



Risk Analysis for Critical Infrastructure and Key Asset Protection: *Methods and Challenges*

Bilal M. Ayyub, Professor and Director

CENTER FOR TECHNOLOGY AND SYSTEMS MANAGEMENT

University of Maryland at College Park

Terrorism Risk Analysis – A CREATE Research Symposium

This project is partly funded by the Homeland Security Institute (HSI). Opinions expressed in this presentation are of the authors and do not necessarily reflect the opinions of HSI.

Objectives

- Definitions and terminology
- National strategy for homeland security 2002
- Risk-informed methods for protecting critical infrastructure and key assets
- Challenges and needs

Risk Terminology

Probability: A measure of likelihood (or chance)

Failure consequences: Economic, human, environmental or other losses as a result of an event

Risk Terminology

Risk: The potential for loss or harm to systems due to the likelihood of an unwanted event and its adverse consequences

Safety: The judgment of risk tolerance

Elements of Risk Analysis:

- ✓ What can go wrong?
- ✓ What are the occurrence likelihoods?
- ✓ What are the consequences?

Risk Terminology

Elements of Security Risk Analysis:

- ✓ What are the threat scenarios?
- ✓ What are the occurrence and success likelihood?
- ✓ What are the consequences?

Risk Terminology

Event Tree: A logic diagram that begins with an initiating event, and progresses through a series of branch points that represent credible alternative outcomes along the path to an overall result (either success or undesired consequences)

Threat: Any indication, circumstance, or event with the potential to cause the loss of or damage to an asset or a population. It can be defined based on the intention and capability of an adversary to undertake actions that would be detrimental to assets or populations

Risk Terminology

Vulnerability: Any weakness in an asset or infrastructure's design, implementation, or operation that can be exploited by an adversary

- ✓ Measured as the success probability for a particular threat scenario

Considerations in Limiting Risk

- Not every risk is avoidable
- Risks are uncertain (subjective information)
- Wealthier is healthier (affordability)
- Countermeasures can have adverse side effects
- More lives would be saved if risks are prioritized

National Strategy for Homeland Security 2002

- Prevent terrorist attacks within the United States
- Reduce America's vulnerability to terrorism
- Minimize the damage and recover from attacks that do occur.

Department of Homeland Security: Strategic Plan

- Awareness
- Prevention
- Protection
- Response
- Recovery
- Organization Excellence
- Communication

ASME Project Objectives

- Produce a Guidance Document containing overall methodology and a common framework for risk analysis for homeland security decision-making
 - ✓ Provide common terminology
 - ✓ Provide common metrics that can be used to compare risks across sectors
 - ✓ Provide a common basis for reporting results
 - ✓ Provide a basis for informing resource allocation decisions
 - Countermeasures
 - Consequence mitigation actions

Project Scope

- Applicable to critical asset sectors including:
 - ✓ Nuclear power plants
 - ✓ Nuclear spent fuel storage facilities
 - ✓ Chemical plants
 - ✓ Petroleum refineries
 - ✓ Liquefied Natural Gas (LNG) storage facilities
 - ✓ Transportation (subways, railroads and highways including bridges and tunnels)
 - ✓ Electric power distribution
- Incorporate attributes of existing methods

Challenges and Needs

- System definition
 - ✓ System boundaries
 - ✓ Analysis resolution
 - ✓ Interdependencies and complexity
 - ✓ Uncertainty-based definition and hierarchical structuring of information
- Challenges
 - ✓ System interactions
 - ✓ Distributed systems (e.g., water/food distribution, transportation, postal, Internet)
 - ✓ System efficiency as a threat
 - ✓ Threat emergence

A Classification of Uncertainty

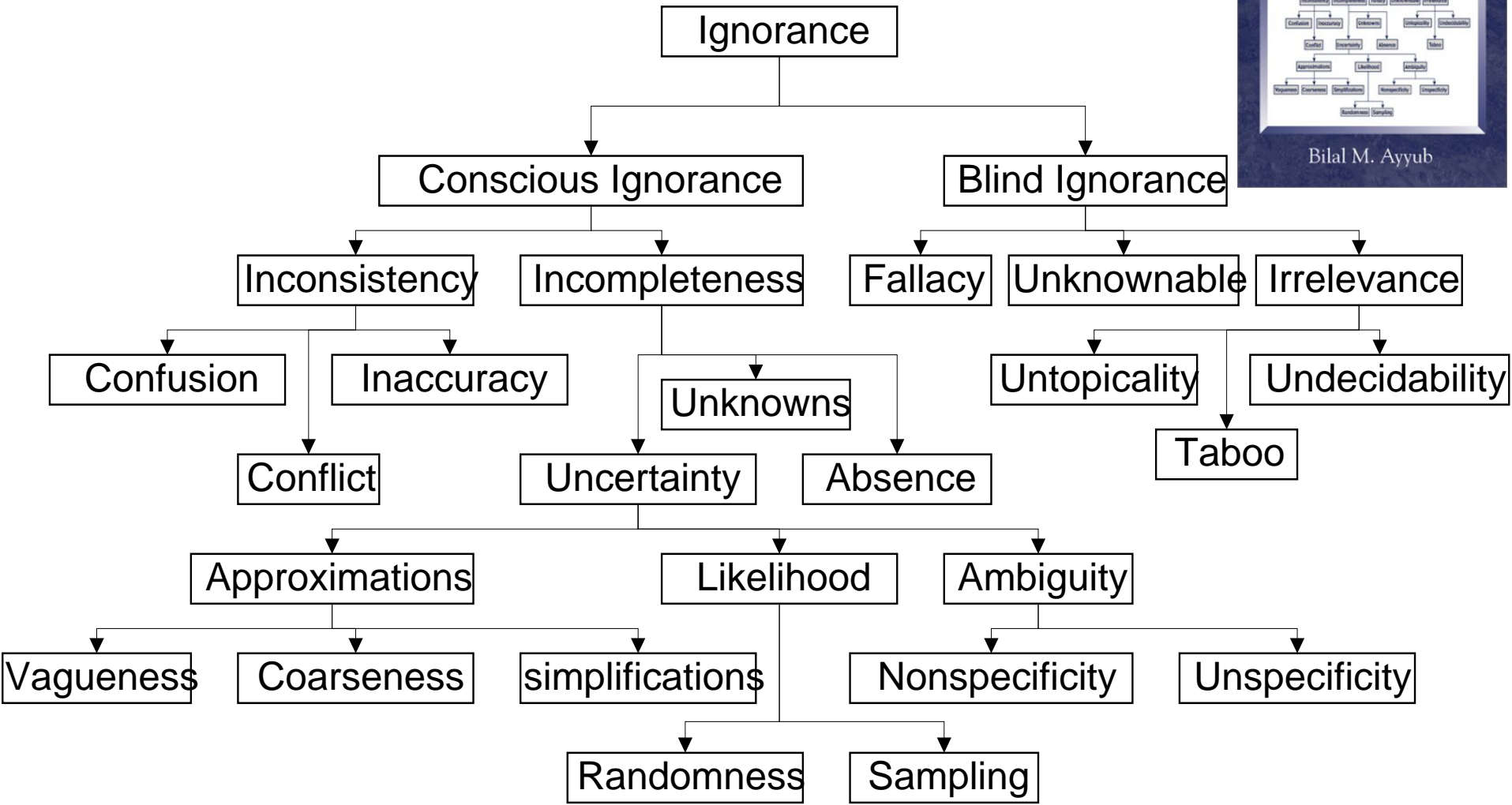
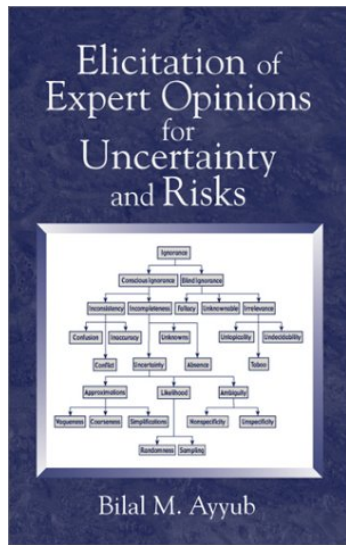
- **Aleatory uncertainty** is defined as the inherent, random or non-reducible uncertainty, such as material strength randomness (\bar{P})
- **Epistemic uncertainty** is defined the knowledge-based, subjective uncertainty that can be reduced with the collection of data or attainment of additional knowledge (\hat{P})
- These two primary uncertainty types can be combined as:

$$P = \bar{P} \hat{P} \quad COV(P) = \sqrt{[COV(\bar{P})]^2 + [COV(\hat{P})]^2}$$

Quantum Knowledge

- **Reality is perceived as a continuum** in its composition of objects, concepts and propositions
- **Knowledge is constructed in quanta** by humans to meet their cognitive abilities and limitations
- **Quantum knowledge** leads to ignorance -- manifested in the form of **blind ignorance** and **conscious ignorance**
- **Uncertainty** (generally **ignorance**) needs to be portrayed in meaningful manner/ forms/ measures for decision making

Ignorance Hierarchy



Open World Assumption

- Statistical Analysis of Sequences
- Transferable Belief Model
 - ✓ Theory of Evidence
 - ✓ Combination rules of evidence
 - ✓ The contradiction in the body of evidence is allocated to unseen events

Challenges and Needs

- Threat analysis (a threat cycle)
 - ✓ Asset selection
 - ✓ Acquisition of knowledge
 - ✓ Acquisition of weapon materials
 - ✓ Weapon development or acquisition
 - ✓ Weapon delivery and attack
 - ✓ Success probability
- Challenges
 - ✓ Using an asset as a weapon
 - ✓ Completeness – blind ignorance

Challenges and Needs

➤ Scenario Development

- ✓ Define primary components (include time and resources):
 - Asset selection
 - Threat
 - Vulnerability
 - Consequence
- ✓ Develop lists of states or possibilities for each component
- ✓ Define credible combinations as scenarios

➤ Challenges and needs

- ✓ Completeness – blind ignorance
- ✓ Metrics and measures (compatibility and dependence)

Challenges and Needs

- Consequences
 - ✓ Types
 - ✓ Cascading effects
 - ✓ Interdependencies
 - ✓ Valuation
- Challenges and needs
 - ✓ Higher-level consequences
 - ✓ Uncertainties

Challenges and Needs

- Dynamic nature of threats
 - ✓ Intelligent threats
 - ✓ Dynamic and engaged
- Challenges and needs
 - ✓ Countermeasures and mitigation strategies
 - ✓ Creation of attractors for threats
 - ✓ Redundancy: physical versus organizational
 - ✓ Indicators and warnings for threats

Challenges and Needs

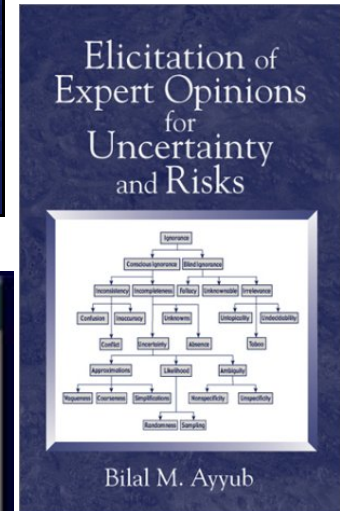
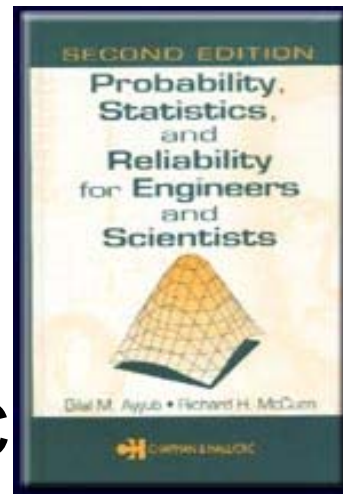
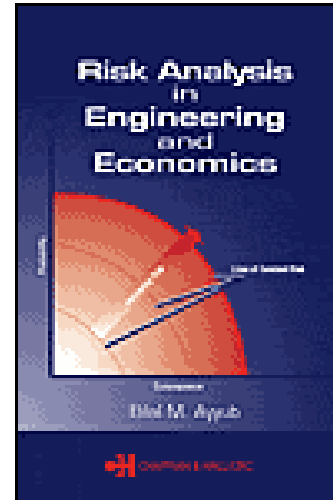
- Data types and sources
 - ✓ Limited or non-existent data
 - ✓ Expert opinion elicitation
- Challenges and needs
 - ✓ Unintentional biases
 - ✓ Elicitation process and protocol
 - ✓ Representation of opinions
 - ✓ Aggregation of opinions
- Knowledge Elicitation Process

Challenges and Needs

- Security and freedom of information
 - ✓ Higher levels of analysis require information sharing
 - ✓ Security: competitors and adversaries
- Challenges and needs
 - ✓ Security clearance at the federal level
 - ✓ Information-access denial at the state level
 - ✓ Freedom of Information Act

Selected References

- Ayyub, B.M., Risk Analysis in Engineering and Economics, Chapman & Hall/CRC Press, 2003.
- Ayyub, B. M. , Elicitation of Expert Opinions for Uncertainty and Risks, CRC Press, FL, 2001.
- Ayyub, B.M., and McCuen, R., Probability, Statistics and Reliability for Engineers and Scientists, Chapman & Hall/CRC Press, 2003.



Elicitation of
Expert Opinions
for
Uncertainty
and Risks



Bilal M. Ayyub