “probability that a sensor detects an intrusion.” This probability is a frequency, the fraction of intrusion attempts that are detected, and has uncertainty due to the inability to perform an infinite number of tests to precisely know the probability (frequency). Uncertainty in the probability (frequency) can also be expressed as a probability (state of knowledge); hence, we have the conundrum of a “probability of a probability.” The confusion is resolved by understanding that **the same name “probability” is used for two different concepts: a frequency and a state of knowledge.** [Kaplan and Garrick] As Kaplan states, “We shall, therefore, assign each idea the dignity of its own name.” Kaplan uses frequency to denote the classical measure of the probability of any event of interest, subsequently presented in Equation B-1. He reserves the name probability to mean state of knowledge in the Bayesian sense, as he states: “What the objectivists are talking about we shall call ‘frequency.’ What the subjectivists are talking about we shall call ‘probability’.”

A variable that is a probability (Kaplan’s frequency) can be treated as a special case of a random variable and the uncertainty in the probability (Kaplan’s frequency) is a probability (state of knowledge) distribution over the possible values of the probability (Kaplan’s frequency).³⁷

This appendix discusses the following for a discrete case: the connection between probability and a sample space using the properties of a probability measure, a random variable, the two meanings of probability, and aleatory and epistemic uncertainty. The appendix also briefly discusses other measures for state of knowledge besides probability such as belief/plausibility.

B.1 Probability as a Frequency

The classical definition of probability is the frequency definition, or the objective definition. With this definition the probability of an event is the fraction of times that an event occurs. More precisely, **probability as a frequency** is defined as

$$P(E) \equiv \lim_{N \rightarrow \infty} \frac{X(N)}{N} \quad (\text{Eqn. B-1})$$

where $X(N)$ is the number of times an event E occurs from a total of N trials. $P(E)$ is a non-negative real number in the interval $[0, 1]$.

Probability as defined by Equation B-1 is what Kaplan calls a frequency. Note that this frequency is dimensionless; it is a ratio of the number of times an event of interest happens divided by the number of times that event could happen (the number of trials), in the limit as the number of trials is infinite. The event can be any event of interest, such as “total precipitation in Albuquerque exceeding the equivalent of 3 inches of water in the month of July.”

³⁷ Probability as a frequency will be denoted as probability (Kaplan’s frequency) and probability as a state of knowledge will be denoted as probability (state of knowledge). The modifier “Kaplan’s frequency” is used to emphasize that this is not a frequency in the engineering sense, a variable with dimensions of inverse time, but is the frequency definition of probability.

The classical probability (Kaplan's frequency) is dimensionless; it is **not** a rate in the engineering sense, such as a number of occurrences per year, but it can be used to describe a random variable that is a rate in the engineering sense. Let the random variable of interest, f , be defined as "the number of earthquakes in Asia per year."³⁸ Consider the event of interest "less than 3 earthquakes per year," and denote this event as $f_{<3}$. Using Equation B-1,

$$P(f_{<3}) \equiv \lim_{\text{Number of years} \rightarrow \infty} \frac{\text{Number of years with less than 3 earthquakes}}{\text{Number of years}}$$

We wish to evaluate probabilities (frequencies) such as $P(E)$, $P(E \cup F)$, and $P(E \cap F)$ where E and F are events and $\cup$ and $\cap$ are union and intersection, respectively.

B.2 Aleatory and Epistemic Uncertainty

$P(E)$ provides an estimate of the likelihood that event E will occur; for any given trial, event E may or may not occur, but is more likely to occur the higher its probability. Even if $P(E)$ is precisely known, the occurrence of event E in the future is uncertain. There is aleatory (or stochastic or random) uncertainty for the event reflected by its probability $P(E)$. Most elementary texts on probability assume $P(E)$ is known and model $P(E)$ as a point value with no uncertainty in that value. To know $P(E)$ exactly we would have to perform an infinite number of trials, which is impossible. Therefore, no matter what information we have, there is uncertainty in $P(E)$. The uncertainty in $P(E)$ depends on epistemic (or state of knowledge) uncertainty. The uncertainty in $P(E)$ can be expressed using probability, hence the two meanings of probability, a frequency and a state of knowledge. When used in the objective (frequency) sense, probability means the fraction of occurrences from a (infinite) number of tests. When used in the subjective (state of knowledge) sense, probability means likelihood based on the information available.

One justification for using the name probability for both concepts is that **both probability as a frequency and probability as a state of knowledge are axiomatically a "probability measure," even though these two uses for probability do not have the same meaning.**³⁹ A probability measure provides the mathematical framework for working with probability whether that probability is used to mean either a frequency or a state of knowledge. Section B.3 discusses a probability measure.

When uncertainty in $P(E)$ is expressed as a probability distribution, that distribution is based on all the information available and includes both aleatory and epistemic types of uncertainty. For example, the value for $P(E)$ observed from test data is the mean of a probability distribution for $P(E)$. **So, we will broaden our understanding of "state of knowledge" to include aleatory as well as epistemic uncertainty as all information available contributes to our state of knowledge.**

³⁸ In practice, only earthquakes with a magnitude above a specified minimum level are counted because the large number of low-intensity earthquakes are not of concern since they cause no damage.

³⁹ Here, Probability Measure means the Kolmogorov development of probability.

An example of aleatory uncertainty is the outcome from tossing a fair coin known to have a heads and a tails side. An example of epistemic uncertainty is the coin may be two-headed or two-tailed. An example with both aleatory and epistemic uncertainty is a heads/tails coin believed to be unfair (e.g., more likely to produce heads than tails).

Epistemic uncertainty can be reduced by gathering more information, aleatory uncertainty cannot.

Consideration of epistemic uncertainty will be discussed in Section B.4; for now, we assume $P(E)$ is known with certainty, and until Section B.4 the term “probability” will mean probability (Kaplan’s frequency).

B.3 Probability Measure for a Sample Space

A probability measure is a function on the events (subsets) of a sample space with certain properties. A sample space S is a set of **all unique** (mutually exclusive) possible outcomes. An event E is a subset of a sample space. Let s denote an element (outcome) of S . Since the set containing the single element s is a subset of S , a unique outcome is also an event, sometimes called an elementary event. Let $\cup$ denote set union (OR) and $\cap$ denote set intersection (AND). Two events E_1 and E_2 are mutually exclusive if $E_1 \cap E_2 = \text{null}$.

A probability measure, P , is **not** the sample space; it is a mapping of the events of S to the set of non-negative real numbers with the following properties (axioms of a probability measure):

1. For any event E , $0 \leq P(E) \leq 1$
2. $P(S) = 1$
3. For any two mutually exclusive events E_1 and E_2 , $P(E_1 \cup E_2) = P(E_1) + P(E_2)$.⁴⁰

The third property is called the “additive” property of probability.

From these three properties for a probability measure we can derive all the standard equations for evaluating probabilities of events.

For example, for any two events E_1 and E_2 in S , $P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$. If E_1 and E_2 are independent, $P(E_1 \cap E_2) = P(E_1) * P(E_2)$. Let E^C denote the complement of E ; E^C is sometimes written as $S - E$ and E^C contains all the elements of S not in E . $E_1 - E_2$ denotes the set of outcomes in E_1 not in E_2 .

⁴⁰ For example, consider $S = \{a, b, c\}$ and define E_1 as $\{a, b\}$ and E_2 as $\{b, c\}$. E_1 and E_2 are not mutually exclusive since they share element b . Define E_3 as $\{c\}$; E_1 and E_3 are mutually exclusive. All elementary events, e.g., $\{a\}$, $\{b\}$, and $\{c\}$, are mutually exclusive of each other.

For two events E_1 and E_2 , the probability of E_1 given E_2 is the probability of E_1 conditional on E_2 and is denoted as $P(E_1|E_2)$. For $P(E_2) > 0$, $P(E_1|E_2) = P(E_1 \cap E_2) / P(E_2)$. E_1 is independent of E_2 if $P(E_1|E_2) = P(E_1)$, and for independence $P(E_1 \cap E_2) = P(E_1) * P(E_2)$.

Once we know the probability over all the elements of a sample space, we can calculate the probability for any event or combinations of events in the sample space using the properties of a probability measure without specific consideration of the sample space; however, the sample space is always implicitly present.

B.3.1 Example of Probability for Events in a Sample Space

Consider the following example. Let A denote one component and B another component. Let A_W denote the outcome that A “works” (functions on demand) and let A_F denote the outcome that A fails. Similarly, B_W and B_F denote the outcome that B works and fails, respectively. Assume we know the probability for the elements of A and B ; specifically, we are given $P(A_F)$ and $P(B_F)$, and since $A_W = A_F^C$ and $B_W = B_F^C$, $P(A_W) = 1 - P(A_F)$ and $P(B_W) = 1 - P(B_F)$.

We wish to calculate the probability of the event “ A fails or B fails.”

Without explicit consideration of the sample space for A combined with B we know that $P(A_F \cup B_F) = P(A_F) + P(B_F) - P(A_F \cap B_F)$ from the mathematics of probability. Furthermore, if A_F and B_F are independent, $P(A_F \cup B_F) = P(A_F) + P(B_F) - P(A_F) * P(B_F)$, and we can easily calculate the probability of failure of A or B .

So, from direct application of the mathematics of a probability measure we have

$$P(A_F \cup B_F) = P(A_F) + P(B_F) - P(A_F \cap B_F). \quad (\text{Eqn. B-2})$$

without explicit consideration of the sample space.

What is the sample space? The sample space is the set of all unique outcomes for combinations of A and B . $S_A = \{A_W, A_F\}$ is the sample space for component A . Similarly, $S_B = \{B_W, B_F\}$ is the sample space for component B . The sample space for both A and B is the Cartesian product $S_A \times S_B = \{<A_W, B_W>, <A_W, B_F>, <A_F, B_W>, <A_F, B_F>\}$.⁴¹

The event “ A fails or B fails” is the following subset of the sample space of $S_A \times S_B$: $\{<A_W, B_F>, <A_F, B_W>, <A_F, B_F>\}$. The probability of the event “ A fails or B fails” is:

$$P(\text{“}A \text{ fails or } B \text{ fails”}) = P(\{<A_W, B_F>, <A_F, B_W>, <A_F, B_F>\}).$$

⁴¹ $\langle \rangle$ denotes a tuple; for a tuple the order of the elements matters. Here the first element of the tuple is an element of S_A and the second element of the tuple is an element of S_B .

Since the elements (tuples) of $A \times B$ are always mutually exclusive, by the additive property of a probability measure $P(\text{"A fails or B fail"}) = P(\{<A_W, B_F>\} + P(\{<A_F, B_W>\} + P(\{<A_F, B_F>\} = P(A_W \cap B_F) + P(A_F \cap B_W) + P(A_F \cap B_F)$.⁴²

So, from explicit consideration of the sample space we have

$$P(\text{"A or B fail"}) = P(A_W \cap B_F) + P(A_F \cap B_W) + P(A_F \cap B_F). \quad (\text{Eqn. B-3})$$

Equations B-2 and B-3 are equivalent. Since $P(A \times B) = 1$, $P(A_W \cap B_F) + P(A_F \cap B_W) + P(A_F \cap B_F) + P(A_W \cap B_W) = 1$, and Equation B-3 can be written $P(\text{"A fails or B fail"}) = 1 - P(A_W \cap B_W) = 1 - (1 - P\{(A_W \cap B_W)^C\}) = 1 - (1 - P(A_F \cup B_F)) = P(A_F \cup B_F)$ which is Equation B-2.⁴³

B.3.2 Simple Examples of Dependence

Consider a sample space S . Consider with two events X and Y on the sample space. The probability of X or Y is $P(X \cup Y) = P(X) + P(Y) - P(X \cap Y)$. The probability of X and Y is $P(X \cap Y)$. Given sufficient information, $P(X \cap Y)$ can be calculated from a conditional probability. For example, $P(X|Y) = P(X \cap Y)/P(Y)$.

If X and Y are independent, $P(X \cap Y) = P(X) * P(Y)$. To illustrate some extreme cases of dependence, consider the simple sample space $S = \{a, b, c, d\}$ with events X and Y .

If X and Y are mutually exclusive, $X \cap Y = \text{null}$ and $P(X \cap Y) = 0$. For example, $X = \{a, b\}$ and $Y = \{c, d\}$.

If X implies Y (if X then Y), X is a subset of Y , and $P(Y|X) = 1$ and $P(X \cap Y) = P(X)$. Also, $P(X|Y) = P(X) / P(Y)$. For example, $X = \{a, c\}$ and $Y = \{a, c, d\}$.

Consider a situation where part of X is common with Y . For example, $X = \{a, c\}$ and $Y = \{b, c\}$. $X \cap Y = \{c\}$ and $X \cup Y = \{a, b, c\}$. $P(X \cap Y) = P(c)$ and $P(X \cup Y) = P(a) + P(b) + P(c)$, or equivalently, $P(X \cup Y) = P(X) + P(Y) - P(c)$.

Consider a situation where identical components A and B have a common mode failure, such as a common design flaw or failure due to a common environmental threat such as a flood. Let C denote the common mode failure and let A_{IF} and B_{IF} denote the independent failures for A and B , respectively. A_{IF} and B_{IF} are independent.

$$\begin{aligned} P(A \text{ fails and } B \text{ Fails}) &= P[(A_{IF} \cup C) \cap (B_{IF} \cup C)] = P[(A_{IF} \cap B_{IF}) \cup C] = \\ &= P(A_{IF}) * P(B_{IF}) + P(C) - P(A_{IF}) * P(B_{IF}) * P(C). \end{aligned} \quad (\text{Eqn. B-4})$$

Assume $P(A_{IF}) = P(B_{IF})$ which is reasonable for identical components, and denote this independent failure probability as P_I . Define P_T as $P_I + P(C)$, and define the common mode

⁴² The outcomes in the sample space for A and B must be unique; thus, the outcomes in the sample space for $A \times B$ are unique.

⁴³ $(E_1 \text{ op } E_2)^C = E_1^C \text{ op }^C E_2^C$ where op is $\cup$ or $\cap$, and op^C is $\cap$ or $\cup$, respectively; this is DeMorgan's law.

fraction β as $P(C) / P_T$. With these definitions, $P(C) = \beta * P_T$ and $P_I = (1 - \beta) * P_T$, and Equation B-4 becomes:

$$P(\text{A fails and B Fails}) = (1 - \beta)^2 * P_T^2 * (1 - \beta * P_T) + \beta * P_T$$

which is the standard formula for failure of a one-of-two system of identical components with a common mode failure expressed as a beta factor.

B.4 Random Variable

The prior discussion summarized the concept of probability as a point-estimate frequency, the properties of a probability measure as a function on the sample space, and how to calculate the probability of combinations of events using a probability measure. This discussion assumed that the probability (Kaplan's frequency) for an event is precisely known. The probability (Kaplan's frequency) is never precisely known due to epistemic uncertainty. To consider epistemic uncertainty, we can assign a probability (state of knowledge) distribution over the possible values for $P(E)$. As discussed in Section B-1, in practice state of knowledge includes all uncertainty, aleatory and epistemic.

The epistemic uncertainty is ignored in many elementary uses of probability, thereby implicitly assuming that there is sufficient information to know $P(E)$ with certainty. But, for many applications, it is not possible to perform tests to know $P(E)$ with any precision. For example, event E may be terrorists attacking Hoover Dam within the next five years, and we wish to estimate $P(E)$, the probability (Kaplan's frequency) of that event. For such events, we cannot consider $P(E)$ as a point value and must consider the uncertainty in $P(E)$.

To consider uncertainty for a variable that is itself a probability (Kaplan's frequency), probability (Kaplan's frequency) can be considered as a random variable and combinations of probabilistic events can be considered as convolution of a function of a random vector using the mathematics of a probability measure.

A random variable is a mapping of the sample space to the set of reals. [Dougherty] Therefore, a random variable is a real valued function with uncertainty as to its exact value. For example, time to failure is a random variable over $[0, \infty]$. The uncertainty for a random variable is expressed as a probability distribution over the range of the function. We can treat $P(E)$, probability as a frequency, as a random variable over $[0, 1]$. **$P(E)$ is a random variable, the frequency of occurrence of event E; $P(E)$ is not the probability (state of knowledge) distribution of a random variable E.**

Unless probability is written as “probability (Kaplan's frequency),” the term “probability” will mean state of knowledge for the remainder of this Appendix.

This section and Section B.4.1 address probability distributions for a random variable; Section B.4.2 discusses the special case of interest where the random variable is a probability (Kaplan's frequency).

Uncertainty for a random variable can be expressed as a probability distribution over the values of the variable. As previously discussed, the probability distribution considers epistemic uncertainty as well as aleatory uncertainty, as indicated in subsequent examples.

The random variable provides a “transformed” sample space that can be used in lieu of the actual sample space. For example, consider tossing a fair coin twice, with a sample space {<Heads, Heads>, <Tails, Tails>, <Heads, Tails>, <Tails, Heads>}. A random variable is the number of heads with the following sample space on the reals: {0, 1, 2}.

The probability of subsets of the range of a random variable is equivalent to the probability of an event in the sample space. Let S represent a sample space with elementary events s . For any event E in S , a probability is a mapping $P: E \rightarrow \text{Reals}$ that obeys the properties of a probability measure as previously discussed. Let X be a random variable for S ; by definition, $X: S \rightarrow \text{Reals}$. Let B be a set of real numbers. $P(B)$ is the probability that X is in the set B ; $P(B) = P(E_B)$ where E_B is *the* event in S containing all s such that $X(s) \in B$.

For the mapping X , the set S is the domain, the set of Reals is the codomain, and the set of values $X(S)$ is the range.⁴⁴ Let r be an element of the range. For a discrete random variable, given a probability distribution $P(r)$, $P(B)$ can be calculated as the sum of the constituent $P(r)$, since the r values are mutually exclusive per the requirement of a sample space.

Functions of a random variable can be evaluated. Let $f(x)$ be a function of x , and let $y = f(x)$. Let x denote a particular value of a discrete random variable X . $Y = f(X)$ is a random variable with a particular value y .

$$P(y) = \sum_{\text{all } x \text{ where } f(x)=y} P(x). \quad (\text{Eqn. B-5})$$

A random vector extends the concept of a random variable to joint combinations of random variables. Let X and Y be two random variables over a common sample space;⁴⁵ (X, Y) is a random vector for joint combinations of X and Y . Let x be a value for X and y a value for Y . The probability of the joint occurrence of (x, y) is $P(x, y)$. If X and Y are independent, $P(x, y) = P_X(x) * P_Y(y)$, where $P_X(x)$ and $P_Y(y)$ are marginal probabilities (specifically, $P_X(x)$ is sum of $P(x, y)$ over all y).

Functions of a random vector can be defined, such as $X + Y$, $X * Y$, etc. Let $f((X, Y))$ denote a function of the random vector (X, Y) , and let z denote a specific value for $f(X, Y)$.

⁴⁴ Let T and V be two nonempty sets. A function f from T into V , denoted as $f: T \rightarrow V$, is a rule that assigns to every element in T a unique element in V . T is the domain of the function and V is the codomain of the function. The set $f(T)$ is the range of the function. The range is a subset of the codomain. For example, let $f: \text{Reals} \rightarrow \text{Reals}$ be defined as $f(x) = x^2$; the domain is the Reals, the codomain is the Reals, and the range is the set of all nonnegative numbers. [Balakrishnan]

⁴⁵ The sample space may be a Cartesian product of other sample spaces; for example, the sample space $S_A \times S_B$ discussed in the example in Section A.3.1.

$$P(z) = \sum_{\text{all } (x,y) \text{ where } f(x,y)=z} P(x,y) \quad (\text{Eqn. B-6})$$

where $P(x, y)$ is the joint probability for (x, y) .

Convolution is a process by which the probability distributions for X and Y are combined to provide a probability distribution for $f(X, Y)$. For example, for independent X and Y , convolution is accomplished by the formula $P(z) = \sum_{\text{all } (x,y) \text{ where } f(x,y)=z} P_X(x) \cdot P_Y(y)$.

For example, the probability distribution for the sum of two random variables $X + Y$ is the convolution of the probability distributions for X and Y under the algebraic addition operation. Under addition $f(x, y) = x + y$ in Equation B-6. The probability distribution for the product of two random variables $X * Y$ is the convolution of the probability distributions for X and Y under the algebraic multiplication operation. Under multiplication $f(x, y) = x * y$ in Equation B-6.

B.4.1 Examples of Probability Distributions for a Discrete Random Variable

When assigning a probability distribution for a discrete random variable, the analyst attempts to include epistemic uncertainty as well as aleatory uncertainty. For discrete distributions, each value r (a real number) for a random variable has a probability $P(r)$, and $P(r)$ over all r is the probability distribution. (For continuous distributions a probability density function $p(r)$ is defined where $p(r)dr$ is the probability that the value of the random variable is in the differential interval $[r, r + dr]$.)

For example, assume that a bag has two marbles, red and blue. The random variable, X , of interest is the number of red marbles selected when one marble is pulled from the bag, **with replacement**. Consider the sample space to be {blue, red} and define the random variable as the number of red marbles selected. For the random variable, the sample space is {0, 1} where 0 corresponds to blue and 1 corresponds to red. The uncertainty of selecting a red marble is purely aleatory, and $P(X = 0)$ is 1/2 and $P(X = 1)$ is 1/2.

However, assume the bag may have either two red marbles, or both a red and blue marble. This involves epistemic uncertainty as well as aleatory uncertainty. **Assuming** equal probabilities for the two cases, (red, red) has a probability 1/2, and (red, blue) has a probability 1/2.⁴⁶ $P(X = 0) = 1/2 * 1/2 = 1/4$. $P(X = 1) = 1/2 * 1 + 1/2 * 1/2 = 3/4$.

Consideration of epistemic uncertainty changes the probability distribution.

Assume we do two trials and draw a red marble both times; this indicates the bag may have two red marbles but two trials are not much information. For this example, we choose to assign $P(X = 1) = 5/8$ and $P(X = 0)$ of 3/8.⁴⁷

⁴⁶ The assumption of equal probability for either case illustrates a problem with using probability to consider epistemic uncertainty. This is discussed in Section 3.1.3.

⁴⁷ A Bayesian update could be used to update the probability distribution based on new information.

Assume we do two trials and draw a blue marble in one or both trials. We know the bag contains both a red and a blue marble, and we assign a $P(X = 1) = 1/2$ and $P(X = 0) = 1/2$.

B.4.2 Probability (Kaplan's Frequency) as Random Variable

As previously discussed, $P(E)$ is a probability (Kaplan's frequency). With complete information, $P(E)$ is known with certainty and is a point estimate value. It is impossible to know $P(E)$ with certainty as that requires an infinite number of tests (Equation B-1) which is another way of saying complete information cannot be obtained.

To consider epistemic uncertainty in $P(E)$, we can treat $P(E)$ as a random variable over $[0, 1]$ and assign a probability distribution to $P(E)$. Our state of knowledge uncertainty in $P(E)$ is reflected by modeling $P(E)$ with a probability distribution instead of a point estimate, and the probability distribution considers both aleatory and epistemic uncertainty. Here the random variable itself is a probability (Kaplan's frequency).

For example, for event E , assume that we have an estimate of the probability (Kaplan's frequency) of E as 0.2, from 2000 failures in 10,000 trials. Based on our state of knowledge (number of tests, similarity of E with other events for which we have information, expert judgment, etc.) assume we select a uniform probability distribution (subjective) for $P(E)$ over $[0.18, 0.22]$ with mean 0.2.⁴⁸

Suppose that instead of 10,000 tests, we ran 100 tests (due to cost constraints) and observed 20 failures. Our probability (frequency) is 0.2 as before, but we are less confident in that value. Due to smaller sample size in the test, we assign a broader uniform probability distribution (subjective) for $P(E)$, say $[0.1, 0.3]$ with mean 0.2.

We can evaluate the probability distribution for a combination of probability (Kaplan's frequency) events by considering each event as a random variable and convoluting the combinations of random variables using the appropriate probabilistic function, e.g., union or intersection.

For example, for two events A and B the probability (Kaplan's frequency) of A OR B is $P(A \cup B) = P(A) + P(B) - P(A \cap B)$, and for independent events $P(A \cup B) = P(A) + P(B) - P(A)*P(B)$. Our state of knowledge uncertainty is considered by assigning probability distributions for $P(A)$ and $P(B)$ and uncertainty in the probability (Kaplan's frequency) of A OR B is calculated by convoluting these probability distributions for the function $P(A) + P(B) - P(A)*P(B)$, assuming independent events.

⁴⁸ The observed $P(E)$ is the best estimate of $P(E)$ and this value is the mean of a likelihood distribution for $P(E)$. As mentioned earlier, a Bayesian update can be used to update the probability distribution based on more information.

B.5 Non-probabilistic Measures for Uncertainty

The use of probability as a frequency to reflect aleatory uncertainty is not controversial. The use of probability to include epistemic uncertainty is controversial for situations in which the information available is nonspecific; less precise measures of uncertainty such as belief/plausibility and necessity/possibility were developed to better represent epistemic uncertainty.

Probability is a special case of belief/plausibility. Measures such as belief/plausibility and necessity/possibility have properties different from the properties of probability, and the mathematics of convolution are different. Appendix A summarizes belief/plausibility and necessity/possibility measures of uncertainty.

Section B.4.1 discussed an example with epistemic uncertainty, the drawing of a red marble from a bag, with replacement, that may contain either two red marbles, or one red and one blue marble. To assign a probability distribution for this case, it was *assumed* that there is equal likelihood that the bag contains either two red marbles, or a red and a blue marble; however, the information available does not support this assumption and the assumption artificially reduces the epistemic uncertainty. Section 3.1.3 addresses this example using belief/plausibility.

To calculate a belief/plausibility distribution for a function of a random vector, belief/possibility distributions are assigned to each constituent random variable and are convoluted as dictated by the functional relational among the random variables.

For example, the probability (frequency) of $A \cup B$ is given by the function $P(A \cup B) = P(A) + P(B) - P(A)*P(B)$ assuming A and B are independent regardless of the measure of uncertainty used for A and B. But, the assignment of belief/plausibility distributions for P(A) and P(B) and the mathematics for convolution of these distributions for this function are different from the assignment and convolution of probability distributions.

Appendix C. Evaluation of P_E with Belief/Plausibility

This appendix provides a discussion of the evaluation of the effectiveness of a physical security system using belief/plausibility as the measure of uncertainty. In Sections C.1 through C.4, the physical security system is the collection of protection elements at the target of concern designed to counter the attack phase of a scenario. Section C.5 discusses how to include the effectiveness of protection elements outside the target of concern, specifically the effectiveness of intelligence-gathering efforts to detect the formulation phase of a scenario.

C.1 Traditional Equation for Conditional Risk

The traditional equation for conditional risk, CR, for a physical security system is:

$$CR = (1 - P_E) \times C \quad (\text{Eqn. C-1})$$

where P_E is the effectiveness of the security system in detecting and defeating a specific threat scenario and C is the consequence, given failure to defeat the threat scenario. The risk is conditional on the attack since CR assumes that the threat scenario will occur.

For a specific path for a specific threat scenario, P_E is evaluated as:

$$P_E = \sum_{i=1}^m \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_{N_i} \quad (\text{Eqn. C-2})$$

where i ranges over the m layers of the security elements, P_{D_i} is the probability of detection at the i^{th} layer, and P_{N_i} is the probability of neutralization given detection at the i^{th} layer.

C.2 Evaluation of P_E

C.2.1 Point Estimate of P_E with Fixed P_N

For some analyses of security systems, it is assumed that the probability of neutralizing the adversary is a constant, given sufficient time to respond; that is, the effectiveness of response is assumed to be independent of where the response force must respond to. With this assumption, and using point estimate values for the variables in equation C-2, the concept of a Critical Detection Point (CDP) is useful. The CDP can be defined as that specific k^{th} layer for which the guard force has sufficient time to interrupt the adversary, assuming the adversary minimizes delay from that point forward, where for layer $k+1$ the guard force does not have time to interrupt the adversary. Thus, P_{N_i} is a constant for any layer i up to k and is zero for any layer i from $k+1$ to m . Detection at or before the k^{th} layer is critical as detection following that layer is useless since there is insufficient time to respond. Let P_N denote the constant value of P_{N_i} for i less than $k+1$. Using these assumptions equation C-2 simplifies to:

$$P_E = \sum_{i=1}^k \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_N \quad (\text{Eqn. C-3})$$

where k is the CDP.

C.2.2 Generalization of Equation for P_E

To facilitate the extension of P_E to more complicated cases, we need to model P_{Ni} to greater detail. For effective neutralization (given detection), the guard force must:

- correctly assess the situation (decide that the detection is not a false/nuisance alarm or a diversion, etc.),
- have sufficient time to interrupt the adversary before the adversary completes the attack,
- and engage and defeat the adversary.

Let P_{ASSESS_i} be the probability that the guard force correctly assesses the threat scenario given detection at layer i , Let P_{TD_i} denote the probability of timely detection at layer i , defined to be the probability that the guard force can respond in time given detection at layer i . P_{TD_i} is a function of T_{ADV_i} and T_{GR_i} , where T_{ADV_i} is the time for the adversary to complete the scenario from layer i and T_{GR_i} is the time for the guards to respond given detection at layer i , including the time required for assessment. Let P_{WIN_i} be the probability that the guard force defeats the adversary given they engage the adversary given detection at layer i . With these definitions we can express P_{Ni} as:^{49, 50}

$$P_{N_i} = P_{ASSESS_i} \times P_{TD_i} \times P_{WIN_i} \quad (\text{Eqn. C-4})$$

Equation C-2 can be written as:

$$P_E = \sum_{i=1}^m \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_{ASSESS_i} P_{TD_i} P_{WIN_i} \quad (\text{Eqn. C-5})$$

If we use point value estimates for each variable, and assume that P_{Ni} is a constant P_N , P_{TD_i} is 1.0 for any layer i at or before the CDP at layer k , and P_{TD_i} is 0.0 for any layer beyond the CDP.

C.2.3 Point Estimate of P_E with Variable P_{Ni}

Let P_{Ni} be allowed to vary at each layer i . For this case, the concept of a CPD is not meaningful since there may not be just one layer beyond which P_{TD_i} is non-zero. Using point estimates for the variables, Equation C-5 is evaluated over all m layers with P_{TD_i} explicitly evaluated at each layer.

C.2.4 Evaluation of P_E with Uncertainty Modeled as Probability

In general, all the variables in Equation C-5 have uncertainty, and to consider uncertainty P_E should be evaluated by convoluting the uncertainty distributions for each variable.

⁴⁹ Other terms can be added to P_{Ni} if needed.

⁵⁰ Assessment of an alarm can be included in P_D instead of P_{Ni} . Correctly responding based on that evidence to the correct location - that is, calling the correct “response plan” from the playbook- can be broken out separately.

Traditionally, probability has been used as a measure of uncertainty.⁵¹ With this approach, a probability distribution is assigned to the variables of interest and Equation C-5 is evaluated by probabilistic convolution of the probability distributions of the constituent variables. The convolution can be performed analytically in some cases or by Monte Carlo or Latin hypercube sampling techniques.

Another approach to performing the convolution is to use discrete probability distributions and directly evaluate the probability for the combination of the discrete values. That is the approach implemented in the BeliefConvolution code.⁵²

Using probability distributions to solve equation C-5, P_{TDi} requires special attention. Given probability distributions for T_{ADV_i} and T_{GRI_i} , we can form the probability distribution for $T_{REMAINING_i} = T_{ADV_i} - T_{GRI_i}$, where $T_{REMAINING_i}$ is the extra time available for response at layer i . Since we are using probability distributions for T_{ADV_i} and T_{GRI_i} , the probability distribution for $T_{REMAINING_i}$ can have negative values where the response time is insufficient. If $T_{REMAINING_i}$ is negative, there is no neutralization. Therefore, to correctly evaluate P_{TDi} in Equation 2, we want only the part of the distribution for which $T_{REMAINING_i}$ is positive; that is, $P_{TDi} = \text{Probability}(T_{REMAINING_i} > 0)$, or equivalently P_{TDi} is the probability that $T_{REMAINING_i}$ exceeds 0. For clarity, this value for P_{TDi} will be denoted as $P_{TD\text{ POSITIVE}_i}$. For discrete probability distributions,

$$P_{TD\text{ POSITIVE}_i} = \sum_{T_j \in T_{REMAINING_i}} p(T_j) | T_j > 0 \quad (\text{Eqn. C-6})$$

Where $p(T_j)$ is the probability for the j^{th} value from the set of values for $T_{REMAINING_i} = T_{ADV_i} - T_{GRI_i}$.

$P_{TD\text{ POSITIVE}_i}$ is a value, not a distribution.

Equation C-5 becomes:

$$P_E = \sum_{i=1}^m \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_{ASSESS_i} P_{WIN_i} P_{TD\text{ POSITIVE}_i} \quad (\text{Eqn. C-7})$$

where each term is evaluated by convolution, with $P_{TD\text{ POSITIVE}_i}$ being a point value in that convolution.⁵³

⁵¹ Probability used for a value, such as P_E , is probability in the objective sense, a frequency. See Appendix B.

⁵² A probability for a discrete point is a degenerate case of a degree of evidence for a discrete interval. Belief/plausibility reduce to probability when the discrete intervals to which evidence are assigned are all points.

⁵³ Equation C-7 suffers from the repeated variable type of dependence, e.g. P_{D_j} .

C.2.5 Evaluation of P_E with Uncertainty Modeled as Belief/Plausibility

If the information is too nonspecific for the use of probability as the measure of uncertainty, belief/plausibility can be used as the measure of uncertainty.⁵⁴ For this case, Equation C-5 is evaluated by convoluting belief/plausibility distributions.

$P_{TD\ POSITIVE_i}$ is taken as the belief that $T_{REMAINING_i} > 0$.⁵⁵ That is:

$$P_{TD\ POSITIVE_i} = Bel(T_{REMAINING_i} > 0) \quad (\text{Eqn. C-8})$$

Then, Equation C-5 is evaluated by convoluting the degrees of evidence for the algebraic operations over all the terms in the equation.

Equation C-8 is conservative as it only assigns evidence to $P_{TD\ POSITIVE_i}$ from the actual set of focal elements (the intervals over $T_{REMAINING_i}$ with evidence) that are totally contained in the interval $T_{REMAINING_i} > 0$. If T_{ADV_i} and T_{GR_i} are modeled using probability as the measure of uncertainty, then these focal elements are point values, the degrees of evidence are probabilities, and Equation C-8 is equivalent to Equation C-6.

The final result for P_E is a set of belief/plausibility intervals over the $[0, 1]$ domain for P_E .

C.3 Evaluation of C and CR

An uncertainty distribution is defined for C . If more than one type of consequence is to be considered, once the separate constituents of C have been assigned a common measure C is calculated by adding the separate consequences using convolution.

For example, let C be comprised of a set of n separate consequences, then:

$$C = \sum_n C_n \quad (\text{Eqn. C-9})$$

where the C_n are expressed using a common measure, such as willingness to pay.

Once P_E and C have been evaluated, then CR is evaluated using Equation C-1 by multiplication using convolution.

That is, the final equation to be evaluated is:

⁵⁴ Since belief/plausibility also includes probability as a degenerate case, some variables can be modeled with probability and others with belief/plausibility.

⁵⁵ Taking the likelihood that $T_{REMAINING_i} > 0$ as belief is conservative, a lower bound. Both an upper bound and a lower bound on the likelihood that $T_{REMAINING_i} > 0$ can be made using plausibility and belief, respectively. Section E.4 uses both an upper bound and lower bound type approach.

$$CR = (1 - \sum_{i=1}^m \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_{N_i}) \times \sum_n C_n \quad (\text{Eqn. C-10})$$

C.4 Example Evaluations

Assume three layers where each variable has uncertainty modeled as probability. The equation to be solved is:

$$\begin{aligned} P_E = & P_{D_1} P_{ASSESS1} P_{WIN1} P_{TD POSITIVE1} + \\ & (1 - P_{D_1}) P_{D_2} P_{ASSESS2} P_{WIN2} P_{TD POSITIVE2} + \\ & (1 - P_{D_1})(1 - P_{D_2}) P_{D_3} P_{ASSESS3} P_{WIN3} P_{TD POSITIVE3} \end{aligned} \quad (\text{Eqn. C-11})$$

C.4.1 Probabilistic Example

Assume the probabilistic degrees of evidence as given in Table C-1.

Table C-1. Probabilistic Evidence for Example

Variable and Domain	Point (degenerate interval)	Probability (Degree of Evidence)
$P_{D1} [0, 1]$	[0.7, 0.7]	0.2
	[0.8, 0.8]	0.6
	[0.9, 0.9]	0.2
$P_{D2} [0, 1]$	[0.8, 0.8]	0.1
	[0.9, 0.9]	0.6
	[0.94, 0.94]	0.3
$P_{D3} [0, 1]$	[0.3, 0.3]	0.9
	[0.4, 0.4]	0.1
$P_{ASSESS1} [0, 1]$	[0.7, 0.7]	0.8
	[0.8, 0.8]	0.2
$P_{ASSESS2} [0, 1]$	[0.9, 0.9]	1.0
$P_{ASSESS3} [0, 1]$	[0.2, 0.2]	0.3
	[0.3, 0.3]	0.4
	[0.4, 0.4]	0.3
$P_{WIN1} [0, 1]$	[0.9, 0.9]	0.5
	[1.0, 1.0]	0.5
$P_{WIN2} [0, 1]$	[0.8, 0.8]	0.5
	[0.9, 0.9]	0.5
$P_{WIN3} [0, 1]$	[0.5, 0.5]	0.5
	[0.6, 0.6]	0.5

Variable and Domain	Point (degenerate interval)	Probability (Degree of Evidence)
T_{ADV1} [10, 20] minutes	[12, 12]	0.4
	[14, 14]	0.6
T_{ADV2} [8, 12] minutes	[9, 9]	0.7
	[10, 10]	0.3
T_{ADV3} [1, 2] minutes	[1, 1]	0.8
	[2, 2]	0.2
T_{GR1} [7, 15] minutes	[11, 11]	0.3
	[13, 13]	0.4
	[15, 15]	0.3
T_{GR2} [7, 15] minutes	[8, 8]	0.3
	[13, 13]	0.4
	[15, 15]	0.3
T_{GR3} [20, 30] minutes	[25, 25]	0.4
	[28, 28]	0.6

Let C be comprised of two types of consequences with evidence as indicated in Table C-2.

Table C-2. Consequences for Example

Variable and Domain	Point (degenerate interval)	Probability (Degree of Evidence)
$C_{n,1}$ [0, 10^8] dollars	[10^5 , 10^5]	0.55
	[10^4 , 10^4]	0.45
$C_{n,2}$ [5, 10^7] dollars	[10^6 , 10^6]	0.60
	[10^4 , 10^4]	0.33
	[10^3 , 10^3]	0.07

Figure C-1 shows the results for CR, a probability distribution.⁵⁶ The mean value for CR is 4.39×10^5 which, as expected, is the same answer obtained by evaluating Equation C-11 using point values equal to the means of the probability distributions for each term in the equation.

⁵⁶ Figure C-1 uses the output from BeliefConvolution and for probabilistic data Belief = Plausibility = Probability and the expected value interval is a point equal to the probabilistic mean.

Figure C-1. Result for CR with Probability

C.4.2 Belief/Plausibility Example

Consider the example in Equation C-11 where the information is not specific enough to justify the use of probability as a measure of uncertainty; the degrees of evidence are over intervals, not over points. Assume the evidence in Tables C-3 and C-4.

Table C-3. Interval Evidence for Example

Variable and Domain	Interval	Probability (Degree of Evidence)
$P_{D1} [0, 1]$	[0.5, 0.7]	0.2
	[0.4, 0.8]	0.6
	[0.7, 0.9]	0.2
$P_{D2} [0, 1]$	[0.8, 0.9]	0.1
	[0.9, 1.0]	0.6
	[0.9, 0.96]	0.3
$P_{D3} [0, 1]$	[0.2, 0.6]	0.9
	[0.4, 0.5]	0.1
$P_{ASSESS1} [0, 1]$	[0.7, 0.9]	0.8
	[0.75, 0.8]	0.2
$P_{ASSESS2} [0, 1]$	[0.9, 0.95]	1.0

Variable and Domain	Interval	Probability (Degree of Evidence)
$P_{\text{ASSESS3}} [0, 1]$	[0.1, 0.2]	0.3
	[0.2, 0.3]	0.4
	[0.2, 0.4]	0.3
$P_{\text{WIN1}} [0, 1]$	[0.7, 0.9]	0.5
	[0.9, 1.0]	0.5
$P_{\text{WIN2}} [0, 1]$	[0.8, 0.9]	0.5
	[0.8, 1.0]	0.5
$P_{\text{WIN3}} [0, 1]$	[0.3, 0.7]	0.5
	[0.6, 0.7]	0.5
$T_{\text{ADV1}} [10, 20]$ minutes	[11, 15]	0.4
	[12, 16]	0.6
$T_{\text{ADV2}} [6, 12]$ minutes	[7, 9]	0.7
	[6, 12]	0.3
$T_{\text{ADV3}} [0, 3]$ minutes	[0, 3]	0.8
	[1, 2]	0.2
$T_{\text{GR1}} [7, 15]$ minutes	[10, 11]	0.3
	[12, 13]	0.4
	[10, 15]	0.3
$T_{\text{GR2}} [6, 15]$ minutes	[6, 7]	0.3
	[10, 13]	0.4
	[11, 15]	0.3
$T_{\text{GR3}} [18, 30]$ minutes	[20, 25]	0.4
	[18, 28]	0.6

Table C-4. Consequences for Example

Variable and Domain	Interval	Probability (Degree of Evidence)
$C_{n,1} [0, 10^8]$ dollars	$[10^4, 10^6]$	0.55
	$[10^3, 10^7]$	0.45
$C_{n,2} [5, 10^7]$ dollars	$[10^2, 10^6]$	0.60
	$[10^4, 10^7]$	0.33
	$[10^1, 10^5]$	0.07

Figure C-2 shows the results for CR, a belief/plausibility interval distribution. The expected value interval for CR is $[6.5 \times 10^3, 8.0 \times 10^6]$.

Figure C-2. Result for CR with Belief/Plausibility

C.5 Evaluation of CR including Detecting Formulation of Threat Resources

The prior sections of this appendix discussed solving the traditional equation of conditional risk (CR) for a physical security system.

With the use of a belief/plausibility measure for highly nonspecific evidence, the evaluation can be extended to address risk, which includes the likelihood that the adversary will choose a specific scenario. This was discussed in Section 4. For some applications an evaluation of the likelihood that an adversary selects a scenario is not performed, but the conditional risk equation is extended to include the probability of detecting the threat scenario during the formulation stage outside the facility boundary *given* the scenario is chosen by the adversary. This allows for consideration of the effectiveness of intelligence gathering efforts to detect the gathering of resources necessary to implement the chosen scenario.

Specifically, we wish to evaluate

$$CR_{with\ Formulation} = (1 - P_{Form}) * (1 - P_E) * C \quad (\text{Eqn. C-12})$$

where P_{Form} is the probability of detecting the threat during its formulation stage.

Equation C-12 is an extension of Equation C-1, and is solved by assigning degrees of evidence to P_{Form} and convoluting the $(1 - P_{Form})$ term with the terms in Equation C-1 using the technique discussed in Section C.4. That is:

$$CR_{with\ Formulation} = (1 - P_{Form}) x \left(1 - \sum_{i=1}^m \left(\prod_{j=1}^{i-1} (1 - P_{D_j}) \right) P_{D_i} P_{N_i} \right) x \sum_n C_n \quad (\text{Eqn. C-13})$$

is solved by convolution.

Appendix D. Java Tools: Belief Convolution and LinguisticBelief

This appendix summarizes two Java codes written by the author to effect convolution of numeric or linguistic variables using the belief/plausibility measure. The codes were written in Java 1.5 using the netbeans 4.1 Integrated Development Environment (IDE). Features of Java 1.5, such as generic classes with parameterized types, were used in the coding so the codes will not compile or execute in versions of Java earlier than 1.5.

BeliefConvolution performs numerical convolution of random variables with evidence assigned to intervals of real numbers. LinguisticBelief uses approximate reasoning to perform convolution of linguistic variables with evidence assigned to fuzzy sets.

Both codes assume that the variables are non-interacting, as discussed in Section A.3.3.

D.1 The BeliefConvolution Code

BeliefConvolution implements the mathematics of belief discussed in Appendix A for algebraic combinations of random variables with evidence assigned to intervals of real numbers. Two aspects of BeliefConvolution are documented here: aggregation of evidence and the ability to evaluate belief for fuzzy sets given evidence on crisp sets.

D.1.1 Aggregation of Evidence

The aggregation approach used in the code is similar to the aggregation technique for discrete probability distributions discussed by Kaplan. [Kaplan 1981] The code allows for aggregation of degrees of evidence for any variable, using linear or logarithmic binning. Aggregation is a process by which the degrees of evidence are reduced by mapping the variable into bins and assigning a point estimate, the midpoint of the bin, to any value of the variable in that bin. The need for aggregation is to reduce the numbers of degrees of evidence from the convolution of a large number of variables. For example, suppose that each variable has 3 degrees of evidence. A convolution of 10 such variables results in a variable with 3^{10} or about 60,000 degrees of evidence and this is a manageable number. But a convolution of 20 such variables results in a variable with 3^{20} or about 3.4×10^9 degrees of evidence and this is a not manageable number.

Unfortunately, convolution using belief/plausibility requires combining the degrees of evidence even if the variables are noninteractive. For two variables X and Y with A a subset (event or interval) of X and B a subset (event or interval) of Y, $\text{Bel}(A \times B) \leq \min[\text{Bel}(A), \text{Bel}(B)]$ where Bel is belief, so we cannot accurately calculate the belief for subsets of $X \times Y$ using belief for subsets of X combined with belief for subsets of Y. However, if X and Y are noninteractive we can combine degrees of evidence, m, as $m(A \times B) = m_X(A) \cdot m_Y(B)$ where m_X and m_Y are marginal degrees of evidence, and using the $m(A \times B)$ for all A and B that are focal elements the $\text{Bel}(A \times B)$ can be calculated from the focal elements of $X \times Y$.⁵⁷

⁵⁷ For probability, if A and B are independent $P(A \times B) = P(A) \cdot P(B)$ where P is probability. For possibility, even if A and B are dependent $\text{Pos}(A + B) = \max[\text{Pos}(A), \text{Pos}(B)]$ where Pos is possibility and the '+' in $\text{Pos}(A + B)$ is the cartesian co-product; if A and B are noninteractive in the possibilistic sense, it is also true that $\text{Pos}(A \times B) = \min[\text{Pos}(A), \text{Pos}(B)]$. The references provide more detailed information, specifically [Dubois and Prade].

Consider a variable X with range the set of all reals in $[\min, \max]$. The binning process involves defining a number of bins that partition X and considering every number within a bin to map to a single number, the value of the midpoint of the bin.

For linear binning into n bins the width of a bin is $(\max - \min)/n$ and the n bins are taken as:

$[\min, \text{bin 1 max}]$, $(\text{bin 1 max}, \text{bin 2 max}]$, $(\text{bin 2 max}, \text{bin 3 max}]$, ...
 $(\text{bin } n-1 \text{ max}, \max]$.

For log binning over the range 0 to 10^{28} the following bins are used:

$[0, 5 \times 10^{-6}]$, $(5 \times 10^{-6}, 1 \times 10^{-5}]$, $(1 \times 10^{-5}, 5 \times 10^{-5}]$, ...
 $(5 \times 10^{27}, 1 \times 10^{28}]$.

Each degree of evidence over X is a value assigned to an interval $[\text{low}, \text{high}]$ in X . The mapping of the degrees of evidence to the binned values of X is as follows. Low maps to the point value of the bin i where low is within $(\text{bin } i \text{ low}, \text{bin } i \text{ high}]$. High maps to the point value of the bin j where high is within $(\text{bin } j \text{ low}, \text{bin } j \text{ high}]$. So the mapped degree of evidence applies to the interval $[\text{bin } i \text{ point value}, \text{bin } j \text{ point value}]$. The mapping is not one-to-one since more than one unique $[\text{low}, \text{high}]$ has the same $[\text{bin } i \text{ point value}, \text{bin } j \text{ point value}]$. In fact, the degrees of evidence reduce, or aggregate, precisely because the mapping is not one-to-one. Each aggregated interval is assigned a degree of evidence equal to the sum of the degrees of evidence for each original interval that mapped into that aggregated interval. Figure D-1 graphically illustrates the aggregation process.

For example let the variable XX be $[4, 100]$ with the following degrees of evidence:

0.2 for $[4, 11]$
0.4 for $[4, 45]$
0.3 for $[8, 20]$
0.1 for $[27, 51]$.

Using linear binning with four bins the bins are:

$[4, 28]$ with midpoint 16
 $(28, 52]$ with midpoint 40
 $(52, 76]$ with midpoint 64
 $(76, 100]$ with midpoint 88.

The mapping of the degrees of evidence is as follows:

$[4, 11] \rightarrow [16, 16]$ with evidence 0.2
 $[4, 45] \rightarrow [16, 40]$ with evidence 0.4
 $[8, 20] \rightarrow [16, 16]$ with evidence 0.3
 $[27, 51] \rightarrow [16, 40]$ with evidence 0.1.

Figure D-1. Aggregation Process

The final aggregated degrees of evidence are:

[16, 16] with evidence 0.5
 [16, 40] with evidence 0.5.

Aggregation is useful when the number of degrees of evidence for a variable in the chain of algebraic operations becomes so large that further convolution would increase the number of degrees of evidence to an unmanageable number. The number of bins must not be set too large or aggregation causes too much loss of fidelity. For our security application, the variable min/max values are such that log aggregation may be better than linear aggregation. For example, a consequence variable may range from 0 to 10^7 deaths so consequences within about a factor of 10 are essentially identical for this scale.

The BeliefConvolution Java code allows for either linear or log aggregation at any step in the convolution.

Figure D-2 shows linear aggregation of evidence in BeliefConvolution for the variable XX just discussed.

Figure D-2. Aggregation of Evidence in BeliefConvolution Java Code

D.1.2 Belief/Plausibility for a Fuzzy Set

The ability to calculate belief/plausibility for fuzzy sets allows results to be summarized as linguistic variables (e.g., “Minor,” “Moderate,” “Major,” “Catastrophic”) and each linguistic variable is a fuzzy set over the appropriate numeric variable. For cases with crisp focal elements, BeliefConvolution calculates the belief/plausibility for a fuzzy set using Equation A-15.

BeliefConvolution requires that the shape of the fuzzy sets be trapezoids (or triangles, or rectangles which are crisp sets). The tuple $\langle \text{lower}, \text{lowerCrisp}, \text{upperCrisp}, \text{upper} \rangle$ specifies a fuzzy set. For example, the fuzzy set $\langle 4, 15, 27, 48 \rangle$ is shown in Figure D-3.

Figure D-3. Example Trapezoidal Fuzzy Set

Degenerate cases are $\langle 15, 15, 27, 27 \rangle$ (the crisp set shown in Figure D-4), and the triangular shaped fuzzy sets $\langle 4, 15, 15, 27 \rangle$ and $\langle 4, 4, 4, 27 \rangle$ shown in Figures D-5 and D-6.

Figure D-4. Example Crisp Set

Figure D-5. Example Triangular Fuzzy Set

Figure D-6. Example Triangular Fuzzy Set

The fuzzy set is divided into three portions: lower fuzzy portion, crisp portion, and upper crisp portion. For the fuzzy sets shown above the portions are:

For $\langle 4, 15, 27, 48 \rangle$

Lower fuzzy portion is $[4, 15)$

Crisp portion is $[15, 27]$

Upper fuzzy portion is $(27, 48]$

For $\langle 15, 15, 27, 27 \rangle$

Lower fuzzy portion is not present

Crisp portion is $[15, 27]$

Upper fuzzy portion is not present

For $\langle 4, 15, 15, 27 \rangle$

Lower fuzzy portion is $[4, 15)$

Crisp portion is not present

Upper fuzzy portion $[15, 27]$

For $\langle 4, 4, 4, 27 \rangle$

Lower fuzzy portion is not present

Crisp portion is not present

Upper fuzzy portion is $[4, 27]$

Note that each fuzzy portion has an area $\frac{1}{2}$ of the area if that fuzzy portion were crisp; see Figure D-7 for example.

Figure D-7. Area Example

As an example of the calculation of belief for a fuzzy set, consider the fuzzy set $\langle 4, 15, 27, 48 \rangle$ shown in Figure D-8.

Assume the degrees of evidence over the crisp intervals indicated in Figure D-8 are as follows:

- Interval A [7, 36] has degree of evidence 0.15
- Interval B [4, 18] has degree of evidence 0.23
- Interval C [25, 40] has degree of evidence 0.07
- Interval D [3, 11] has degree of evidence 0.49
- Interval E [33, 48] has degree of evidence 0.06.

Figure D-8. Crisp Evidence with a Fuzzy Set

Using BeliefConvolution, the belief and plausibility for this fuzzy set can be calculated:

```
// report fuzzy set belief example input
Variable reportFuzzySet = new Variable("ReportFuzzySet," 1, 50, false);
reportFuzzySet.addEvidenceInterval(new EvidenceInterval(reportFuzzySet.getName(), 7, 36, 0.15));
reportFuzzySet.addEvidenceInterval(new EvidenceInterval(reportFuzzySet.getName(), 4, 18, 0.23));
reportFuzzySet.addEvidenceInterval(new EvidenceInterval(reportFuzzySet.getName(), 25, 40, 0.07));
reportFuzzySet.addEvidenceInterval(new EvidenceInterval(reportFuzzySet.getName(), 3, 11, 0.49));
reportFuzzySet.addEvidenceInterval(new EvidenceInterval(reportFuzzySet.getName(), 33, 48, 0.06));

reportFuzzySet.printOverallResults();
reportFuzzySet.printBelPIForFuzzySet("Example Fuzzy Set," 4, 15, 27, 48);
reportFuzzySet.printBelPIForCrispSet(9.5, 37.5);
```

RESULTS FOR: ReportFuzzySet

Minimum value: 1.00000E+00 Maximum value: 5.00000E+01

Expected value interval for Variable ReportFuzzySet is: [7.17000E+00, 2.06100E+01]

Intervals and Degrees of Evidence follow

Number of focal elements (intervals with non-zero degree of evidence): 5

Sum of degrees of evidence for all focal elements: 1.00000E+00

For Variable named ReportFuzzySet [3.00000E+00, 1.10000E+01] has evidence 4.90000E-01

For Variable named ReportFuzzySet [4.00000E+00, 1.80000E+01] has evidence 2.30000E-01

For Variable named ReportFuzzySet [7.00000E+00, 3.60000E+01] has evidence 1.50000E-01

For Variable named ReportFuzzySet [2.50000E+01, 4.00000E+01] has evidence 7.00000E-02

For Variable named ReportFuzzySet [3.30000E+01, 4.80000E+01] has evidence 6.00000E-02

Exceedance likelihoods follow

Number of discrete steps in the exceedance results: 10

For Variable named ReportFuzzySet Exceedance result for greater than 3.00000E+00 up to and including 5.00000E+01 is Belief 5.10000E-01 and Plausibility 1.00000E+00

For Variable named ReportFuzzySet Exceedance result for greater than 4.00000E+00 up to and including 5.00000E+01 is Belief 2.80000E-01 and Plausibility 1.00000E+00
 For Variable named ReportFuzzySet Exceedance result for greater than 7.00000E+00 up to and including 5.00000E+01 is Belief 1.30000E-01 and Plausibility 1.00000E+00
 For Variable named ReportFuzzySet Exceedance result for greater than 1.10000E+01 up to and including 5.00000E+01 is Belief 1.30000E-01 and Plausibility 5.10000E-01
 For Variable named ReportFuzzySet Exceedance result for greater than 1.80000E+01 up to and including 5.00000E+01 is Belief 1.30000E-01 and Plausibility 2.80000E-01
 For Variable named ReportFuzzySet Exceedance result for greater than 2.50000E+01 up to and including 5.00000E+01 is Belief 6.00000E-02 and Plausibility 2.80000E-01
 For Variable named ReportFuzzySet Exceedance result for greater than 3.30000E+01 up to and including 5.00000E+01 is Belief 0.00000E+00 and Plausibility 2.80000E-01
 For Variable named ReportFuzzySet Exceedance result for greater than 3.60000E+01 up to and including 5.00000E+01 is Belief 0.00000E+00 and Plausibility 1.30000E-01
 For Variable named ReportFuzzySet Exceedance result for greater than 4.00000E+01 up to and including 5.00000E+01 is Belief 0.00000E+00 and Plausibility 6.00000E-02
 For Variable named ReportFuzzySet Exceedance result for greater than 4.80000E+01 up to and including 5.00000E+01 is Belief 0.00000E+00 and Plausibility 0.00000E+00

For Variable named ReportFuzzySet the fuzzy set Example Fuzzy Set with {lower, lowerCrisp, upperCrisp, upper} of {4.00000E+00, 1.50000E+01, 2.70000E+01, 4.80000E+01} has Belief 6.75758E-02 and Plausibility 8.04675E-01

For the example problem, the fuzzy set has Belief/Plausibility of 0.068/0.80.

The fuzzy set can be approximated by the crisp set <9.5, 9.5, 37.5, 37.5> and for this crisp set the code calculates:

For Variable named ReportFuzzySet the crisp set [9.50000E+00, 3.75000E+01] has Belief 0.00000E+00 and Plausibility 1.00000E+00

This crisp set has Belief/Plausibility of 0/1.0.

D.2 The LinguisticBelief Code

LinguisticBelief implements the mathematics of belief discussed in Appendix B for rule-based combinations of linguistic variables with evidence assigned to fuzzy sets. For a variable formed from a rule base, no more than three input variables are allowed.

Figure D-9 shows a screen capture of the LinguisticBelief code in the netbeans IDE, for the example of Section 3.3.

Based on the mapping of input fuzzy sets to output fuzzy sets per the rule base, an automatic “aggregation” of focal elements is performed in the LinguisticBelief code. (As discussed in Section D.1, for convolution of numeric variables using BeliefConvolution, aggregation requires user-specified binning.)

This aggregation is best discussed by an example. Consider the rule base for the linguistics Quality Of Life and Happiness presented in Section 3.3. Using the LinguisticBelief Code the following results are obtained (selected output presented).

Figure D-9. LinguisticBelief in the netbeans IDE

Quality of Life Focal Elements

For RuleLinguistic Quality of Life a FocalElement with degree of evidence 2.4000e-01 is:

Bad_&_Middle Class
Moderate_&_Middle Class

For RuleLinguistic Quality of Life a FocalElement with degree of evidence 5.6000e-01 is:

Bad_&_Poor
Bad_&_Middle Class
Moderate_&_Poor
Moderate_&_Middle Class

For RuleLinguistic Quality of Life a FocalElement with degree of evidence 6.0000e-02 is:

Moderate_&_Middle Class
Excellent_&_Middle Class

For RuleLinguistic Quality of Life a FocalElement with degree of evidence 1.4000e-01 is:

Moderate_&_Poor
Moderate_&_Middle Class
Excellent_&_Poor
Excellent_&_Middle Class

Quality of Life Rule Base

For RuleLinguistic Quality of Life the fuzzy sets from union of rules with output FuzzySet Not So Good are:

Bad_&_Poor
Moderate_&_Poor
Bad_&_Middle Class
Moderate_&_Middle Class
Bad_&_Rich

For RuleLinguistic Quality of Life the fuzzy sets from union of rules with output FuzzySet Good are:

Excellent_&_Poor
Excellent_&_Middle Class
Moderate_&_Rich
Excellent_&_Rich

Quality of Life Belief / Plausibility Intervals

For BasicLinguistic Quality of Life For fuzzy set Not So Good Belief / Plausibility interval is: 8.00000e-01 / 1.00000e+00

For BasicLinguistic Quality of Life For fuzzy set Good Belief / Plausibility interval is: 0.00000e+00 / 2.00000e-01

Outlook on Life Belief / Plausibility Intervals

For BasicLinguistic Outlook On Life For fuzzy set Pessimist Belief / Plausibility interval is 2.0000e-02 , 1.0000e+00

For BasicLinguistic Outlook On Life For fuzzy set Optimist Belief / Plausibility interval is 0.0000e+00 , 9.8000e-01

To evaluate “Happiness” using the rule base, its focal elements need to be expressed in terms of the fuzzy sets of its input variables, which is accomplished by aggregation. For example, before aggregation the focal elements for “Happiness” are:

- (1) For RuleLinguistic Happiness a FocalElement with degree of evidence: 4.8000e-03 is
Bad_&_Middle Class_&_Pessimist
Moderate_&_Middle Class_&_Pessimist
- (2) For RuleLinguistic Happiness a FocalElement with degree of evidence: 2.3520e-01 is
Bad_&_Middle Class_&_Pessimist
Bad_&_Middle Class_&_Optimist
Moderate_&_Middle Class_&_Pessimist
Moderate_&_Middle Class_&_Optimist
- (3) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.1200e-02 is:
Bad_&_Poor_&_Pessimist
Bad_&_Middle Class_&_Pessimist
Moderate_&_Poor_&_Pessimist
Moderate_&_Middle Class_&_Pessimist
- (4) For RuleLinguistic Happiness a FocalElement with degree of evidence 5.4880e-01 is:
Bad_&_Poor_&_Pessimist
Bad_&_Poor_&_Optimist
Bad_&_Middle Class_&_Pessimist
Bad_&_Middle Class_&_Optimist
Moderate_&_Poor_&_Pessimist
Moderate_&_Poor_&_Optimist
Moderate_&_Middle Class_&_Pessimist
Moderate_&_Middle Class_&_Optimist
- (5) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.2000e-03 is:
Moderate_&_Middle Class_&_Pessimist
Excellent_&_Middle Class_&_Pessimist
- (6) For RuleLinguistic Happiness a FocalElement with degree of evidence 5.8800e-02 is:
Moderate_&_Middle Class_&_Pessimist
Moderate_&_Middle Class_&_Optimist
Excellent_&_Middle Class_&_Pessimist
Excellent_&_Middle Class_&_Optimist
- (7) For RuleLinguistic Happiness a FocalElement with degree of evidence 2.8000e-03 is:
Moderate_&_Poor_&_Pessimist
Moderate_&_Middle Class_&_Pessimist
Excellent_&_Poor_&_Pessimist
Excellent_&_Middle Class_&_Pessimist
- (8) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.3720e-01 is:
Moderate_&_Poor_&_Pessimist
Moderate_&_Poor_&_Optimist
Moderate_&_Middle Class_&_Pessimist
Moderate_&_Middle Class_&_Optimist
Excellent_&_Poor_&_Pessimist
Excellent_&_Poor_&_Optimist
Excellent_&_Middle Class_&_Pessimist
Excellent_&_Middle Class_&_Optimist

The rule base for “Happiness” is:

For RuleLinguistic Happiness the fuzzy sets from union of rules with output FuzzySet Very Happy are:
Good_&_Optimist

For RuleLinguistic Happiness the fuzzy sets from union of rules with output FuzzySet Accepting are:
Not So Good_&_Optimist
Good_&_Pessimist

For RuleLinguistic Happiness the fuzzy sets from union of rules with output FuzzySet Depressed are:
Not So Good_&_Pessimist

The focal elements for “Happiness” contain “Quality Of Life” in terms of the fuzzy sets of its input variables “Health” and “Wealth,” but the rule base for “Happiness” is expressed in terms of the fuzzy sets for “Quality Of Life.” The focal elements for “Happiness” must be aggregated to be expressed in terms of the fuzzy sets of “Quality Of Life” instead of being expressed in terms of the fuzzy sets for the input variables for “Quality Of Life.”

Aggregation is performed in two steps. First, for any given focal element, its constituent input fuzzy sets are mapped to the appropriate output fuzzy set per the rule base. For “Happiness,” this results in the following focal elements:

- (1) For RuleLinguistic Happiness a FocalElement with degree of evidence 4.8000e-03 is:
Not So Good_&_Pessimist
- (2) For RuleLinguistic Happiness a FocalElement with degree of evidence 2.3520e-01 is:
Not So Good_&_Pessimist
Not So Good_&_Optimist
- (3) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.1200e-02 is:
Not So Good_&_Pessimist
- (4) For RuleLinguistic Happiness a FocalElement with degree of evidence: 5.4880e-01 is
Not So Good_&_Pessimist
Not So Good_&_Optimist
- (5) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.2000e-03 is:
Not So Good_&_Pessimist
Good_&_Pessimist
- (6) For RuleLinguistic Happiness a FocalElement with degree of evidence 5.8800e-02 is:
Not So Good_&_Pessimist
Not So Good_&_Optimist
Good_&_Pessimist
Good_&_Optimist
- (7) For RuleLinguistic Happiness a FocalElement with degree of evidence 2.8000e-03 is:
Not So Good_&_Pessimist
Good_&_Pessimist
- (8) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.3720e-01 is:
Not So Good_&_Pessimist
Not So Good_&_Optimist
Good_&_Pessimist
Good_&_Optimist

Second, focal elements resulting from step one containing identical fuzzy sets are combined by adding the degrees of evidence, resulting in the following focal elements for “Happiness.”

(A) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.6000e-02 is:
Not So Good_&_Pessimist

(B) For RuleLinguistic Happiness a FocalElement with degree of evidence 7.8400e-01 is:
Not So Good_&_Pessimist
Not So Good_&_Optimist

(C) For RuleLinguistic Happiness a FocalElement with degree of evidence 4.0000e-03 is:
Not So Good_&_Pessimist
Good_&_Pessimist

(D) For RuleLinguistic Happiness a FocalElement with degree of evidence 1.9600e-01 is:
Not So Good_&_Pessimist
Not So Good_&_Optimist
Good_&_Pessimist
Good_&_Optimist

This two-step aggregation operation reduced the number of focal elements for “Happiness” from eight to four.

This page intentionally left blank.

Appendix E. Risk as Exceedance Frequency of Consequence

E.1 Introduction

Risk for a scenario can be expressed as the product of the likelihood of the scenario and the consequence given the scenario. A low likelihood, high-consequence scenario can have the same risk as a high likelihood, low-consequence scenario.

To convey more information, it is desirable to summarize risk as a likelihood of exceeding consequence. This appendix discusses how to express risk from a number of sequences as an exceedance frequency of consequence. Section E.2 summarizes the risk triplet approach of Kaplan and Garrick by way of examples where uncertainty is evaluated using a probability measure. [Kaplan and Garrick]

Section E.3 addresses the issue of evaluating the occurrence of the initiating event as a probability or a frequency.⁵⁸

Section E.4 discusses how to express risk as an exceedance frequency of consequence when belief/plausibility is used as the measure of uncertainty.

E.2 Risk Triplet Approach

The risk triplet approach is summarized in the paper by Kaplan and Garrick. Each of a number of scenarios has two variables: the probability of the scenario and the consequence given the scenario. Let $p(S_i)$ denote the probability of occurrence of scenario S_i where “i” denotes the number assigned to identify the scenario, and let $C|S_i$ denote the consequence given the occurrence of S_i . We have a risk triplet (3-tuple) $\langle S_i, p(S_i), C|S_i \rangle$ for each scenario. Risk is defined as the set of risk triplets over all “n” scenarios: $\text{Risk} = \{ \langle S_i, p(S_i), C|S_i \rangle \mid i = 1, 2, \dots, n \}$. This assumes that the scenarios are mutually exclusive: $S_i \cap S_j = \text{null}$ for any two scenarios “i” and “j.”⁵⁹ That is, the sample space is $\{S_i \mid i = 1, 2, \dots, n\}$.

The following sections use simple examples to explain the risk triplet approach for three progressively more complicated situations: (1) no uncertainty, (2) uncertainty in the likelihood of the scenario and (3) uncertainty in both the likelihood of the scenario and the consequence. Probability is used as the measure of uncertainty.

E.2.1 No Uncertainty

If there is no uncertainty, order the scenarios such that $C_i \leq C_{i+1}$.

For example, consider the three scenarios in Table E-1.

⁵⁸ In the paper by Kaplan and Garrick, the authors use the name frequency to mean objective probability and reserve the name probability to mean subjective probability. (See Appendix B of this report.) In Appendix E, frequency always means a physical rate, e.g., number of events per year, and probability is used in both the subjective and objective sense.

⁵⁹ As stated in the Kaplan and Garrick paper footnote #4: “The categories of scenarios, incidentally, should of course be chosen so that they are mutually exclusive and the same event does not show up in more than one category.”

Table E-1. Three Scenarios, No Uncertainty

Scenario S_i and Probability of Scenario $p(S_i)$	Consequence for Scenario $C S_i$	Probability of Consequence C or Greater ⁶⁰
S_1 2e-2	5	5.4e-2
S_2 3e-2	7	3.4e-2
S_3 4e-3	9	4e-3

The last column in Table E-1 is formed by summing the probability for the indicated consequence with the probabilities for all higher consequences. The results are summarized in Figure E-1, which presents risk from all three scenarios as an exceedance probability of consequence.

Figure E-1. Exceedance Probability of Consequence

This development assumed that the scenarios are mutually exclusive. This requirement is discussed in the next section.

E.2.1.1 Scenarios that are Not Mutually Exclusive

⁶⁰ In the paper by Kaplan and Garrick, for cases where the consequence from each scenario is a single value with no uncertainty, as discussed here in Sections E.2.1 and E.2.2, the results for exceeding a given consequence are actually for consequences equal to or greater than the given consequence. For consequence that has uncertainty, as discussed here in Section E.2.3, the results for exceeding a given consequence are for consequences greater than the given consequence, since the complementary cumulative distribution function (CCDF) is used.

The risk triplet approach as just described assumes that the scenarios are mutually exclusive: $p(S_i \cap S_j) = 0$ and $p(S_i \cup S_j) = p(S_i) + p(S_j)$.⁶¹ In general, scenarios may not be mutually exclusive and $p(S_i \cup S_j) = p(S_i) + p(S_j) - p(S_i \cap S_j)$. If $p(S_i \cap S_j)$ is small relative to $p(S_i)$ and $p(S_j)$ we can use the “rare event” approximation:

$p(S_i \cup S_j) \approx p(S_i) + p(S_j)$. Note that the rare event approximation does not require that the events be independent, it only requires that the likelihood of occurrence of multiple events be small. For scenarios that are independent, $p(S_i \cap S_j) = p(S_i) \cdot p(S_j)$, and if $p(S_i) \cdot p(S_j)$ is small relative to $p(S_i)$ and $p(S_j)$ the rare event approximation is valid.

If the likelihood of occurrence of multiple occurrences is not small, the approach must be modified to include occurrence of multiple scenarios.

Consider two scenarios that are independent, but have a high probability of occurrence.⁶²

Let $\bar{S}_i$ indicate the non-occurrence of scenario “i.

The sample space is: $\{ \langle S_1, S_2 \rangle, \langle S_1, \bar{S}_2 \rangle, \langle \bar{S}_1, S_2 \rangle, \langle \bar{S}_1, \bar{S}_2 \rangle \}$.

Let scenario 1 have a probability of 0.8 and scenario 2 have a probability of 0.7; let 5 and 7 be the consequences of the two scenarios, respectively. Since the probabilities are not small, we must consider the probabilities of the scenarios not occurring and the associated consequences. The probability of scenario 1 not occurring is 0.2 with consequence 0; the probability of scenario 2 not occurring is 0.3 with consequence 0.

Table E-2 and Figure E-2 summarize the results.

Table E-2. Two Independent Scenarios, No Uncertainty, Probabilities Not Small

Combination of Scenarios and Probability of Combination	Consequence for Combination	Probability of Consequence C or Greater
$\bar{S}_1$ and $\bar{S}_2$ 0.2·0.3 = 0.06	0 + 0 = 0	1
S_1 and $\bar{S}_2$ 0.8·0.3 = 0.24	5 + 0 = 5	0.94
$\bar{S}_1$ and S_2 0.2·0.7 = 0.14	0 + 7 = 7	0.70
S_1 and S_2 0.8·0.7 = 0.56	5 + 7 = 12	0.56

⁶¹ Using a probability measure, if events A and B are mutually exclusive, $p(A \cap B) = 0$. If events A and B are independent, $p(A \cap B) = p(A) \cdot p(B)$. Therefore, events that are mutually exclusive cannot be independent (except for the degenerate case where A and B both have probability zero).

⁶² For example, one scenario could be a flood in North America and the second scenario could be an earthquake in Asia, both scenarios considered over a period of time of 10 years.

Figure E-2. Exceedance Probability of Consequence

The occurrence of a scenario can be quantified as a physical frequency (number of occurrences per unit time) rather than a probability. Let F_i denote the frequency of scenario S_i . For example, consider two independent scenarios 1 and 2 with frequencies of occurrence of 0.8 per year and 0.7 per year, respectively. Table E-3 and Figure E-3 summarize the results for frequency exceedance of consequence.

Table E-3. Two Independent Scenarios with No Uncertainty

Scenario S_i and Frequency of Scenario F_i (per year)	Consequence for Scenario $C S_i$	Frequency (per year) of Consequence $C S_i$ or Greater
S_1 0.8 per year	5	1.5 per year
S_2 0.7 per year	7	0.7 per year

Note that frequencies simply add (e.g., $F_1 + F_2$) while probabilities “add probabilistically”, e.g., $P_1 + P_2 - P_1 \cap P_2$.

Figure E-3. Exceedance Frequency of Consequence

Section E.3 addresses the issue of whether the initiating event should be expressed as a probability or a frequency. In the remainder of this appendix, it is assumed that the initiating events are evaluated as a frequency with units of per year, and that the scenarios are independent.

E.2.2 Uncertainty in the Frequency of a Scenario

In this situation, the frequency of occurrence of each scenario is uncertain, but the consequence of each scenario is certain. Consider the following example for three scenarios. It is assumed that for each scenario the random variables F_i and $C|S_i$ are independent.⁶³

F_1 is modeled with a lognormal probability distribution with mean $2e-2$ and standard deviation $3e-2$. F_2 is modeled with a lognormal probability distribution with mean $3e-2$ and standard deviation $1e-2$. F_3 is modeled with a lognormal probability distribution with mean $4e-3$ and standard deviation $3e-3$. The consequence of each scenario is 5, 7, and 9, respectively. In this case, the addition in the third column of Table E-1 is accomplished by convoluting the probability distributions for the frequency of the scenarios under addition. For example, the probability distribution for consequence of 7 or greater is the convolution $F_2 + F_3$, and the probability distribution for consequence of 5 or greater is the convolution $F_1 + F_2 + F_3$. Results

⁶³ See both Section 5.3 and the Appendix in the paper by Kaplan and Garrick for the generalization considering dependence between F_i and $C|S_i$.

are expressed for any desired percentile of the resulting distribution.⁶⁴ Results for 5%, 50%, and 95% percentiles are summarized in Table E-4 and Figure E-4; the calculations were performed using the Crystal Ball software to convolute probability distributions [Crystal Ball].

Table E-4. Three Scenarios with Uncertainty in Frequency of Occurrence of Scenario

Scenario S_i and Frequency F_i (per year) of Scenario	Consequence for Scenario $C S_i$	Frequency (per year) of Consequence $C S_i$ or Greater for Selected Percentiles		
		5%	50%	95%
S_1 lognormal mean $2e-2$ std dev $3e-2$	5	$2.71e-2$	$4.67e-2$	$1.03e-1$
S_2 lognormal mean $3e-2$ std dev $1e-2$	7	$1.99e-2$	$3.24e-2$	$5.33e-2$
S_3 lognormal mean $4e-3$ std dev $3e-3$	9	$1.07e-3$	$3.20e-3$	$9.63e-3$

Figure E-4. Exceedance Frequency of Consequence

⁶⁴ For a random variable X with a continuous probability distribution, the value x_p such that $P(x \leq x_p) = p$ is called the 100pth percentile [Dougherty 1990]. It is sometimes stated that x_p is the value of X to a “confidence” of $p\%$. We avoid using the term confidence for a percentile since typically confidence means a confidence interval for a parameter, not a percentile of a probability distribution.

E.2.3 Uncertainty in Frequency and Uncertainty in Consequence

In this situation, the frequency of occurrence of each sequence is uncertain, and the consequence of each sequence is uncertain. Consider the following example for three sequences.

F_1 is modeled with a lognormal probability distribution with mean $2e-2$ and standard deviation $3e-2$. F_2 is modeled with a lognormal probability distribution with mean $3e-2$ and standard deviation $1e-2$. F_3 is modeled with a lognormal probability distribution with mean $4e-3$ and standard deviation $3e-3$. Assume that the first scenario has consequence with a uniform distribution over $[0, 10]$. The second scenario has consequence with a triangular distribution with minimum 2, most likely 7, and maximum 15. The third scenario has consequence with lognormal distribution, mean 9 and standard deviation 2.

Let $P(C|S_i)$ denote the complementary cumulative distribution function (CCDF) for $C|S_i$. (See note 60). Let $P(C_j|S_i)$ denote the probability that scenario S_i has consequence greater than C_j , given the scenario occurs; $P(C_j|S_i)$ is $P(C|S_i)$ at a specific C_j . For our example, we will consider consequence as the set $\{2, 4, 6, 8, 10, 12, 14, 16\}$; “j” denotes one element of this set and the elements are ordered by increasing value. The $P(C_j|S_i)$ are given in Table E-5, calculated using Crystal Ball. [Crystal Ball]

Table E-5. $P(C_j|S_i)$

C_j	$P(C_j S_1)$	$P(C_j S_2)$	$P(C_j S_3)$
2	0.8	1	1
4	0.6	0.93	0.98
6	0.4	0.75	0.95
8	0.2	0.47	0.65
10	0	0.2	0.25
12	0	0.08	0.08
14	0	0.01	0.04
16	0	0	0.03

For scenario S_i , the frequency of exceeding consequence C_j is $F_i \cdot P(C_j|S_i)$. Let $\text{Freq}(C_j)$ denote the frequency of exceeding consequence C_j from all the scenarios.

$\text{Freq}(C_j) = F_1 \cdot P(C_j|S_1) + F_2 \cdot P(C_j|S_2) + F_3 \cdot P(C_j|S_3)$. For each C_j , the probability distribution for $\text{Freq}(C_j)$ is calculated by convolution where the $P(C_j|S_i)$ are the *point values* from Table 5. Results are summarized for percentiles of interest in Table E-6 and Figure E-5 for our simple example. With 95% probability the frequency of exceeding a consequence of 8 is not larger than about 3.4×10^{-2} . With 50% probability the frequency of exceeding a consequence of 8 is not larger than about 1.9×10^{-2} .

Table E-6. Three Scenarios, Uncertainty in Frequency of Occurrence of Scenario and Uncertainty in Consequence

Consequence C_j	Frequency of Consequence greater than C_j $Freq(C_j)$ for Elected Percentiles		
	5%	50%	95%
2	2.6e-2	4.4e-2	9.1e-2
4	2.4e-2	4.0e-2	7.6e-2
6	1.9e-2	3.2e-2	5.8e-2
8	1.2e-2	1.9e-2	3.4e-2
10	4.1e-3	6.7e-3	1.1e-2
12	1.6e-3	2.6e-3	4.3e-3
14	2.6e-4	4.3e-4	7.6e-4
16	3.2e-5	9.6e-5	2.9e-4

Figure E-5. Exceedance Frequency of Consequence

In general, for “i” scenarios and “j” consequences:

$$Freq(C_j) = \sum_i F_i \cdot P(C_j | S_i) \quad (\text{Eqn. E-1})$$

is the frequency of exceedance of consequence value C_j with uncertainty in F_i and $C_j|S_i$, expressed as a probability distribution.

This is the general approach for calculating frequency of exceedance of consequence when a probability measure is used for uncertainty; the cases discussed in Sections E.2.2 and E.2.1 are degenerate cases of this general solution.

E.3 Occurrence of Sequence: Probability or Frequency

In application, risk for a scenario consists of three terms: likelihood of occurrence of the scenario, likelihood of system failure given the scenario occurs, and consequence given system failure. In this section, to focus on the issue of interest, all these variables are assumed to be known with certainty. Uncertainty can be considered by convoluting likelihood distributions.

Consider the likelihood of occurrence of the scenario. If the scenario is a random event, with a likelihood that does not change significantly with time, such as an earthquake, the likelihood is typically modeled as a frequency; e.g., the number of times per year the event occurs. It is not required that the frequency be a small value, although for many scenarios it is a small value. The frequency of the consequence C for the scenario S_i is $f_i \cdot P_i$ where f_i is the frequency of the scenario and P_i is the probability of system failure given the initiating event; e.g., the probability that a building fails given an earthquake of a specified magnitude. Let $F_i \equiv f_i \cdot P_i$; F_i is the rate at which consequence $C|S_i$ will occur.⁶⁵

The probability of occurrence of the scenario within time period T is $P(T) = 1 - \exp(-f_i \cdot T)$. To be precise, $P(T)$ is the probability that the scenario occurs *one or more* times within the time period T .⁶⁶ For f_i with units of per year and T of 1 year, if $f_i \cdot T$ is small (much less than 1) then $P(T=1 \text{ year})$ is numerically equal to f_i . For example, if f_i is $1e-3$ per year, $P(T=1 \text{ year}) = 9.995e-4$ which is essentially $1e-3$. Therefore, it is sometimes stated that f_i is the “annual probability” of occurrence for the scenario, but this is not true unless $f_i \cdot T$ is small. For example, if f_i is 2 per year, $P(T=1 \text{ year}) = 0.86$.

To avoid confusion in the interpretation of results, for a random event with a high frequency, its likelihood of occurrence should be modeled as a frequency instead of a probability. Consider an event with frequency f_i of 2 per year. The probability that the event happens *one or more* times in a year is 0.86. Assume that the probability of system failure given the event is $1e-6$. The probability that the event occurs and the system fails *one or more* times in a year is $8.6e-7$. Assume that the consequence of system failure is 10 deaths. If we calculate risk as probability of occurrence $\times$ probability of system failure $\times$ consequence, we calculate risk as $8.6e-6$ deaths *one*

⁶⁵ Since F_i is a frequency, the risk curves for frequency of exceedance of consequence can be generated using by simple addition of frequencies as discussed in Section E.2.1.1.

⁶⁶ For an event with a frequency F , the probability that the event occurs one or more times during a specific (fixed) time T is $P(T) = 1 - \exp(-F \cdot T)$ using the exponential probability distribution function. There are many assumptions associated with using the exponential distribution. [Fault Tree Handbook] It is assumed that the occurrences have the properties of a stationary Poisson process. For “repairable” systems, it is assumed that after an occurrence the system is instantly restored to good-as-new status. (The exponential distribution is also used to model the time of first failure; if T is not fixed, but considered to be a random variable, $P(T)$ is the probability distribution for the time of first failure.)

or more times in a year. This result is valid, but the problem is in the interpretation of the result. We have seen the result misstated as simply $8.6\text{e-}6$ deaths in a year; the important qualifier *one or more* times is omitted.

Had we modeled the initiating event as a frequency, we would evaluate the risk from the event as frequency of occurrence x probability of system failure x consequence: two per year x $1\text{e-}6$ x 10 deaths = $2\text{e-}5$ per year. The risk is $2\text{e-}5$ deaths per year. This result is not subject to confusion and misuse as is the earlier result where the likelihood of the initiating event is quantified as a probability.

Probabilistic safety analyses for nuclear power plants typically model the occurrence of the initiating event as a frequency (e.g. number of occurrences per year).

For a terrorist act, the likelihood of occurrence of a scenario is the likelihood that the terrorist intentionally selects that scenario. Should this likelihood of occurrence be modeled as a frequency, or should it be modeled as a probability over a specified time period?

One argument for modeling it as a probability is that it is not a random event and its likelihood will change significantly with time; changes occur in the adversary resources (for example, due to defender response) and the adversary may change scenarios based on many factors (changes in world political situation, changes in prioritization of targets to be attacked, etc.).

However, for some scenarios, such as attacks against US soldiers in Iraq, the likelihood of the scenario is not small and this argues for modeling the likelihood of occurrence as a frequency to avoid misinterpretation of the results as previously discussed. One solution is to model the occurrence of the initiating event as a time dependent frequency, $f_i(t)$.

For evaluating the risk of terrorist acts, we will model the initiating event as a physical frequency (rate), not as a probability.

E.4 Risk as Exceedance Frequency of Consequence using a Belief/Plausibility Measure for Uncertainty

The earlier sections discussed evaluating a collection of scenarios where probability is the measure used for uncertainty. This section discusses evaluation of a collection of scenarios where belief/plausibility is used as the measure of uncertainty.

It is desirable to express risk as a frequency of exceedance of consequence similar to the risk triplet approach. That is, we wish to adapt the approach of Section E.2.3- where probability was used as a measure of uncertainty- to the situation where belief/plausibility is used as a measure of uncertainty.

Consider Equation E-1; each term is the frequency of a scenario reduced by the probability that the consequence is greater than the specific consequence of concern.

Let us generalize equation E-1 to:

$$Freq(C_j) = \sum_i F_i \cdot L(C_j | S_i) \quad (\text{Eqn. E-2})$$

where L is a general measure of likelihood (a fuzzy measure). Equation E-2 states that the frequency of a scenario is reduced by the likelihood that the scenario has a consequence greater than C_j . When probability is used as the measure of likelihood, $L(C_j | S_i)$ is the exceedance probability of C_j using the CCDF for $C | S_i$ as discussed in Section E.2.3.

This is illustrated in Figure E-6.

Figure E-6. $L(C_j | S_i) = P(C_j | S_i)$

With belief/plausibility used as the measure of uncertainty for Equation E-2, $L(C_j | S_i)$ is not a point value but an interval, $[Bel(C_j | S_i), Pl(C_j | S_i)]$ where $Bel(C_j | S_i)$ is the belief that the consequence from scenario S_i exceeds C_j , and $Pl(C_j | S_i)$ is the plausibility that the consequence from scenario S_i exceeds C_j , as indicated in Figure E-7.

Figure E-7. $L(C_j|S_i) = [Bel(C_j|S_i), Pl(C_j|S_i)]$

There is uncertainty in the value of $L(C_j|S_i)$ since it is an interval. We cannot assign a single value to $L(C_j|S_i)$ as this would violate our original assignment of evidence by in effect assuming no “nonspecificity” in the assignment of evidence.⁶⁷ We will evaluate both an Lower Bound and an Upper Bound for Equation E-2, using $Bel(C_j|S_i)$ as the point value of $L(C_j|S_i)$ for the lower bound and using $Pl(C_j|S_i)$ as the point value of $L(C_j|S_i)$ for the upper bound.

The lower bound of each term in Equation E-2 will be evaluated as follows. Each interval for F_i will be multiplied by the point $Bel(C_j|S_i)$. The upper bound of each term in Equation E-2 will be evaluated as follows. Each interval of F_i will be multiplied by the point $Pl(C_j|S_i)$.

This process is explained using the following example. Consider three scenarios.

S_1 has the following focal elements for F_1 (per year):

- [1e-4, 1.5] with $m = 0.2$
- [3e-3, 0.04] with $m = 0.8$

S_1 has the following focal elements for $C|S_1$:

- [0, 10] with $m = 0.3$
- [1, 9] with $m = 0.7$

S_2 has the following focal elements for F_2 (per year):

- [8e-3, 0.12] with $m = 0.3$
- [0.02, 0.04] with $m = 0.7$

⁶⁷ A focal element that is an interval has a type of uncertainty called “nonspecificity;” a focal element that is a point value has no nonspecificity.

S_2 has the following focal elements for $C|S_2$:

[2, 15] with $m = 0.6$

[4, 12] with $m = 0.4$

S_3 has the following focal elements for F_3 (per year):

[1e-4, 0.06] with $m = 0.1$

[1e-3, 8e-3] with $m = 0.9$

S_3 has the following focal elements for $C|S_3$:

[3.7, 24] with $m = 0.45$

[6.6, 12] with $m = 0.55$

Consider consequence as the set $\{2, 4, 6, 8, 10, 12, 14, 16\}$. Using the BeliefConvolution code, the following results were obtained.

Table E-7. [Bel($C_j|S_i$), PI($C_j|S_i$)] For Example

Consequence C_j	[Bel($C_j S_1$), PI($C_j S_1$)]	[Bel($C_j S_2$), PI($C_j S_2$)]	[Bel($C_j S_3$), PI($C_j S_3$)]
2	[0, 1]	[0.4, 1]	[1, 1]
4	[0, 1]	[0, 1]	[0.55, 1]
6	[0, 1]	[0, 1]	[0.55, 1]
8	[0, 1]	[0, 1]	[0, 1]
10	[0, 0]	[0, 1]	[0, 1]
12	[0, 0]	[0, 0.6]	[0, 0.45]
14	[0, 0]	[0, 0.6]	[0, 0.45]
16	[0, 0]	[0, 0]	[0, 0.45]

For the lower bound, the focal elements are as follows.

Table E-8. Focal Elements for $F_i \cdot L(C_j|S_i)$ Lower Bound For Example

Consequence C_j	Focal Elements for Lower Bound: [Interval], Evidence		
	$F_1 \cdot L(C_j S_1)$	$F_2 \cdot L(C_j S_2)$	$F_3 \cdot L(C_j S_3)$
2	[0], ⁶⁸	[3.2e-3, 0.048], 0.3 ⁶⁹ [8e-3, 0.016], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
4	[0], 1	[0], 1	[5.5e-5, 0.033], 0.1 [5.5e-4, 4.4e-3], 0.55
6	[0], 1	[0], 1	[5.5e-5, 0.033], 0.1 [5.5e-4, 4.4e-3], 0.9
8	[0], 1	[0], 1	[0], 1

⁶⁸ [1e-4, 1.5]·[0] + [3e-3, 0.04]·[0] = [0] with evidence is 0.2·1 + 0.8·1 = 1.

⁶⁹ [8e-3, 0.12]·[0.4] = [3.2e-3, 0.048] with evidence 0.3·1 = 0.3. [0.02, 0.04]·[0.4] = [8e-3, 0.016] with evidence 0.7·1 = 0.7.

Consequence C_j	Focal Elements for Lower Bound: [Interval], Evidence		
	$F_1 \cdot L(C_j S_1)$	$F_2 \cdot L(C_j S_2)$	$F_3 \cdot L(C_j S_3)$
10	[0], 1	[0], 1	[0], 1
12	[0], 1	[0], 1	[0], 1
14	[0], 1	[0], 1	[0], 1
16	[0], 1	[0], 1	[0], 1

For the upper bound, the focal elements are as follows.

Table E-9. Focal Elements for $F_i \cdot L(C_j|S_i)$ Upper Bound For Example

Consequence C_j	Focal Elements for Upper Bound: [Interval], Evidence		
	$F_1 \cdot L(C_j S_1)$	$F_2 \cdot L(C_j S_2)$	$F_3 \cdot L(C_j S_3)$
2	[1e-4, 1.5], 0.2 [3e-3, 0.04], 0.8	[8e-3, 0.12], 0.3 [0.02, 0.04], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
4	[1e-4, 1.5], 0.2 [3e-3, 0.04], 0.8	[8e-3, 0.12], 0.3 [0.02, 0.04], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
6	[1e-4, 1.5], 0.2 [3e-3, 0.04], 0.8	[8e-3, 0.12], 0.3 [0.02, 0.04], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
8	[1e-4, 1.5], 0.2 [3e-3, 0.04], 0.8	[8e-3, 0.12], 0.3 [0.02, 0.04], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
10	[0], 1	[8e-3, 0.12], 0.3 [0.02, 0.04], 0.7	[1e-4, 0.06], 0.1 [1e-3, 8e-3], 0.9
12	[0], 1	[4.8e-3, 0.072], 0.3 [0.012, 0.024], 0.7	[4.5e-5, 0.027], 0.1 [4.5e-4, 3.6e-3], 0.9
14	[0], 1	[4.8e-3, 0.072], 0.3 [0.012, 0.024], 0.7	[4.5e-5, 0.027], 0.1 [4.5e-4, 3.6e-3], 0.9
16	[0], 1	[0], 1	[4.5e-5, 0.027], 0.1 [4.5e-4, 3.6e-3], 0.9

We will focus on the upper bound of $\text{Freq}(C_j) = F_1 \cdot L(C_j|S_1) + F_2 \cdot L(C_j|S_2) + F_3 \cdot L(C_j|S_3)$. We will calculate the Plausibility of exceedance of the upper bound of $\text{Freq}(C_j)$ for each C_j . For any event A, $\text{Belief}(A) = 1 - \text{Plausibility}(\bar{A})$ where $\bar{A}$ is “not A;” therefore, the Belief of “not exceeding $\text{Freq}(C_j)$ ” is one minus the Plausibility of “exceeding frequency $\text{Freq}(C_j)$.” We will summarize the upper bound as a family of curves, each curve corresponds to a specific belief. A point on a curve with belief Bel, is a frequency, $\text{Freq}(C_j)$, and a consequence, C_j ; our belief is Bel that the frequency of exceeding consequence C_j is *not* greater than $\text{Freq}(C_j)$. The results are given in Figure E-8, which provides results using Belief/Plausibility similar to those of Figure E-5 using Probability. Due to the interval nature of the data, the curves for 0.05 and 0.50 Belief are the same for this example.

Figure E-8. Exceedance Frequency of Consequence, Upper Bound using Belief/Plausibility

With 0.95 belief, the frequency of exceeding a consequence of 8 is not larger than about 1.6.
With 0.50 belief, the frequency of exceeding a consequence of 8 is not larger than about 0.09.

This page intentionally left blank.

Glossary

This glossary presents practical definitions of various terms used in this report. As appropriate, the main body of the report provides precise mathematical definitions of these terms.

Aleatory	Uncertainty due to randomness. Stochastic uncertainty.
Ambiguity	Uncertainty associated with the likelihood of an event.
Belief	A measure of the likelihood that an event <i>will</i> happen.
Convolution	Propagation of uncertainty under a combination of uncertain variables.
Crisp Set	A set whose members can only have full membership.
Discord	Ambiguity due to evidence assigned to different focal elements.
Epistemic	Uncertainty due to state of knowledge.
Evidence	A measure of the likelihood of a focal element.
Focal Element	An event, or equivalently a subset of a sample space, to which evidence is assigned.
Fuzzy Set	A set whose members can have partial membership.
Likelihood	A measure of the certainty of an event.
Linguistic	A word used to describe an event.
Necessity	Belief when the focal elements are nested.
Noninteraction	For belief, noninteraction means that each focal element for a random vector is a Cartesian product of focal elements of the constituent random variables, and the evidence for the focal element of the random vector is the product of the evidence of the focal elements for the constituent random variables.
Nonspecificity	Ambiguity due to focal element(s) not being singletons.
Plausibility	A measure of the likelihood that an event <i>could</i> happen.
Possibility	Plausibility when the focal elements are nested.
Probability	A Kolmogorov probability measure. Both belief and plausibility become probability if the focal elements are singletons.

Sample Space	A set containing all possible mutually exclusive outcomes for a subject of interest.
Strife	See Discord.
Uncertainty	Inability to precisely know or categorize the outcome of a process of interest.
Universe of Discourse	See Sample Space.
Vagueness	Uncertainty in categorizing a known outcome.

References

- Balakrishna, V.K., 1991, *Introductory Discrete Mathematics*, Prentice-Hall International, Inc.
- Crystal Ball software, version 7.2, Decisioneering, Inc.
- Darby, John, 2004, "Estimating Terrorist Risk with Possibility Theory," Los Alamos National Laboratory, LA-14179.
- Darby, J., Bush, B., Eisenhower, S., Bott, T., 2003, "Methodology for Optimizing Allocation of Resources to Protect Infrastructure against Acts of Terrorism," LA-UR 04-0590, Dec. 8, 2003.
- Dougherty, Edward R. 1990, *Probability and Statistics for the Engineering, Computing, and Physical Sciences*, Prentice Hall.
- Dubois, D., and Prade, H, 1988, *Possibility Theory, An Approach to Computerized Processing of Uncertainty*, Plenum Press English Translation
- Ferson, Scott, et al., 2003, "Constructing Probability Boxes and Dempster-Shafer Structures," SAND2002-4015, January, 2003.
- Ferson, S., 2003, *RAMAS Risk Calc 4.0 Software: Risk Assessment with Uncertain Numbers*, Lewis Publishers.
- Ferson, Scott, et al., 2004, "Dependence in Probabilistic Modeling, Dempster-Shafer Theory, and Probability Bounds Analysis," SAND2004-3072, October, 2004.
- Helton, J.C., Johnson, J.D., and Oberkampf, W. L., 2004, "An Exploration of alternative approaches to the representation of uncertainty in model predictions," *Reliability Engineering and System Safety* 85, pp. 39-71.
- Helton, J.C., Johnson, J.D., Oberkampf, W. L., Storlie, C.B., "A Sampling-Based Computational Strategy for the Representation of Epistemic Uncertainty in Model Predictions with Belief Theory," submitted to *Computer Methods in Applied Mechanics and Engineering* in 2006.
- Kaplan, S., 1981, "On the Method of Discrete Probability Distributions in Risk and Reliability Calculations-Application to Seismic Risk Assessment," *Risk Analysis*, Vol. 1, No. 3, pp. 189-196.
- Kaplan, S., and Garrick, B.J., 1981, "On the Quantitative Definition of Risk," *Risk Analysis*, Vol. 1 No. 1, pp. 11-27.
- Klir and Yuan, 1995, *Fuzzy Sets and Fuzzy Logic, Theory and Applications*, Prentice Hall PTR.
- Merkle, P., 2006, "Extended Detection and Defense: 1. Adversary-Defender Modeling Grammar for Vulnerability Analysis and Threat Assessment," SAND2006-1484, Printed March 2006.

Oberkampf, W. L., and Helton, J.C., 2005, "Evidence Theory for Engineering Applications," Chapter 10 of *Engineering Design Reliability Handbook*, Nikolaides, E., Ghiocel, D.M., and Singhal, S., eds., CRC Press.

Shafer, S., 1976, *A Mathematical Theory of Evidence*, Princeton University Press.

US Nuclear Regulatory Commission, 1981, Fault Tree Handbook, NUREG-0492, January, 1981.

Yager, R., 1986, "Arithmetic and other operations on Dempster Shafer structures," *International Journal of Man-Machine Studies*, 25: pp. 357-366.

Yager, R.R., J. Kacprzyk, and M. Fedrizzi, 1994, *Advances in the Dempster-Shafer Theory of Evidence*, JohnWiley and Sons.

Distribution

3	MS0757	John L. Darby, 6442
1	MS0757	Carla Ulibarri, 6442
1	MS 0839	John Cummings, 07000
1	MS 0779	Jon Helton, 01533
2	MS 9018	Central Technical Files, 08944
2	MS 0899	Technical Library, 04536

EXTERNAL DISTRIBUTION

1	Scott Ferson Applied Biomathematics 100 North Country Road Setauket, NY 11733
1	Ronald Yager Machine Intelligence Institute Iona College New Rochelle, NY 10801
1	Donald Sunil D6, Los Alamos National Laboratory P.O. Box 1663, MS K557 Los Alamos, NM 87545

This page intentionally left blank.