SAND2006-5769C

Evaluating Risk from Acts of Terrorism with Belief and Fuzzy Sets

SAND XXXX

Presented October 19, 2006 at
IEEE 2006 International Carnahan Conference
On Security Technology
Lexington, KY

John Darby
Sandia National Laboratories

jdarby@sandia.gov 505-284-7862

Presentation Topics

- Risk
  - Intentional acts are different from Random acts
- Uncertainty
  - Epistemic uncertainty
  - Ambiguity and Vagueness
- Adversary/Defender Model for Evaluation of Risk from Intentional Acts of Terrorism

Risk of Terrorist Attack

- Risk = f x P x C
  - Risk of a successful terrorist attack
  - f is frequency of attack
  - P is probability adversaries succeed given attack
  - C is consequence given adversaries succeed
- Risk depends on the Adversary Scenario
  - Scenario: Adversary Resources, Target, Attack Plan
- Why Evaluate Risk?
  - Allocation of Resources for Protection

Risk of Terrorist Attack

- What is frequency f_i for a Scenario "i"?
- Which "i" scenarios?

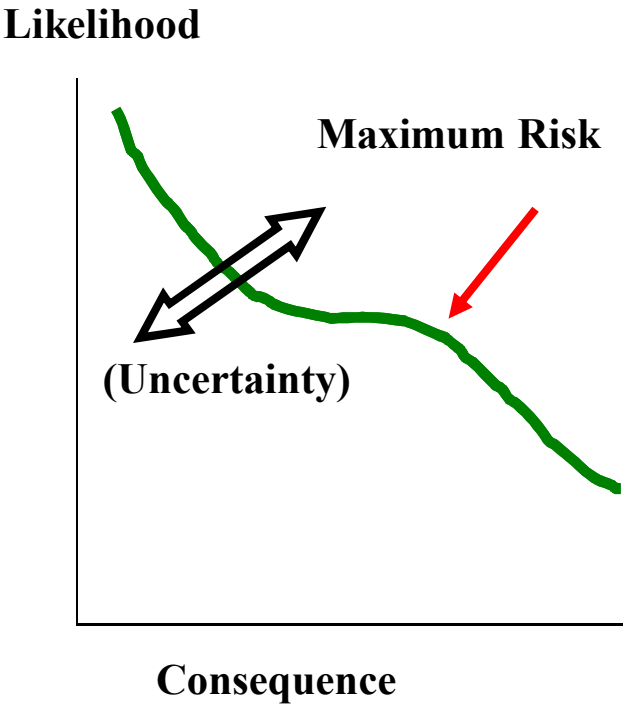
$$Risk_i = f_i \times P_i \times C_i$$

Adversary: Select scenario "i" from choice of *all* scenarios

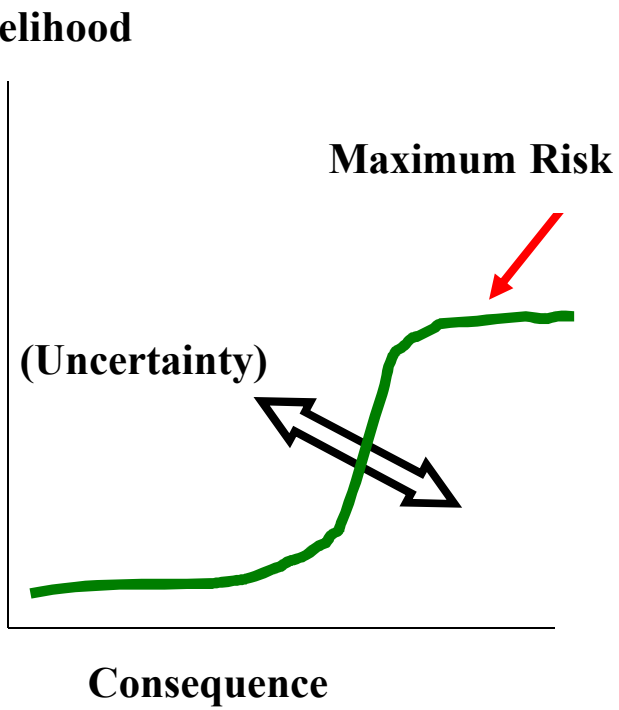
Defender: Evaluate the *single* scenario "i"

Safety Risk vs. Terrorist Risk

Safety Risk (Random)



Terrorist Risk (Intentional)



Uncertainty

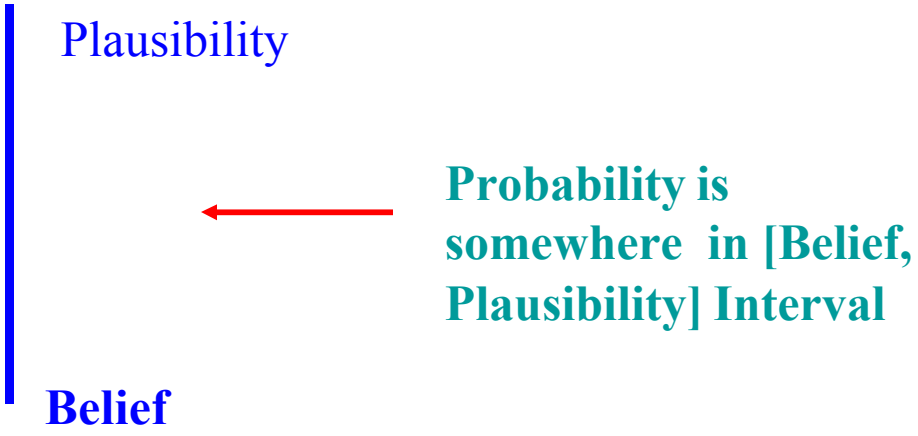
- Ambiguity
  - Uncertainty as to what will occur in the future
    - Dow Jones Industrial Average Close on Dec. 31, 2006
      - Will be one value
      - Ambiguity as to what that value will be
- Vagueness
  - Uncertainty as how to categorize a known outcome
    - Dow Jones close is 11,300 on Dec. 31, 2006
      - Is this “High” ?
      - What do you mean by “High”?
  - Vagueness can be expressed Linguistically (Words)

Belief/Plausibility for Epistemic Uncertainty

- For a Fair Coin
  - Uncertainty is Aleatory (random)
  - Probability Heads is ½
  - Probability Tails is ½
- But if we cannot toss coin, we do not know coin is fair, we do not even knows if coin has Heads and Tails
  - May not be Fair Coin (may be Weighted for Tails)
  - May be Two-Headed or Two-Tailed Coin
  - Epistemic (state of knowledge) uncertainty
  - Insufficient information to assign Probability to Heads and Tails
  - For Total Ignorance
    - Belief/Plausibility for Heads is 0/1
    - Belief/Plausibility for Tails is 0/1
- With more information (actually tossing the coin) we can reduce Epistemic Uncertainty
  - If at least one Heads and one Tails occur in a series of tosses, we know coin has Heads and Tails
  - Many tosses needed to assess if coin is fair
- For Fair Coin we cannot reduce aleatory uncertainty

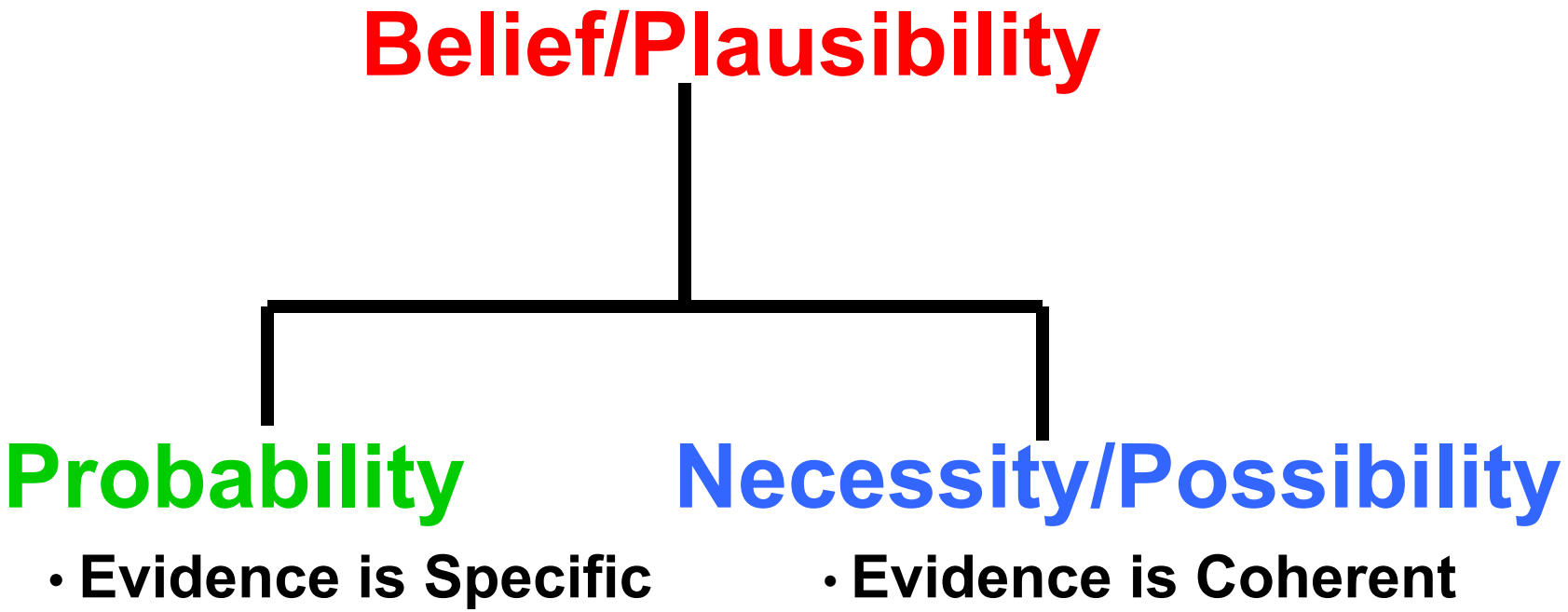
Belief and Plausibility

- Belief / Plausibility form a Lower / Upper Bound for Probability
- Belief is what probability will be
- Plausibility is what probability could be



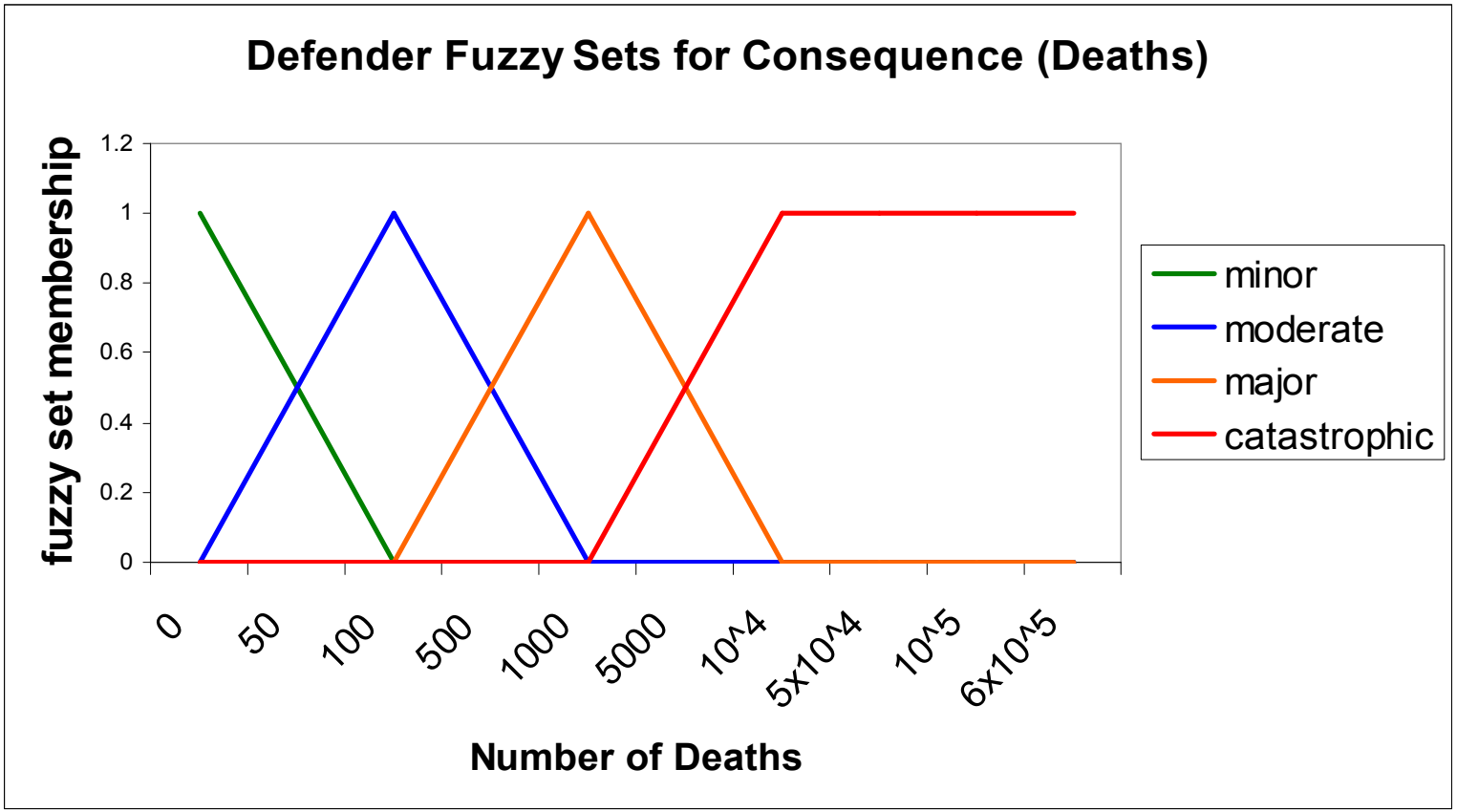
- Similar to a Confidence Interval for a Parameter of a probability distribution; a confidence measure that parameter is in interval, but exactly where in interval is not known
- Belief/Plausibility both reduce to Probability if Evidence is Specific

Measures of Ambiguity



Fuzzy Sets represent Vagueness

- Consequence (Deaths) are “Major”
  - “Major” is fuzzy: between *about* 500 and *about* 5000 deaths



Adversary/Defender Model

- Adversary (them)
- Defender (us)
- Adversary and Defender each have different goals and different states of knowledge
- Risk = Threat x Vulnerability x Consequence
  - Defender goal: Minimize Risk with available resources
  - Adversary goal: Maximize Consequence with available resources (working assumption)
- Adversary is the Threat
  - Epistemic Uncertainty for Vulnerability and Consequence
- Defender knows Vulnerability and Consequence
  - Epistemic Uncertainty for Threat

Defender Model for a Scenario

- Risk = f x P x C = f x (1 – P_E) x C
  - f is frequency of attack
  - P is probability of success given attack
    - P_E is effectiveness of security system in defeating attack
  - C is consequence given success of attack
- f, P, and C are random variables with uncertainty
- Degrees of Evidence to f, P, C based on state of knowledge
- Numerical Convolution using Belief/Plausibility Measure of Uncertainty

Example of Defender Model

- f and P have considerable epistemic uncertainty
- C has only aleatory uncertainty (for this example)
- C is Deaths

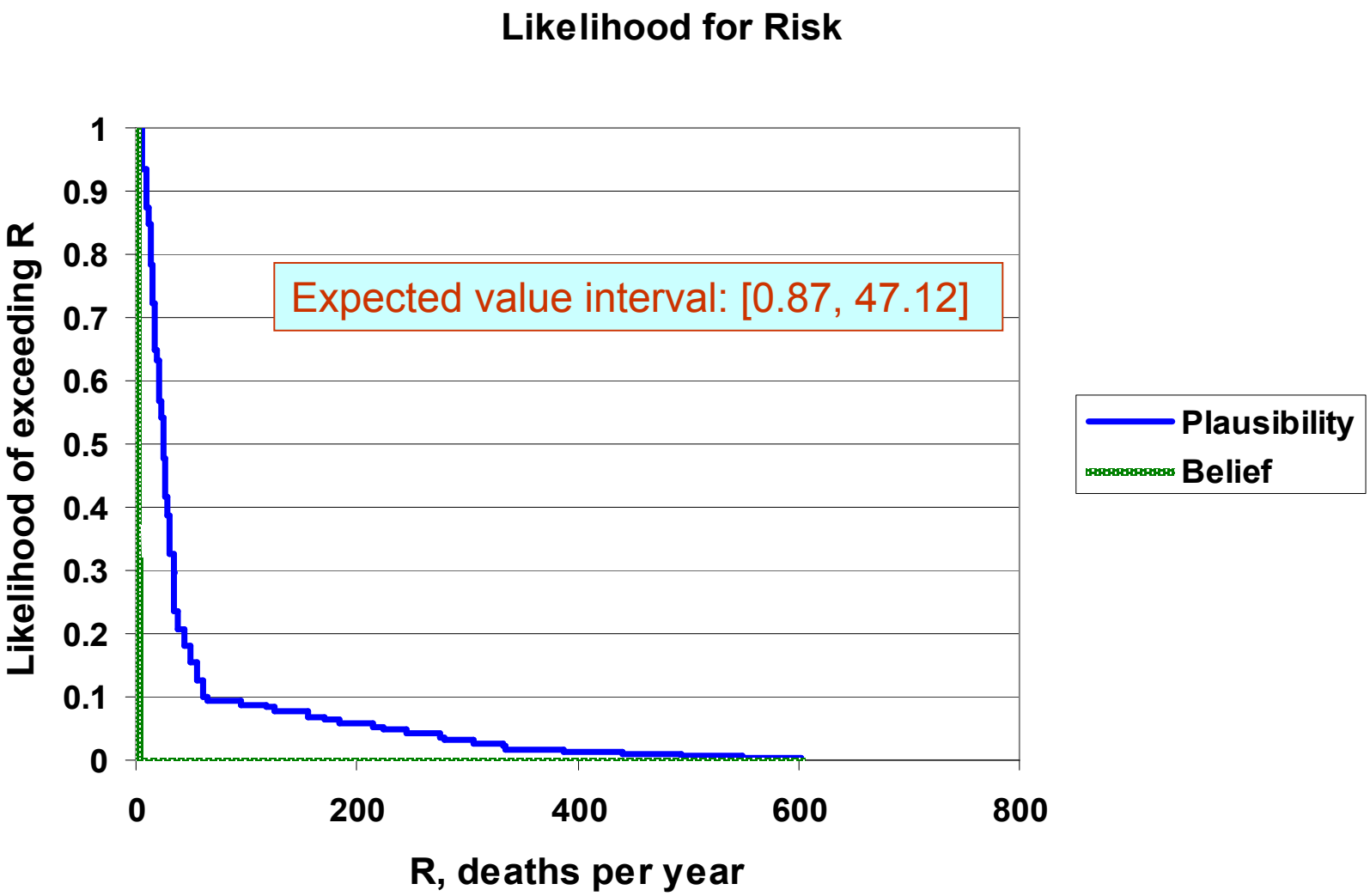
Example of Defender Model

- Evidence for frequency of attack, f, per year
  - 0.1 to interval [1 x 10^{-4}, 0.1]
  - 0.9 to the interval [1 x 10^{-3}, 0.01]
- Evidence for probability of adversary success, P
  - 0.3 to interval [0.1, 0.9]
  - 0.7 to interval [0.3, 0.5]

Example of Defender Model

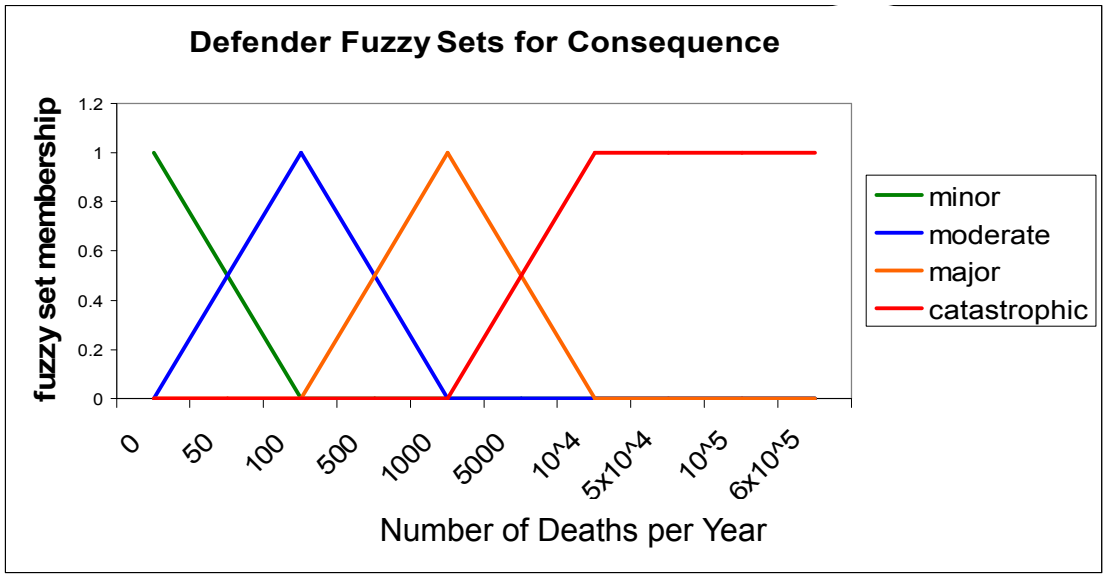
- Evidence for consequence, C, deaths
  - Uniform probability distribution
    - Minimum 1000
    - Maximum 7000
    - Mean 4000

Example of Defender Model

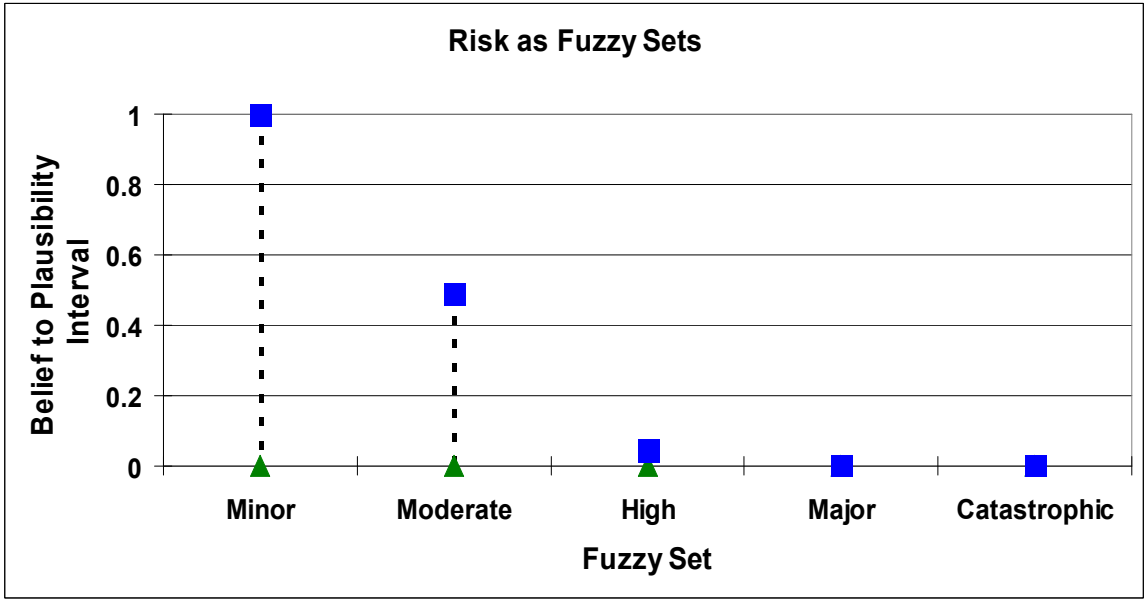


Likelihood for Risk using Fuzzy Sets

Define Fuzzy Sets For Risk:

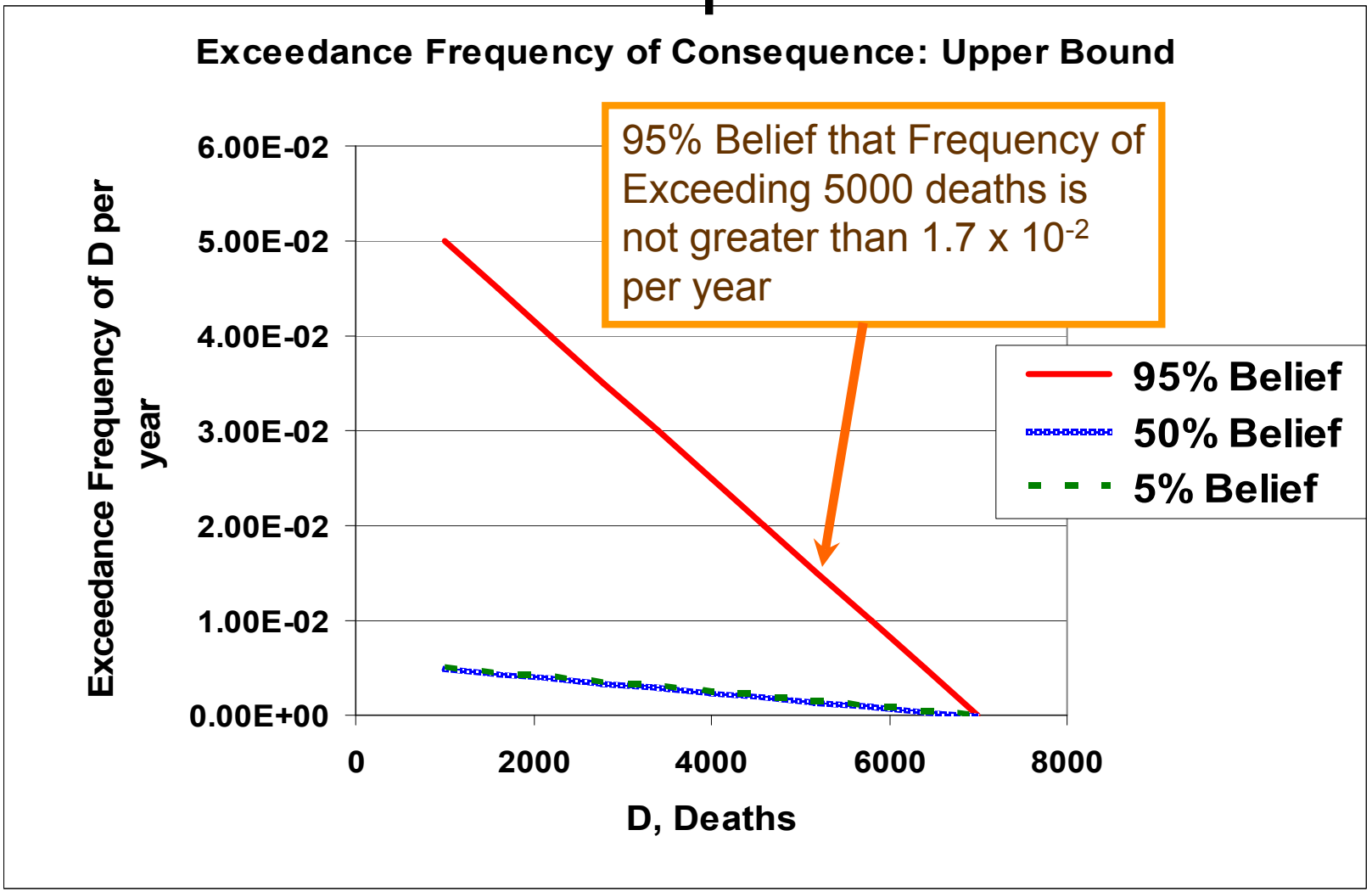


Likelihood of Fuzzy Sets, [Belief, Plausibility]:



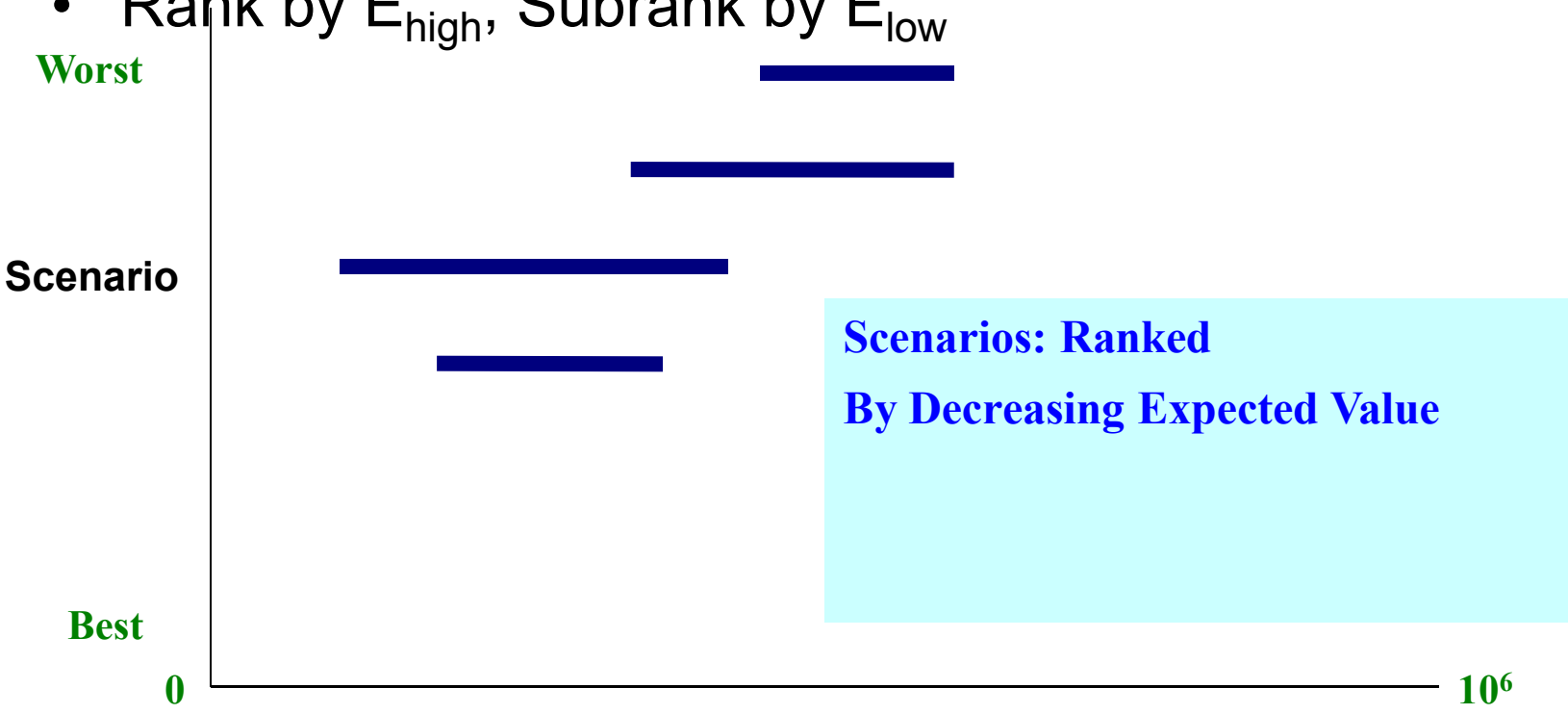
NNSA
National Nuclear Security Administration

Exceedance Frequency of Consequence



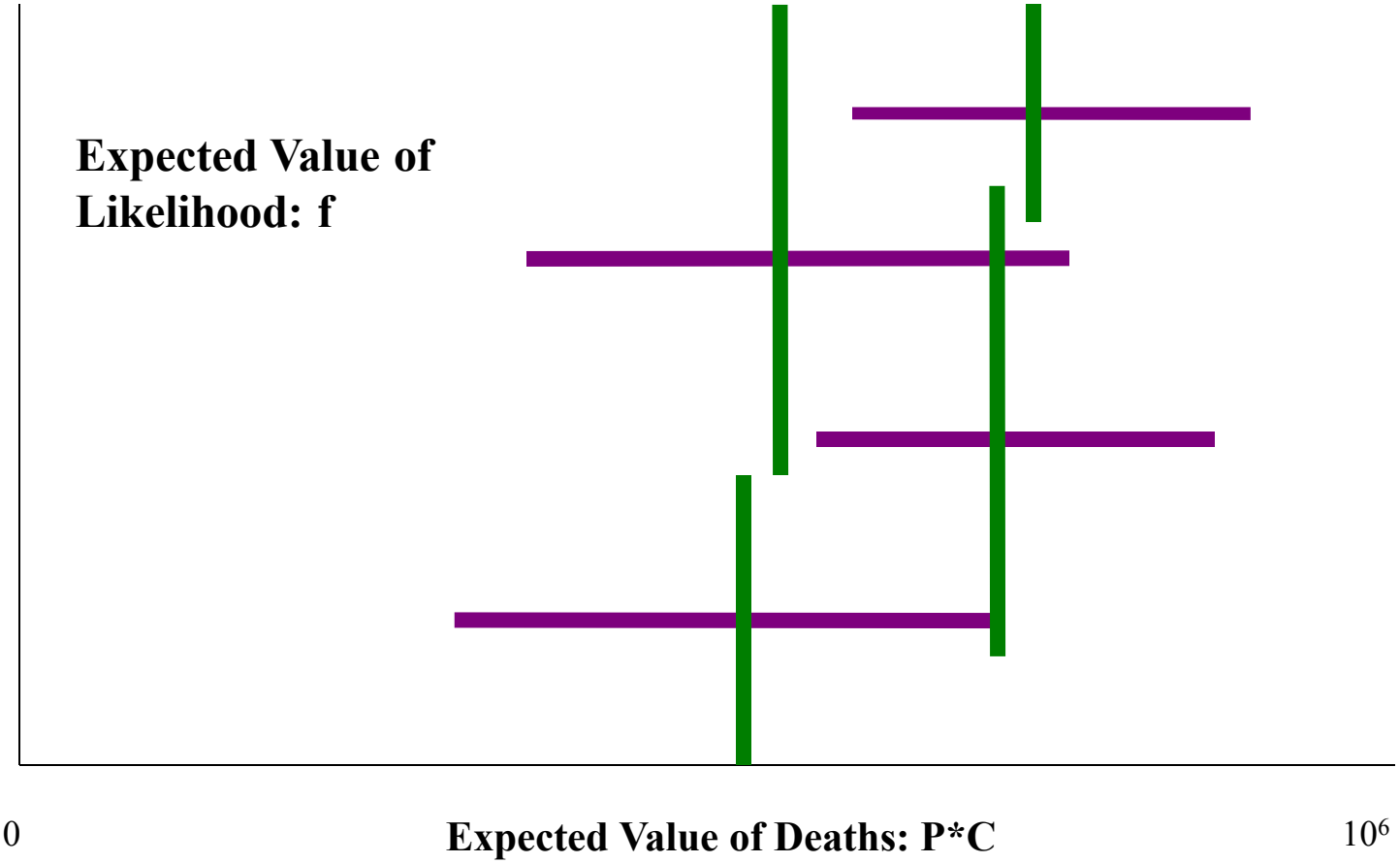
Defender Ranking of Scenarios

- For Belief/Plausibility Expected Value is an Interval $[E_{low}, E_{high}]$. Reduces to point (Mean) for Probability
- Rank by E_{high}, Subrank by E_{low}



jdarby@sandia.gov 505-284-7862

Next Level Of Detail for Defender Ranking



Adversary Model

- Use Surrogate Adversary (Special Forces)
- Adversary has Choice
  - All Variables of concern must be "OK" or

    Adversary will pick another scenario
    - Recruit Insider? Not unless already placed
    - Large Team? Concern about being detected by Intelligence
    - Uncertainty?
      - Door was green yesterday, is red today…What else changed?
- Variables for Adversary Decision are Not all Numeric
  - Consequence = Deaths x Economic Damage x Fear in Populace x Damage to National Security x Religious Significance x …..
  - Deaths and Economic Damage are numeric
  - Fear in Populace, Damage to National Security, and Religious Significance are not numeric

Adversary Model

- Purely Linguistic Model
- Develop Fuzzy Sets for Each Variable
- Develop Approximate Reasoning Rule Base for Linguistic Convolution of Variables to Reflect Scenario Selection Decision Process
- We are not the Adversary, we try to think like the Adversary
  - Considerable Epistemic Uncertainty
  - Use Belief/Plausibility Measure of Uncertainty Propagated up the Rule Base

Adversary Model

- Assume Adversary Goal is Maximize Expected Consequence
  - Expected Consequence ≡ P x C
  - Expected Consequence is Adversary estimate of Consequence, C, weighted by Adversary estimate of Probability of Success, P

Example of Adversary Model

- Rule Base and Variables

Expected Consequence

- Probability Of (Adversary) Success
  - Probability Resources Required Gathered Without Detection
  - Probability Information Required Can Be Obtained
  - Probability Physical Security System can be Defeated
- Consequence
  - Deaths
  - Damage To National Security

Example of Adversary Model

- Linguistics: Fuzzy Sets
  - Expected Consequence = {No, Maybe, Yes}
  - Probability Of Success = {Low, Medium, High}
  - Consequence = {Small, Medium, Large}
  - Probability Resources Required Gathered Without Detection = {Low, Medium, High}
  - Probability Information Required Can Be Obtained = {Low, Medium, High}
  - Probability Physical Security System can be Defeated = {Low, Medium, High}
  - Deaths = {Minor, Moderate, Major, Catastrophic}
  - Damage To National Security = {Insignificant, Significant, Very Significant}

Example of Adversary Model

Rule Base for Expected Consequence

Probability Of Success *Expected Consequence* Consequence	Low	Medium	High
Small	*No*	*No*	*No*
Medium	*No*	*No*	*Maybe*
Large	*No*	*Maybe*	*Yes*

Example of Adversary Model

Portion of Rule Base for Probability Of Success

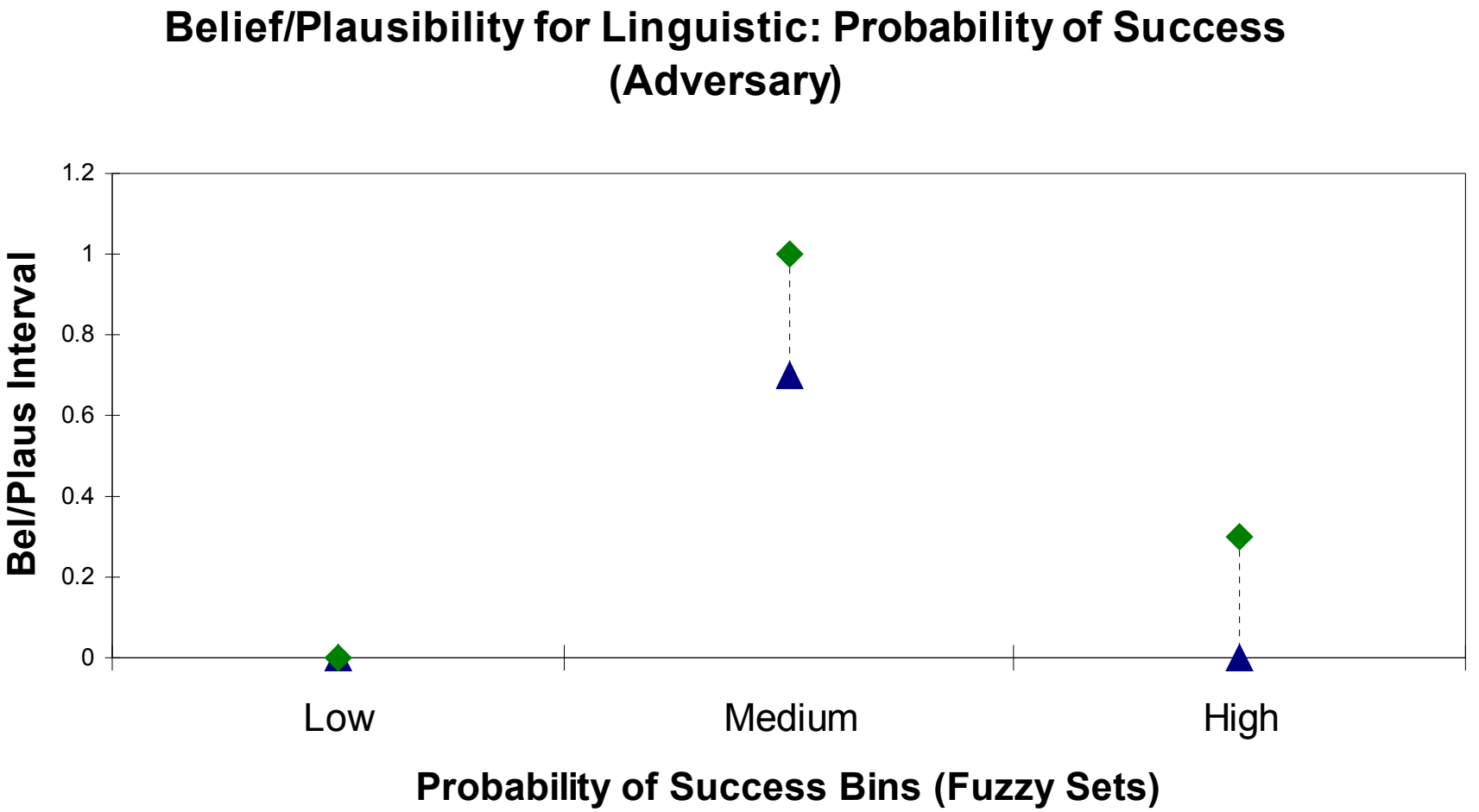
Probability Physical Security System can be Defeated = High

Probability Resources Required Gathered Without Detection ***Probability Of Success*** **Probability Information Required can Be Obtained**	**Low**	**Medium**	**High**
Low	***Low***	***Low***	***Low***
Medium	***Low***	***Medium***	***Medium***
High	***Low***	***Medium***	***High***

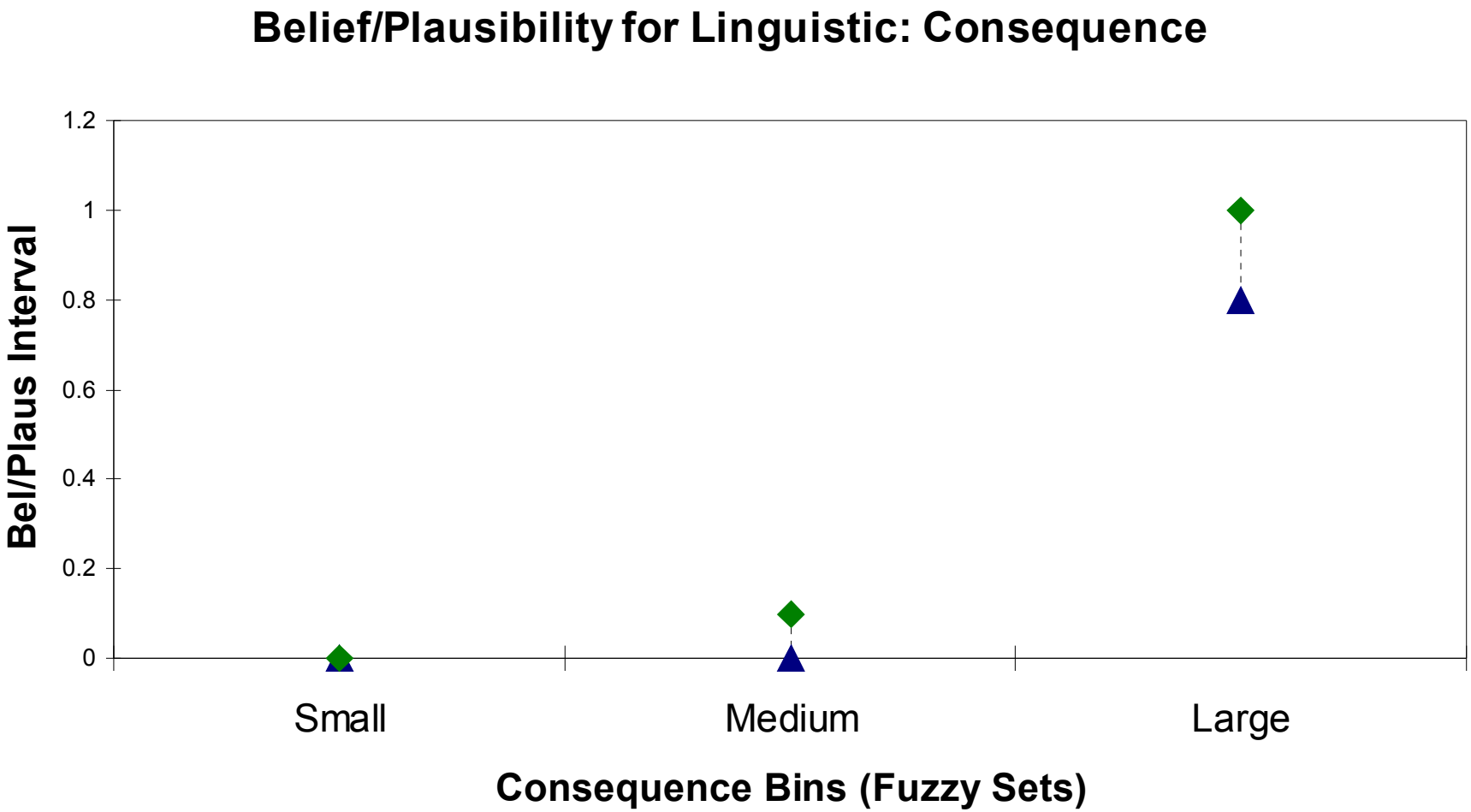
Example of Adversary Model

- Focal Elements (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}

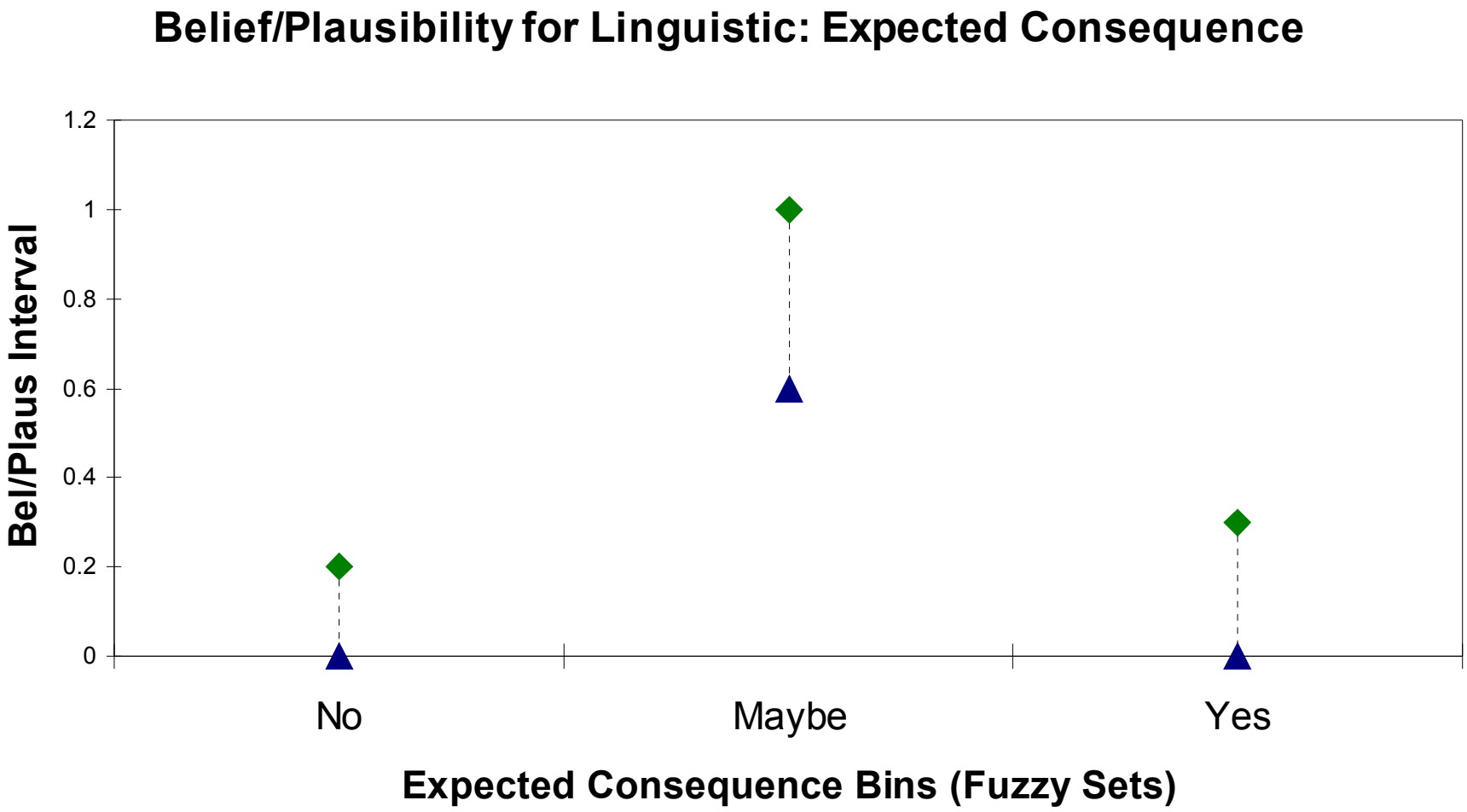
Example of Adversary Model



Example of Adversary Model



Example of Adversary Model



Ranking of Scenarios from Adversary Model

- Defender (thinking like Adversary) Ranks by Plausibility
  - 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
- Note: Actual Adversary using the Model would Rank by Belief
  - “We will not attempt a scenario unless we *believe* it will succeed”… Osama

Software Tools

- Numerical Evaluation of Risk for Defender
  - BeliefConvolution Java code (written by author)
  - RAMAS RiskCalc
- Linguistic Evaluation for Adversary
  - LinguisticBelief Java code (written by author)
  - LANL LEDTools

LinguisticBelief Code