ENCE 620 – Risk Analysis for Engineering

2. Terminology & Fundamental Risk Methods

Textbook: Risk Analysis in Engineering and Economics

Introduction

- Risk can be associated with all aspects in our life and all projects
- Risk is present in various forms and levels
  - Small domestic projects, such as adding a deck to a house
  - Large multibillion-dollar projects, such as developing and producing a space shuttle

Introduction (cont'd)

- The chapter objective is to introduce needed terminology and methods for performing risk analysis, management and communication
- This chapter covers:
  - Risk and its dimensions
  - Risk assessment and management processes
  - Fundamental analytical tools needed for this purpose

Risk Terminology

- Technical terms that are needed for presenting risk-based technology methods and analytical tools include:
  - Hazard
  - Reliability
  - Event Consequences
  - Risks
  - Performance
  - Risk-Based Technology

Risk Terminology

- **Hazard**
  - A hazard is an act or phenomenon posing potential harm to some person(s) or thing(s), i.e., a source of harm, and its potential consequences
  - Hazards need to be identified and considered in projects' lifecycle analyses since they could pose threats and could lead to project failures

Risk Terminology (cont'd)

- **Reliability**
  - Reliability of a system or a component is defined as the system or component ability to fulfill its design functions under designated operating or environmental conditions for a specified time period
  - Reliability is, therefore, the occurrence probability of the complementary event to failure as provided in the following expression:

$$\text{Reliability} = 1 - \text{Failure Probability}$$

Risk Terminology (cont'd)

- **Event Consequences**
  - *Consequence* – is the immediate, short-, and long-term effects of an event affecting objectives, e.g., an explosion of a chlorine storage tank
  - Each failure of a system has some consequences
  - A failure could cause economic damage, environmental damage, injury or loss of human life, or other possible outcomes
  - Consequences need to be quantified using relative or absolute measures for various consequence types to facilitate risk analysis

Risk Terminology (cont'd)

- **Risks**
  - Risk can be defined as the potential losses resulting from an exposure to a risk event or hazards
  - Risk can be viewed to be a multi-dimensional quantity that includes
    - event occurrence probability
    - event occurrence consequences
    - consequence significance
    - population at risk

Risk Terminology (cont'd)

- **Risks (ISO 31000: 2009)**
  - Risk is defined as "effect of uncertainty on objectives"
    - An effect is a deviation from the expected that can be positive and/or negative effect
    - Objectives can have different aspects, such as financial, health and safety, and environmental goals, and can apply at different levels, such as strategic, organization-wide, project, product and process

Risk Terminology (cont'd)

- **Risks (ISO 31000: 2009)**
  - Risk is often characterized by reference to potential events and consequences, or a combination of these as provided in the commonly used definition
  - Risk is often expressed in terms of a combination of the consequences of an event, including changes in circumstances, and the associated likelihood of occurrence as provided in the commonly used definition

Risk Terminology (cont'd)

- **Risks and Opportunities**
  - Gains could results from identifying opportunities and meeting or exceeding objectives

Risk Terminology (cont'd)

- **Risks (cont'd)**
  - However, it is commonly measured as a pair of the probability of occurrence of an event, and the outcomes or consequences associated with the event's occurrence
  - This pairing can be represented by the following equation:

$$Risk \equiv \left[(p_1, c_1), (p_2, c_2), \ldots, (p_i, c_i), \ldots, (p_n, c_n) \right] \qquad (1)$$

p_i = occurrence probability of an outcome or event i

c_i = occurrence consequences or outcomes of the event

Risk Terminology (cont'd)

- **Risks (cont'd)**
  - A generalized expression for risk is given as

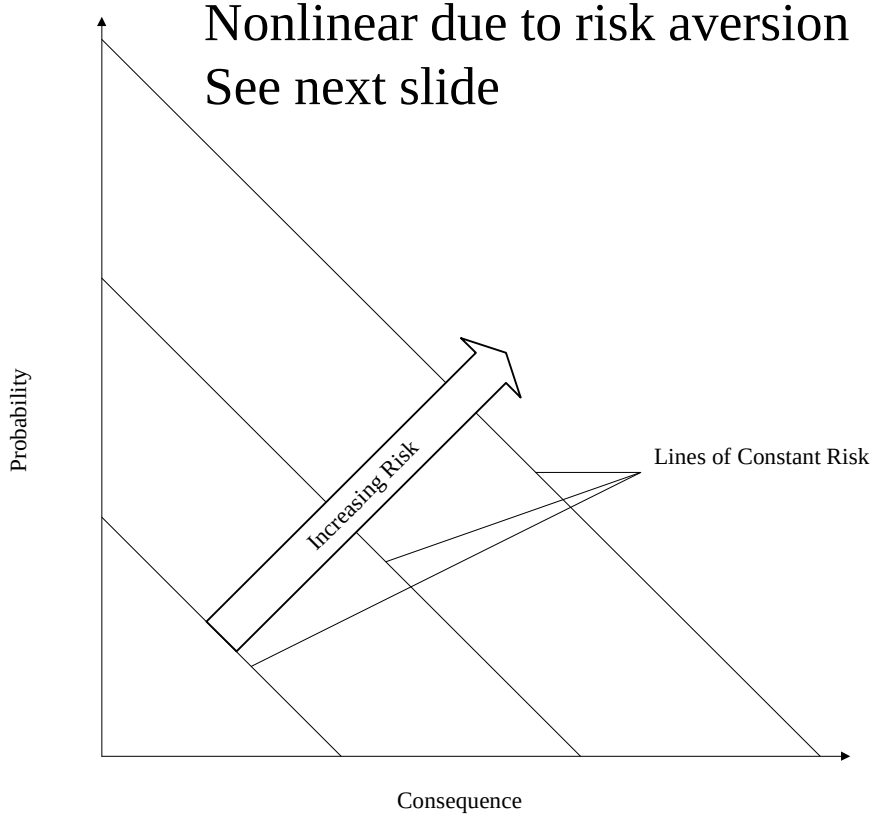
$$Risk \equiv \left[(cs_1, l_1, o_1, u_1, po_1), (cs_2, l_2, o_2, u_2, po_2), \ldots, (cs_n, l_n, o_n, u_n, po_n) \right] \quad (2)$$

cs = causal scenario
l = likelihood
o = outcome
u = utility (or significance)
po = population affected by the outcome
n = number of outcomes

Risk Terminology (cont'd)

- **Risks (cont'd)**
  - Risk is commonly evaluated as the Cartesian product of likelihood of occurrence and the impact severity of occurrence of the event:

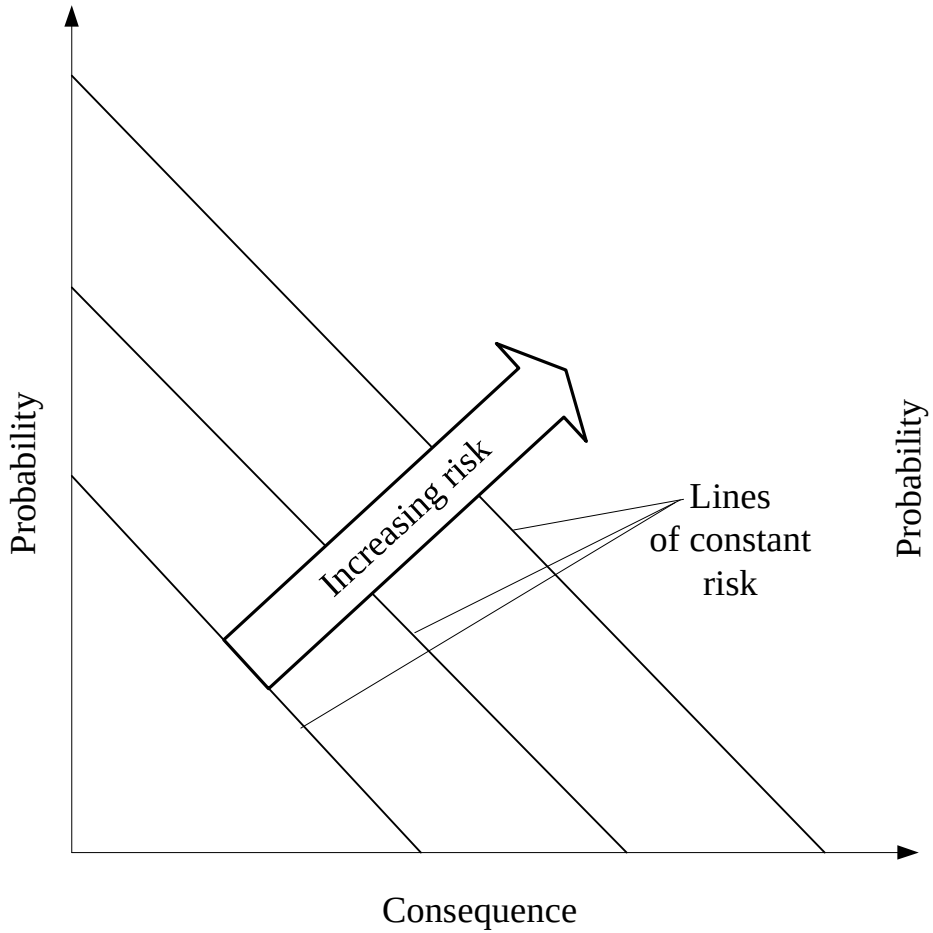
Nonlinear due to risk aversion
See next slide

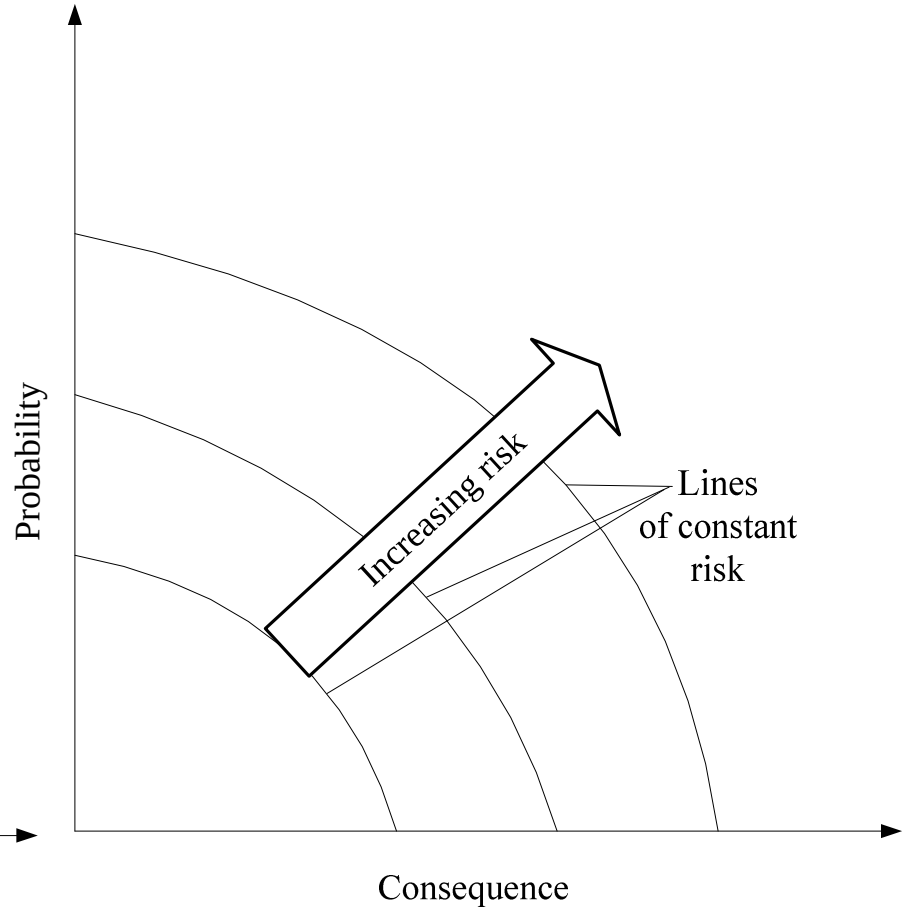


$$RISK\left(\frac{Consequence}{Time}\right) = LIKELIHOOD\left(\frac{Event}{Time}\right) \times IMPACT\left(\frac{Consequence}{Event}\right) \quad (3)$$

Risk Terminology (cont'd)

- **Risks (cont'd)**





Risk Terminology (cont'd)

- **Risks (cont'd)**
  - The occurrence probability (p) of an outcome (o) can be decomposed into an occurrence probability of an threat (t), success probability ($s|t$) called the vulnerability or fragility, and outcome ($o|t,s$) probability
  - The occurrence probability of an outcome can be expressed as follows:

$$p(o) = p(t)\,p(s \mid t)\,p(o \mid t,s) \quad (4)$$

Risk Terminology (cont'd)

- **Risks (cont'd)**
  - *Threat* – is the potential intent to cause harm or damage on, with, or through a system by exploiting its vulnerabilities
  - Threats can be associated with intentional human actions as provided in the table of next slide

Threat Types and Examples

Selected Threat Type	Example Delivery Mode	Example Weapon / Agent	Example Quantity/Quality
Chemical	Outdoor Dispersal	Ricin	Potent
		Mustard Gas	Potent
	Crop Duster	VX	Potent
		Chlorine Gas	Potent
	Missile	Any of the above	Potent
	Postal Mail	Ricin	Potent
Biological	Outdoor Dispersal	Anthrax	Potent
		SARS	Potent
	Postal Mail	Anthrax	Potent
	Food Buffets	Hepatitis	Potent
		Salmonella	Potent
	Missile	Any of the above	Potent
Radiological	Standard Deployment	Dirty Bomb	Strong
		Radiological Release	Strong
Nuclear	Standard Deployment	Improvised Nuclear Device	2 kT
		Strategic Nuclear Weapon	100 kT
Explosive	Standard Deployment	Backpack Bomb	10lb TNT
		Missile	50 ton
	Truck	Fertilizer Bomb	200 pounds
			500 pounds
			1000 pounds
			4000 pounds
	Boat	C4	200 pounds
	Airplane	Jet Fuel	5000 gallons
Sabotage	Physical	Cut Power Cable	Not Applicable
		Cut Bolts	Not Applicable
		Improper operation or maintenance	Not Applicable
	Cyber	Providing unauthorized access	Obvious
Cyber	Physical	Cut SCADA Cable	Not Applicable
		Magnetic weapons	Power units
	Cyber	Worm Virus	Obvious

Asset Taxonomy

Agriculture & Food	**Information & Telecommunications**	**Banking & Finance**
Supply	Public Switched Telecommunications Network (PSTN)	Physical facilities (buildings)
Processing	Internet	Operations centers
Production	Switch/ router areas	Regulatory institutions
Packaging	Access tandems	Physical repositories
Storage	Fiber/copper cable	Telecommunications networks
Distribution	Cellular, microwave, satellite systems	Emergency redundancy service areas
Transportation	Operations, Administration, Maintenance & Provisioning systems	**Chemical /Hazardous Materials Industry**
Water	Network operations centers	Manufacturing plants
Dams, wells, reservoirs, aqueducts	Underwater cables	Transport systems
Transmission pipelines	Cable landing points	Distribution systems
Pumping stations	Collocation sites, peering points, telecom hotels	Storage/ stockpile/ supply areas
Sewer systems	Satellite control stations Radio cell towers	Emergency response & communications systems
Treatment facilities	**Energy**	**Postal & Shipping**
Storage facilities	**Electricity (Non-nuclear)**	Processing facilities
Public Health	Hydro electric dams	Distribution networks
National strategic stockpile	Fossil-fuel electric power generation plants	Air, truck, rail and boat transport systems
National Institutes of Health	Distribution systems	Security
State & local health departments	Key substations	**National Monuments & Icons**

State & local health departments	Key substations	**National Monuments & Icons**
Hospitals	Communications	National parks
Health clinics	**Oil & Natural Gas**	Monuments
Mental health facilities	Off shore platforms	Historic buildings
Nursing homes	Refineries and Pipelines	**Nuclear Power Plants**
Blood supply facilities	Storage facilities	Commercial owned/operated
Laboratories	Gas processing plants	Government owned/operated
Mortuaries	Product terminals	Physical facilities
Pharmaceutical stockpiles	Strategic Petroleum Reserve	Spent fuel storage facilities
Emergency Services	**Transportation**	Safety/security systems
Fire houses and Rescue	Aviation	**Dams**
Federal Emergency Manage. Agency	Railways	Large
Emergency medical services	Highways	Small
Law enforcement	Trucking	Government owned
Mobile response	Busing	Private/corporate owned
Communications systems	Bridges	**Government Facilities**
Defense Industry Base	Tunnels	**National Security Special Events**
Supply systems	Borders	**Commercial Assets**
Critical R&D facilities	Seaports	Prominent commercial centers
	Pipelines	Office buildings
	Maritime	Sports centers/ arenas
	Mass transit	Theme parks
		Processing/service centers

Risk Terminology (cont'd)

- *System* – is a group of interacting, interrelated, or interdependent elements, such as, people, property, materials, environment, and processes (Chapter 3)
- *Event* – is occurrence or outcome or change of a particular set of circumstances
- *Scenario – is defined as joint events and system state that lead to an outcome of interest*

Risk Terminology (cont'd)

- *Initiating event* – is an event that appears at the beginning of a chain of events or a sequence of events, such as in an event tree
- *Event tree analysis* – is an inductive analysis method that utilizes an event tree graphical construct to show the logical sequence of the occurrence of events in, or states of, a system following an initiating event
  - *Probability tree analysis removes the limitation by allowing any number of branching of two or more*

Risk Terminology (cont'd)

- *Fault tree analysis* – is a deductive analysis method for representing the logical combinations of various system states and possible causes which can contribute to a specified event, called the top event
- *Failure mode* – is a way that failure can occur, described by the means or underlying physics, and can be modeled as an event
- *Vulnerability* – is defined as the intrinsic properties of a system making it susceptible to a hazard or a threat

Risk Terminology (cont'd)

- *Likelihood* – is the chance of something happening
- *Probability* – is a measure of chance of occurrence, likelihood, etc. between 0 and 1
- *Subjective probability* – is a probability that is based on the state of knowledge.
- *Conditional probability* – is the probability of event occurrence based on the assumption that another event (or multiple events) has occurred

Risk Terminology (cont'd)

- *Frequency* – is the count of an outcome of interest from a number of repeated observations of identical experiments or systems (if expressed as a fraction or percent, it is called relative frequency)
- *Rate – commonly is the count of an outcome of interest for a system occurring within a time period*
  - *It can be time dependent due to changes in the system's state, for example due to aging*
  - *Frequency is sometimes incorrectly used to mean the rate*

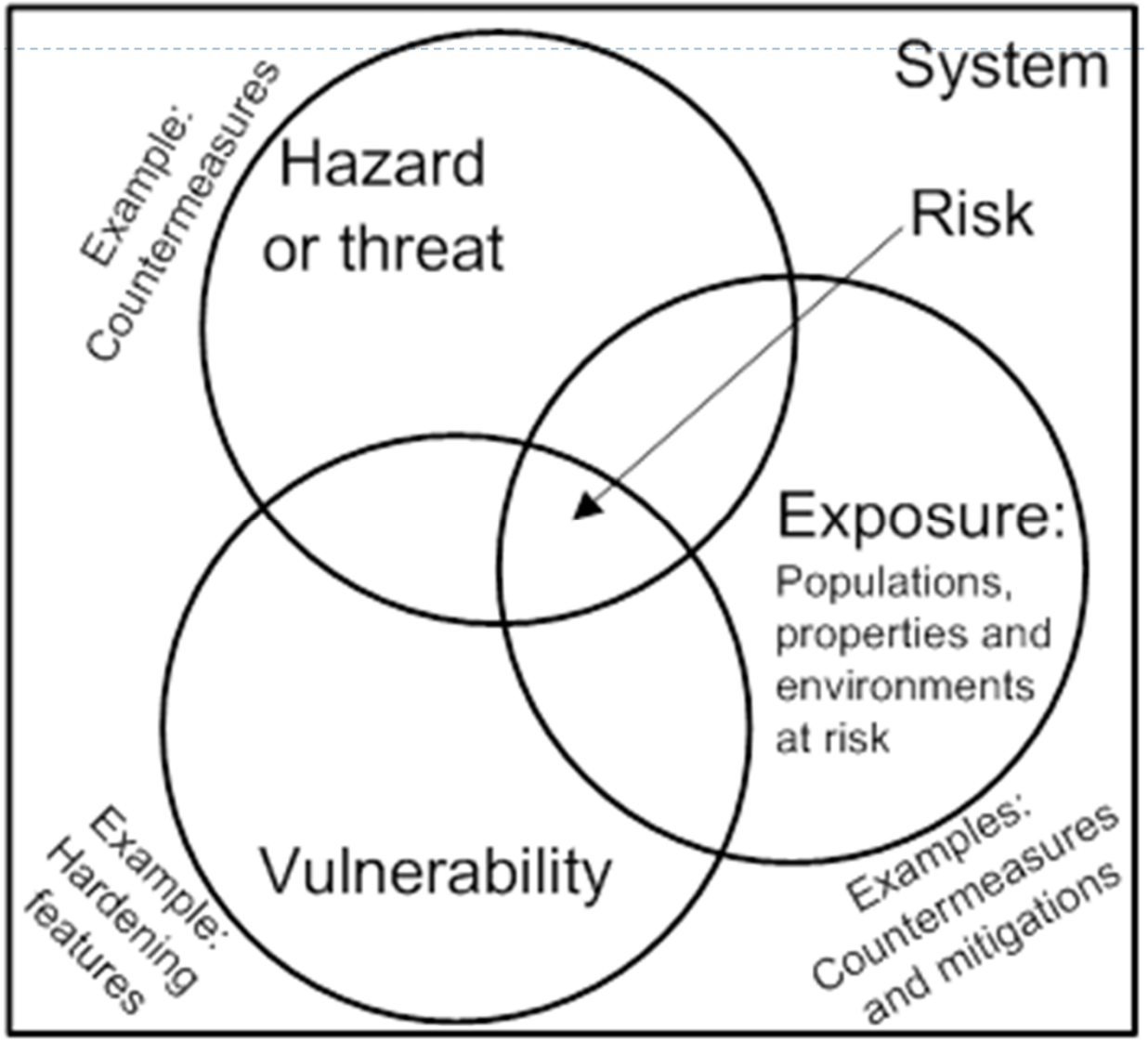
Risk Terminology (cont'd)

- *Exposure* – is the extent to which an organization and/or stakeholder is subject to an event, and defined by things at risk that might include population at risk, property at risk and ecological and environmental concerns at risk
- *Consequence* – is the immediate, short-, and long-term effects of an event affecting objectives, e.g., an explosion of a chlorine storage tank

Risk Terminology (cont'd)

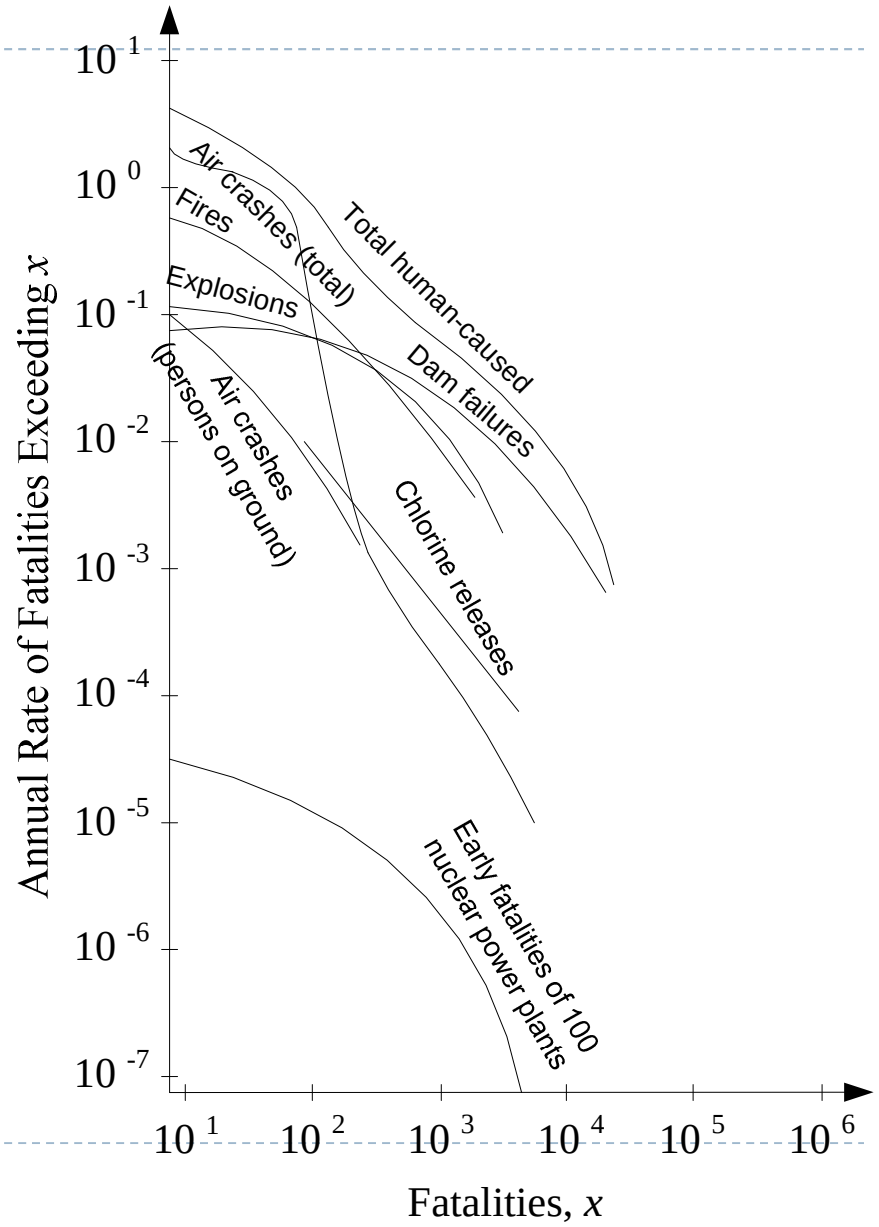
- *Consequence mitigation* – is the preplanned and coordinated actions or system features that are designed to reduce or minimize the damage caused by an event

Risk Terminology (cont'd)

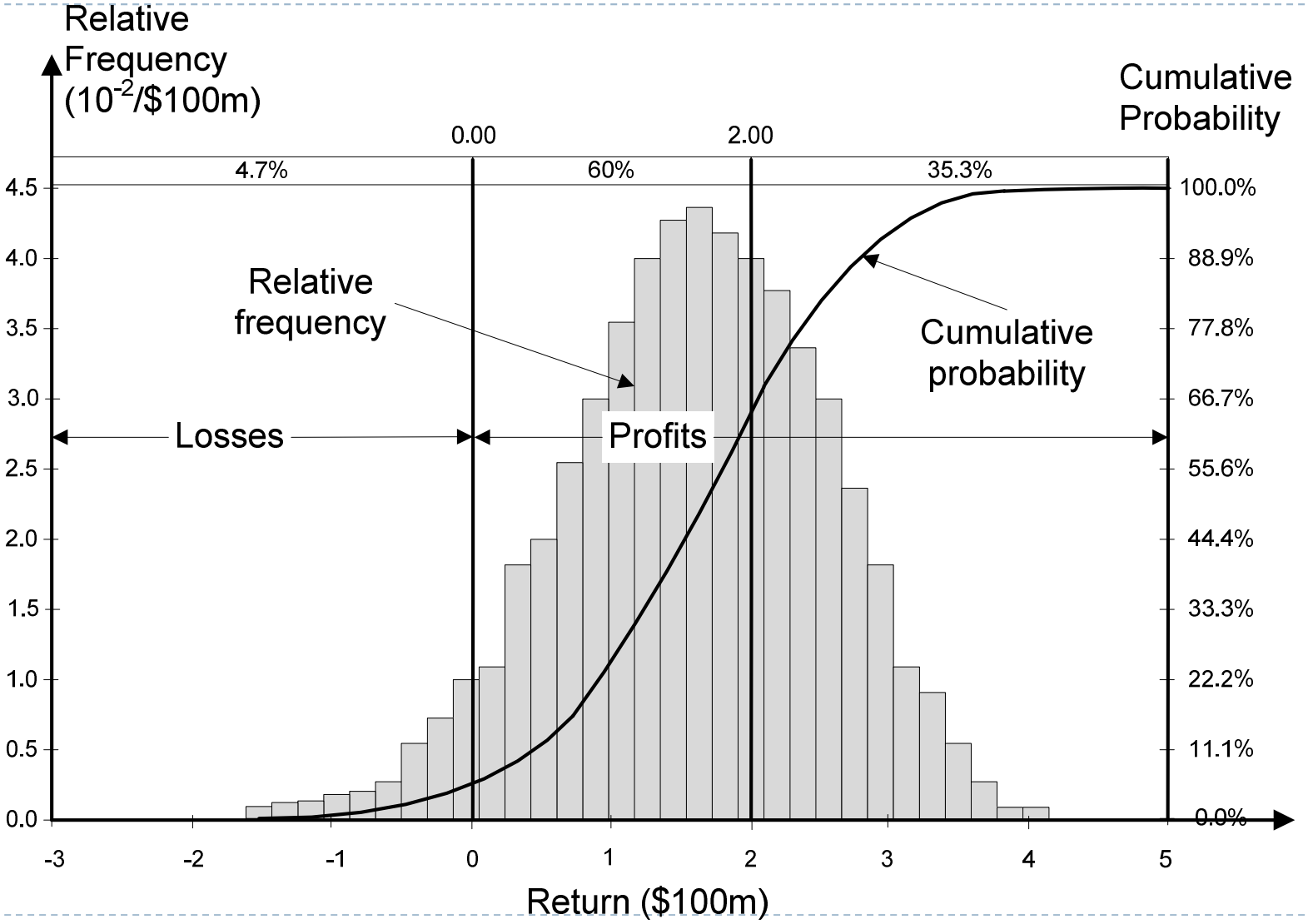


Risk Terminology (cont'd)

- **Risks (cont'd)**
  - A plot of occurrence probability and consequences is a *risk profile* or a *Farmer curve*

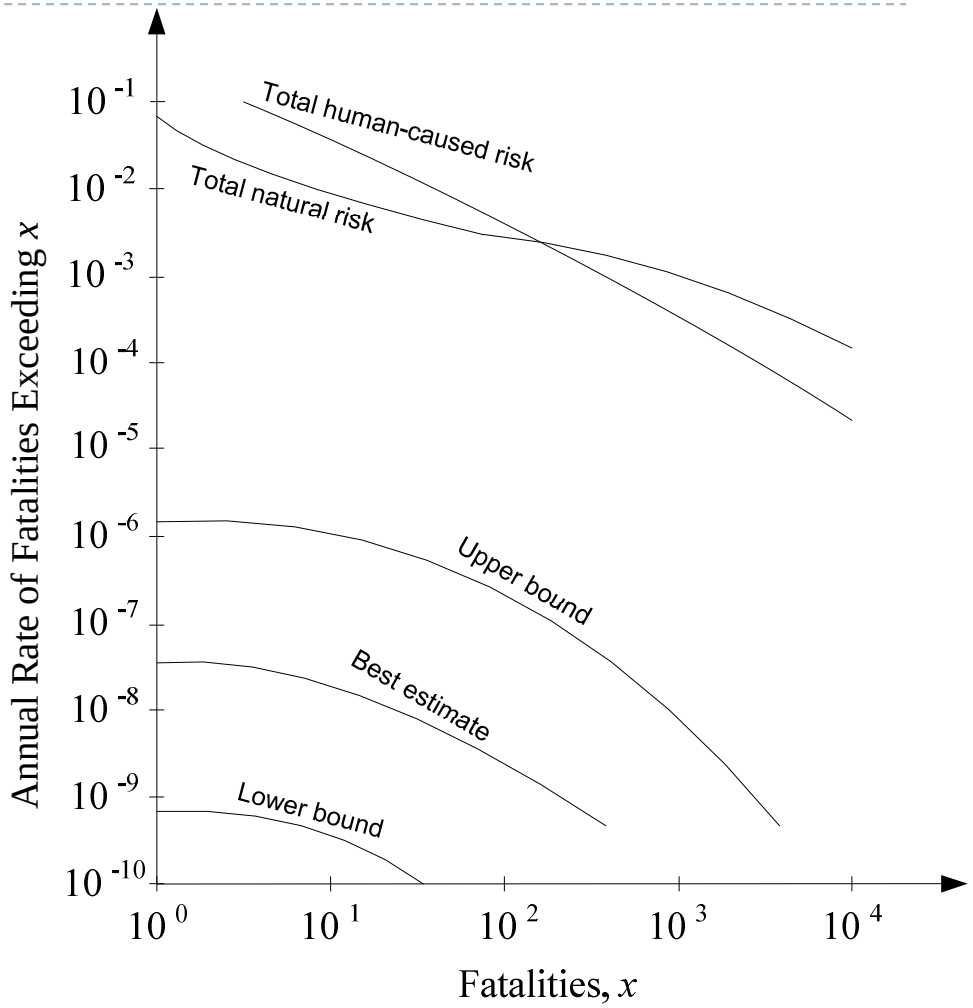


Example Project Risk Profile



Risk Terminology (cont'd)

- **Risks (cont'd)**
  - Examples of curves with bands (meta-uncertainty)
    - Aleatory uncertainty
    - Epistemic uncertainty



Risk Terminology (cont'd)

- **Performance**
  - The performance of a system or component can be defined as its ability to meet functional requirements
  - The performance of an item can be described by various elements including such items as speed, power, reliability, capability, efficiency, and maintainability
  - The design and operation of the product or system influence performance
  - Performance risk (e.g., constructing a power plants)

Risk Terminology (cont'd)

- *Risk register* – is a record of information about identified risks, sometimes called risk log
- *Risk profile* – is a description of any set of risks that may relate to the whole organization, part of the organization, or a group of stakeholders
- *Risk aggregation* – is combination of a number of risks into one risk measure to develop a more complete understanding of the overall risk

Risk Terminology (cont'd)

- *Risk management* – is the coordinated activities to direct and control an organization with regard to risk following a framework consisting of designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization
- *Stakeholder* – is a person, such as a decision maker, owner, etc., or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Risk Terminology (cont'd)

- *Risk owner* – is a person or entity with the accountability and authority to manage a risk
- *Risk criteria* – are the terms of reference against which the significance of a risk is evaluated reflecting organizational objectives expressed in external and internal contexts and in keep with standards, laws, policies and other requirements

Risk Terminology (cont'd)

- *Residual risk* – is the amount of risk remaining after realizing the net effect of risk reducing actions
- *Risk tolerance* – is the degree of risk associated with normal daily activities that people tolerate, usually without making a conscious decision
- *Risk acceptance* – is the degree of risk associated with a system or endeavor that a decision-maker perceives and accepts associated actions under a given set of circumstances and with associated costs

Risk Terminology (cont'd)

- *Risk aversion* – is the attitude to turn away from risk
- *Risk attitude* – is an organization's approach to assess and eventually pursue, retain, take or turn away from risk
- *Risk appetite* – is the amount and type of risk that an organization is willing to pursue or retain

Risk Terminology (cont'd)

- *Risk retention* – is the acceptance of the potential benefit of gain, or burden of loss, from a particular risk, includes the acceptance of residual risks, and depends on risk criteria
- *Risk perception* – is stakeholders' view on a risk reflecting their needs, issues, knowledge, belief and values
- *Risk treatment* – is the process to modify risk by several means (see the list on the next)

Risk Terminology (cont'd)

- *Risk treatment*
  - *Risk financing* – is a form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur, such as insurance, bonds, etc.
  - *Risk avoidance* – is an informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk
  - *Risk control* – is a measure in place that is risk modifying

Risk Terminology (cont'd)

- *Risk treatment* (cont.)
  - *Risk sharing* – is a form of risk treatment involving the agreed distribution of risk with other parties, such as insurance, contracts, etc. Sometimes, legal or regulatory requirements can limit, prohibit or mandate risk sharing
  - *Risk transfer* – is a form of risk sharing
  - *A countermeasure* – is an action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities or to reduce the frequency of attacks

Risk Terminology (cont'd)

- *Risk monitoring – is a process of continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected*
- *Risk communication – is the continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk to achieve an interactive process of exchange of information and opinions among stakeholders such as individuals, groups and institutions*

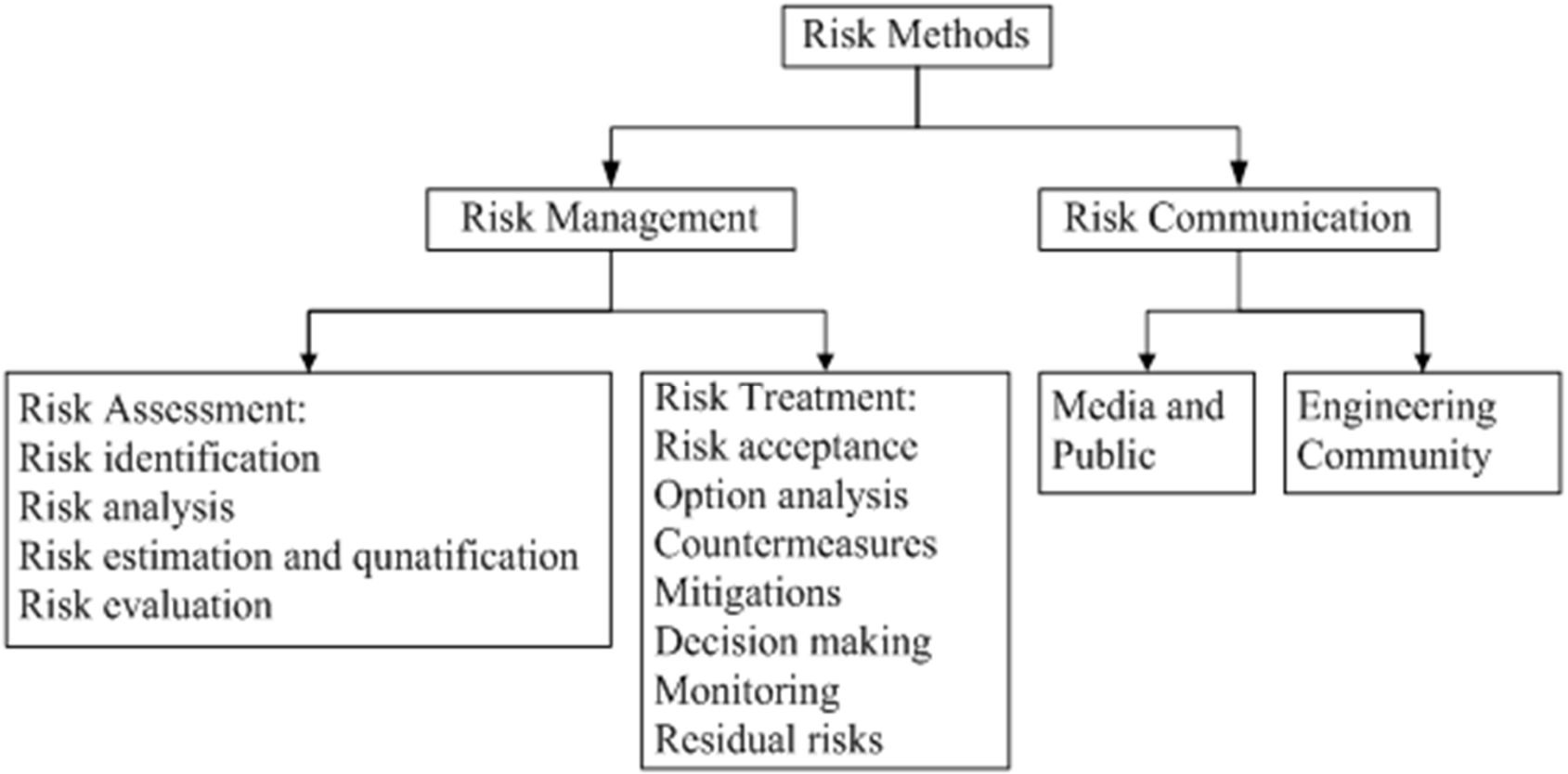
Risk Terminology (cont'd)

- **Risk-based Technology**
  - Risk-based technologies (RBT) are methods or tools and processes used to assess and manage the risks attributed to components or systems
  - RBT methods can be classified into
    - Risk management that includes risk assessment/risk treatment
    - Risk communication

(next slide)

Risk Terminology (cont'd)

- **Risk-based Technology (cont'd)**



Risk Terminology (cont'd)

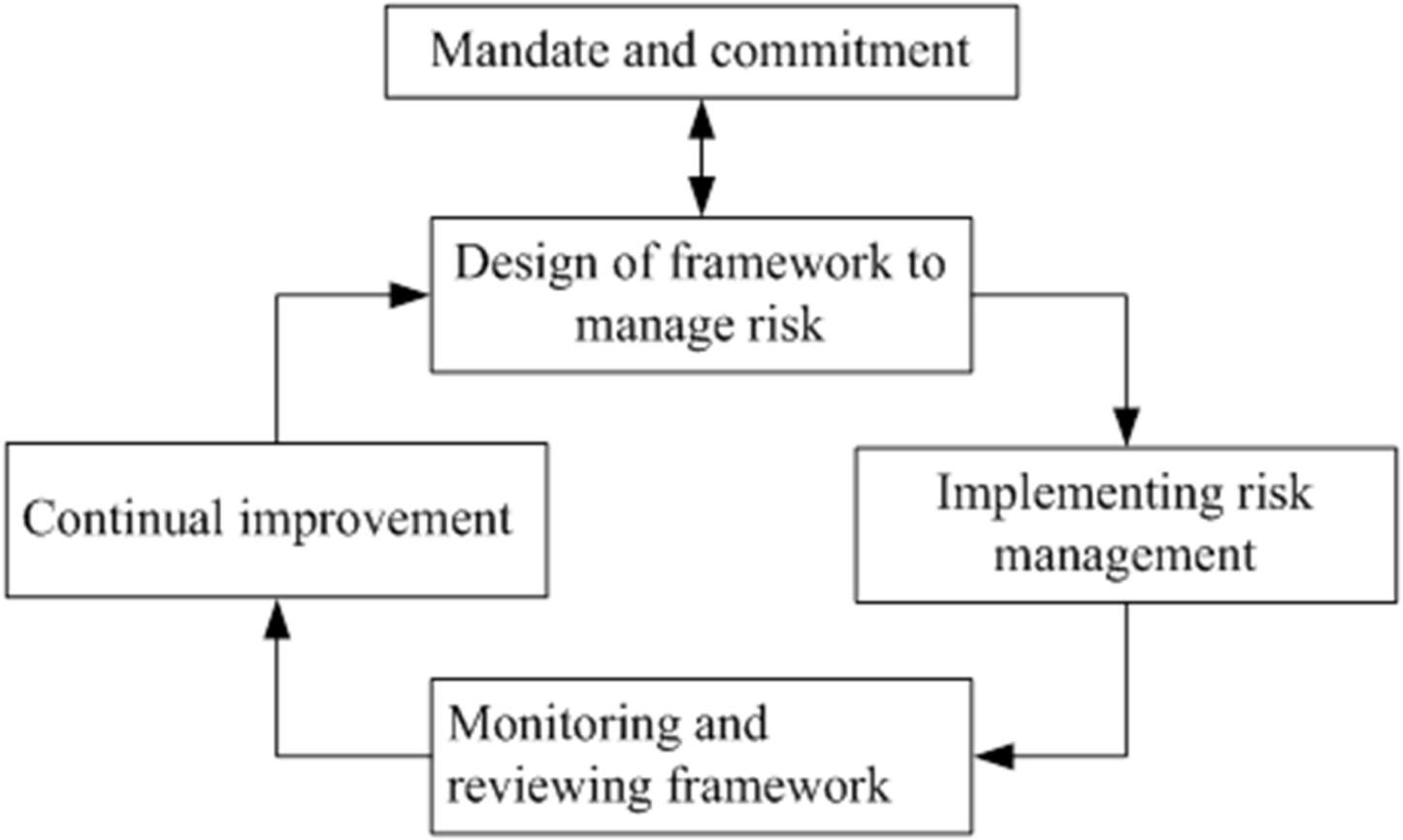
- **Risk-based Technology (cont'd)**
  - *Risk assessment* consists of
    - Hazard identification
    - Event probability assessment
    - Consequence assessment
  - *Risk treatment* require the definition of acceptable risk and comparative evaluation of options and/or alternatives through monitoring and decision analysis
  - Risk control also includes risk transfer, failure prevention and consequence mitigation

Risk Terminology (cont'd)

- **Risk-based Technology (cont'd)**
  - *Risk communication* involves perceptions of risk and depends on the audience targeted
  - It is classified into risk communication to the
    - Media
    - Public
    - Engineering community
    - Management
    - Decision makers

Risk Terminology (cont'd)

- **Risk Management**



Risk Terminology (cont'd)

- **Safety**
  - Safety can be defined as the judgment of risk acceptability for the system
  - Safety is a relative term
  - Different people are willing to accept different risks as demonstrated by such factors as
    - Location
    - Hazard or system types
    - Occupation
    - Lifestyle

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 1. Relative Risk of Different Activities

Risk of Death	Occupation	Lifestyle	Accidents/ Recreation	Environmental Risk
1 in 100	Stunt-person			
1 in 1,000	Racecar driver	Smoking (one pack/day)	Skydiving Rock climbing Snowmobile	
1 in 10,000	Fire fighter Miner Farmer Police officer	Heavy drinking	Canoeing Automobile All home accidents Frequent air travel	

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 1. Relative Risk of Different Activities

Risk of Death	Occupation	Lifestyle	Accidents/ Recreation	Environmental Risk
1 in 100,000	Truck driver Engineer Banker Insurance agent	Using contraceptive pills Light drinking	Skiing Home fire	Substance in drinking water Living downstream of a dam
1 in 1,000,000		Diagnostic X-rays Smallpox vaccination (per occasion)	Fishing Poisoning Occasional air travel (one flight per year)	Natural background radiation Living at the boundary of a nuclear power
1 in 10,000,000		Eating charcoal-broiled steak (once a week)		Hurricane Tornado Lightning Animal bite or insect sting

Risk Terminology (cont'd)

- **Safety (cont'd)**
  - Figure 1 (next slide) illustrates risk exposure during a typical day that starts by waking up in the morning and getting ready
    - Going to work
    - Commuting and working during the morning hours
    - Taking a lunch break
    - Having additional work hours
    - Commuting back home to have dinner
    - Using a motorcycle to a local pub

Risk Terminology (cont'd)

- **Safety (cont'd)**

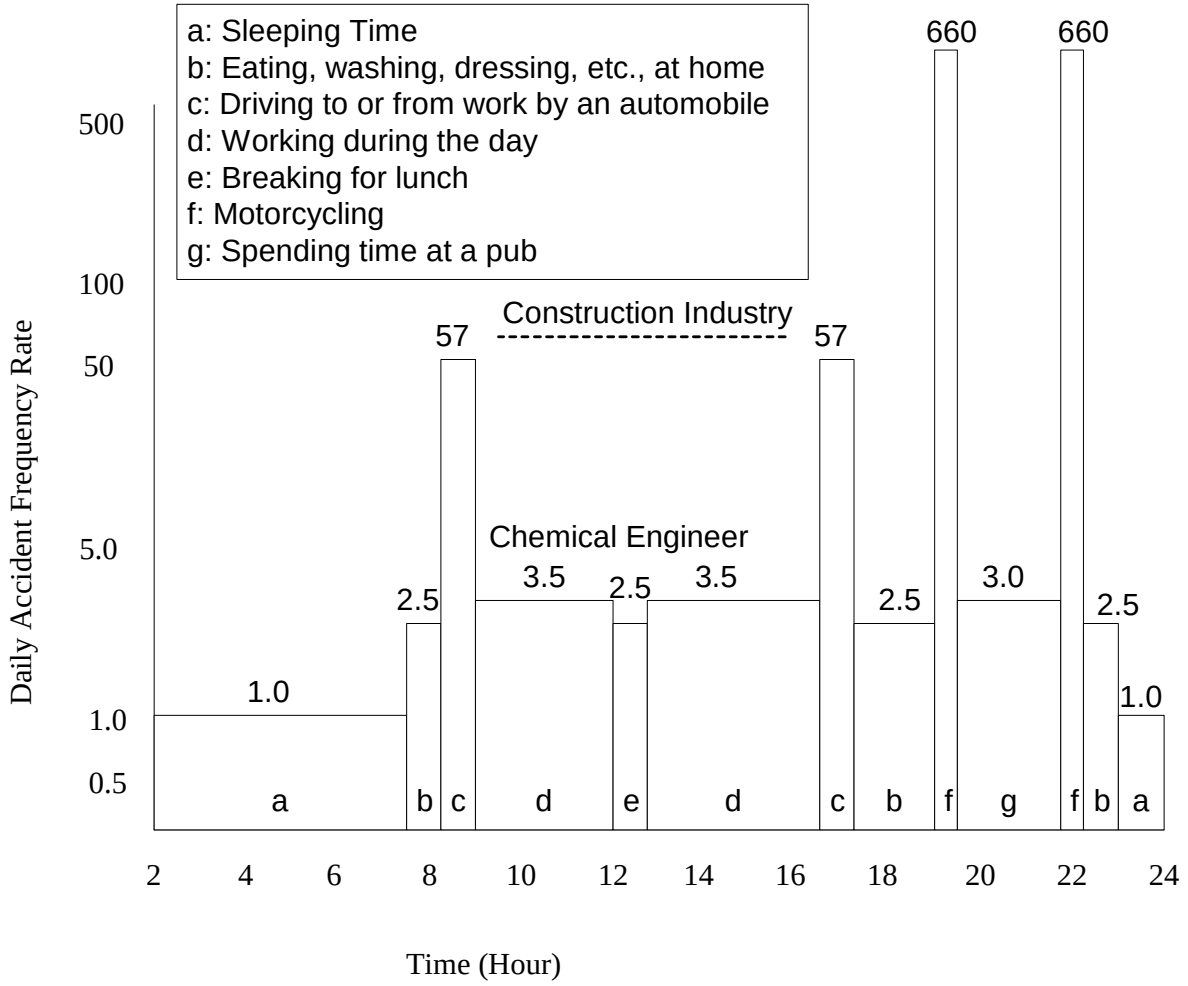


Figure 1. Daily Death Risk Exposure for a Working Healthy Adult

Risk Terminology (cont'd)

- **Safety (cont'd)**
  - The actual level of risk in some activities may not be reflected by risk perceptions of safety
  - Table 2 shows the differences in risk perception for 29 risk items by
    - League of Women Voters
    - College students
    - Experts

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 2. Risk Perception

Activity or Technology	League of Women Voters	College Students	Experts
Nuclear Power	1	1	20
Motor Vehicles	2	5	1
Hand Guns	3	2	4
Smoking	4	3	2
Motorcycles	5	6	6
Alcoholic Beverages	6	7	3
General Aviation	7	15	12

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 2. (cont.) Risk Perception

Activity or Technology	League of Women Voters	College Students	Experts
Police Work	8	8	17
Pesticides	9	4	8
Surgery	10	11	5
Fire Fighting	11	10	18
Large Construction	12	14	13
Hunting	13	18	23
Spray Cans	14	13	25

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 2. (cont.) Risk Perception

Activity or Technology	League of Women Voters	College Students	Experts
Mountain Climbing	15	22	28
Bicycles	16	24	15
Commercial Aviation	17	16	16
Electric (Non-nuclear) Power	18	19	9
Swimming	19	29	10
Contraceptives	20	9	11
Skiing	21	25	29

Risk Terminology (cont'd)

- **Safety (cont'd)**

Table 2. (cont.) Risk Perception

Activity or Technology	League of Women Voters	College Students	Experts
X-rays	22	17	7
High School or College Sports	23	26	26
Railroads	24	23	19
Food Preservatives	25	12	14
Food Coloring	26	20	21
Power Mowers	27	28	27
Prescription antibiotics	28	21	24
Home Applications	29	27	22

Risk Terminology (cont'd)

- **Systems for Risk Analysis**
  - A system can be defined as a deterministic entity comprising an interacting collection of discrete elements and commonly defined using deterministic models
  - "Deterministic" implies that the system is identifiable and not uncertain in its architecture
  - The definition of the system is based on analyzing its functional and/or performance requirements

Risk Terminology (cont'd)

- **Systems for Risk Analysis**
  - A description of a system may be a combination of functional and physical elements
  - Usually functional descriptions are used to identify high information levels on a system
  - A system may be divided into subsystems
  - Additional details lead to a description of
    - physical elements
    - components
    - various aspects of the system

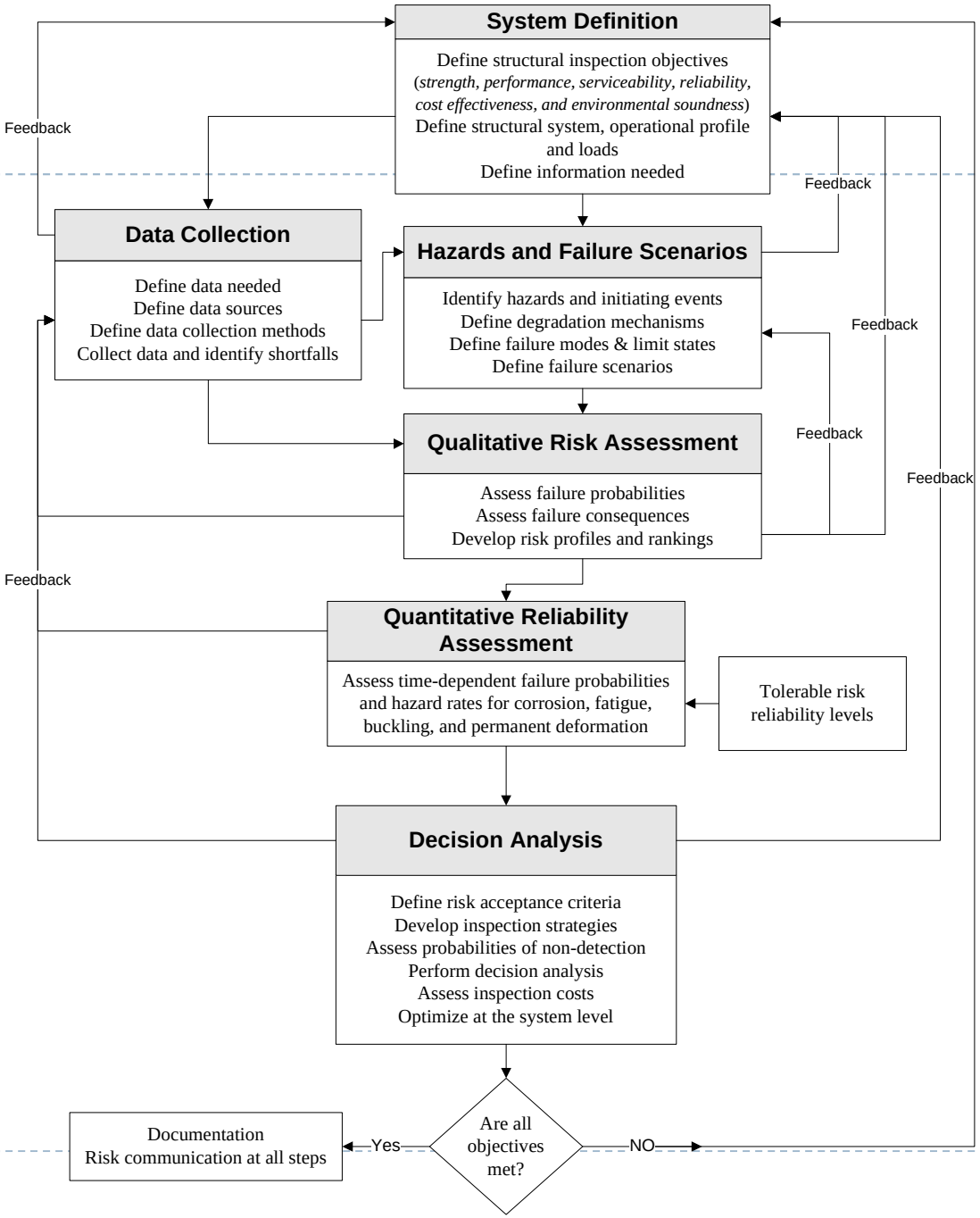
Risk Assessment

Definition: The scientific and engineering process of characterizing an adverse effect associated with an action or a situation

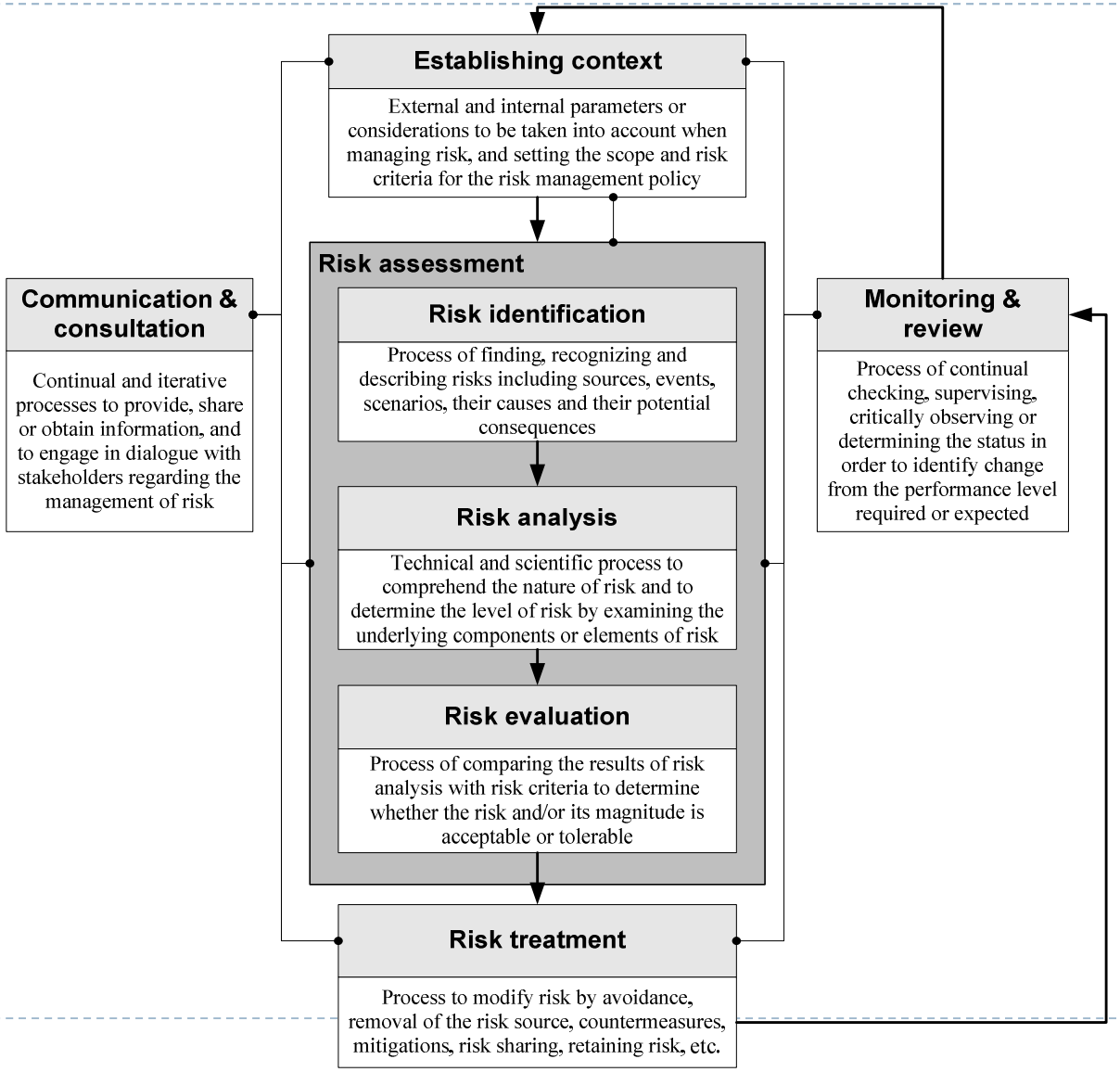
- The risk assessment process is essentially the same for every anticipated effect
- There is a great deal of confusion on the components of risk assessment
- There is a an obvious benefit for a common approach to risk assessment

Risk Assessment

- A Typical Risk Assessment Methodology
  - System definition
  - Hazard or threat identification
  - Definition of failure system scenarios
  - Qualitative risk assessment
    - Scenario likelihood
    - Scenario consequences
  - Quantitative risk assessment
    - Scenario likelihood
    - Scenario consequences
  - Decision analysis
    - Solution strategies
    - Benefits and costs
  - Uncertainty analysis
  - Data collection and risk communication at each step


System Definition
Define structural inspection objectives
(strength, performance, serviceability, reliability, cost effectiveness, and environmental soundness)
Define structural system, operational profile and loads
Define information needed
Data Collection
Define data needed
Define data sources
Define data collection methods
Collect data and identify shortfalls
Hazards and Failure Scenarios
Identify hazards and initiating events
Define degradation mechanisms
Define failure modes & limit states
Define failure scenarios
Qualitative Risk Assessment
Assess failure probabilities
Assess failure consequences
Develop risk profiles and rankings
Quantitative Reliability Assessment
Assess time-dependent failure probabilities and hazard rates for corrosion, fatigue, buckling, and permanent deformation
Tolerable risk reliability levels
Decision Analysis
Define risk acceptance criteria
Develop inspection strategies
Assess probabilities of non-detection
Perform decision analysis
Assess inspection costs
Optimize at the system level
Are all objectives met?
Yes
NO
Documentation
Risk communication at all steps
Feedback
Feedback
Feedback
Feedback
Feedback
Feedback

Risk Assessment (ISO 31000: 2009)



Unique Features of Risk Analysis for Asset Protection from Deliberate Human Threats

Features	**Unique Characteristics**
Risk analysis framework	Should be performed accounting for the perspectives of adversaries as well as the perspectives of defenders; and as a multi-level analysis ranging from an asset, to multi-assets, to a sector, and to multi-sectors, to sufficiently account for interdependencies that may affect the risks pertinent to the decision being made.
Asset (target) features	Include attractive assets; critical assets; soft assets; assets with vulnerabilities that are sufficiently known to adversaries.
Assets (targets) selected by adversaries	Include high-consequence assets (or scenarios) with high probability of success
Threat features	Include the dynamic nature of threats, threat types and probabilities; their non-randomness but deliberateness using design-basis threats; possibly being of unknown or unknowable types.
Threat-asset dependencies	Include dynamically responding to asset protection using countermeasures and consequence mitigation.
Ingenuity of adversaries	Includes converting assets to threats by capitalizing on the efficiency of infrastructures, e.g.: • Transportation efficiency by converting airplane assets into explosive weapons. • Mail efficiency by using mail items for bio-agent delivery. • Other efficient infrastructure systems include power and information systems.
Capabilities of adversaries	Include the ability to select targets and accurately deliver the weapon to them and the ability to adapt to countermeasures to redirect the weapon to another target.
Asset vulnerabilities	Include identifying targets outside the system boundaries to exploit system vulnerabilities through system dependencies.
Consequences	Are broadly defined to include public health, economic loss, loss of vital commodities, interruption of government operation, and national psyche.
Asset and sector interdependencies	Include interdependencies in functionality and subsequently in consequences.
Decision analysis	Includes tradeoffs based on national security, safety, and economics.
Information flow	Is a two-way flow of defenders acquiring knowledge about the adversaries; adversaries acquiring knowledge about the assets, countermeasures, and consequence mitigation plans.
Countermeasures	Include countermeasures at the asset level, and meta-countermeasures at the multi-asset, sector and multi-sector levels. Countermeasures reduce the probability of selection of an asset as well as the probability of success of an attack.
Consequence mitigation plans	Include mitigation at the local level, and meta-mitigations at the state level, regional level and national level. Mitigation actions reduce consequences.
Risk perception and communication	Could include fear factors, hype, psychological aspects, communication effectiveness, and misconceptions.

Risk Assessment (cont'd)

- Risk Events and Scenarios
  - Risk events and scenarios can be categorized as follows:
    - Technical, technological, quality, or performance risks
    - Project-management risks
    - Organizational risks
    - External risks
    - Natural hazards, such as earthquakes, floods, strong winds, etc.

Risk Assessment (cont'd)

Table 3. Risk Events and Scenarios

Risk Event Category or Scenario	Description
Unmanaged Assumptions	Unmanaged assumptions are neither visible nor apparent as recognizable risks. They are commonly introduced by organizational culture and that when unknowingly present in the project environment bring about incorrect perceptions and unrealistic optimism.
Technological Risk	A technological risk can arise from using unfamiliar or new technologies. At one end is the application of the state of art and familiar technology, where the technological risk can be quite low. At the other end, a new technology is used generating the greatest uncertainty and risk.
Economic Climate	For example, uncertain inflation rates, changing currency rates, etc., affect the implementation of a project in terms of cash flow. A forecast of the relative valuations of currencies can be relevant for industries with multinational competitors and project partners.

Risk Assessment (cont'd)

Table 3. (cont'd) Risk Events and Scenarios

Risk Event Category or Scenario	Description
Domestic Climate	Risk events in this category include tendencies among political parties, local governments, attitudes and policies toward trade and investment, and any recurring governmental crises.
Social Risks	Risks in this category are related to social values such as preservation of environment. Some projects had to be aborted after an investment decision had been made due to resistance from the local population.
Political Risks	Political risks are associated with political stability both at home and abroad. A large investment may require looking ahead several years from the time the investment is made.
Conflicts Among Individuals	Conflicts can affect the success of a project. These conflicts could arise from cognitive differences or biases including self-motivated bias.

Risk Assessment (cont'd)

Table 3. (cont'd) Risk Events and Scenarios

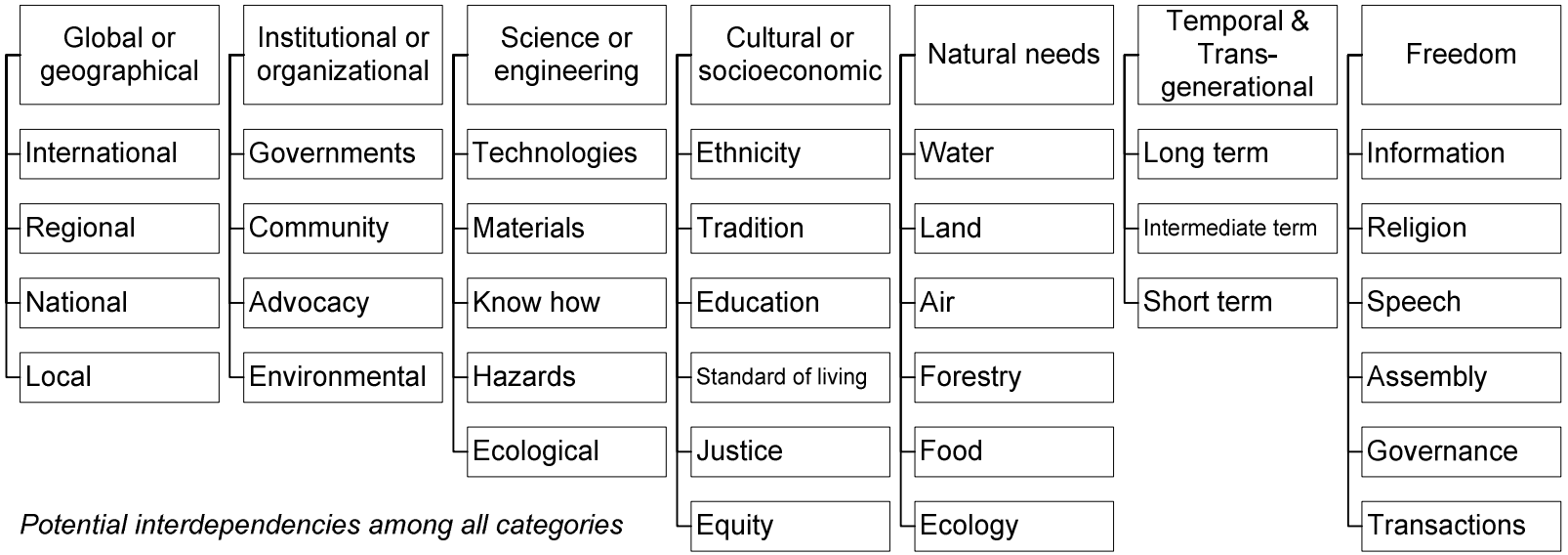
Risk Event Category or Scenario	Description
Large and Complex Project Risks	Large and complex projects usually call for multiple contracts, contractors, suppliers, outside agencies, and complex coordination systems and procedures. Complex coordination between the subprojects is itself a potential risk, as a delay in one area can cause a ripple effect in other areas.
Conceptual Difficulty	A project may fail if the basic premise from which it was conceived was faulty. For example, if an investment is planned to remove some of the operational or maintenance bottlenecks ignoring market requirements and forces, the risk of such a project not yielding desired financial benefits is extremely high.
Use of External Agencies	Appointing an external agency as project manager without creating a large project organization may not ensure the kind of ownership required for successful implementation or the liquidation of defects that the client can visualize through an earlier experience of operating the facilities.

Risk Assessment (cont'd)

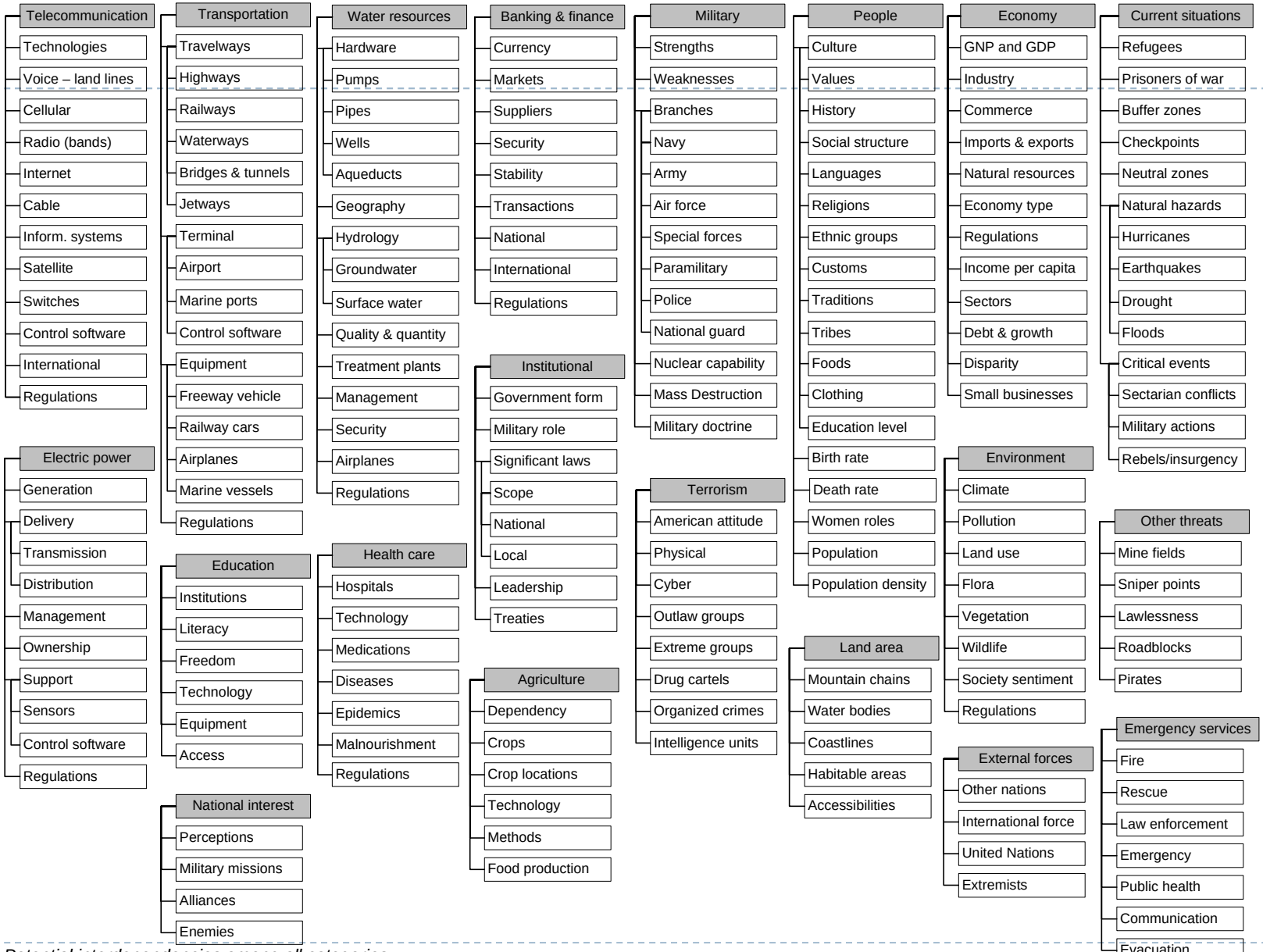
Table 3. (cont'd) Risk Events and Scenarios

Risk Event Category or Scenario	Description
Contract and Legal Risks	A contract as an instrument to transfer the risk from the owner to the contractor, the contractor risks only his fees, whereas the owner runs the risks of not having the plant at all. Although there are many modes available – like multiple split contracting, turnkey, engineering-procurement-construction-commissioning – , none of these come without risks.
Contractors	Contractor failure risk may originate from the lowest-cost syndrome, lack of ownership, financial soundness, inadequate experience, etc. In the face of immense competition, the contractor squeezes his profit margin to the maximum just to stay in the business. Contractors sometimes siphon mobilization advance to other projects in which they have greater business interest. If a contractor has difficulty with cash flow, then the project suffers.

Abbreviated Categories for Risk Event and Factor Identification



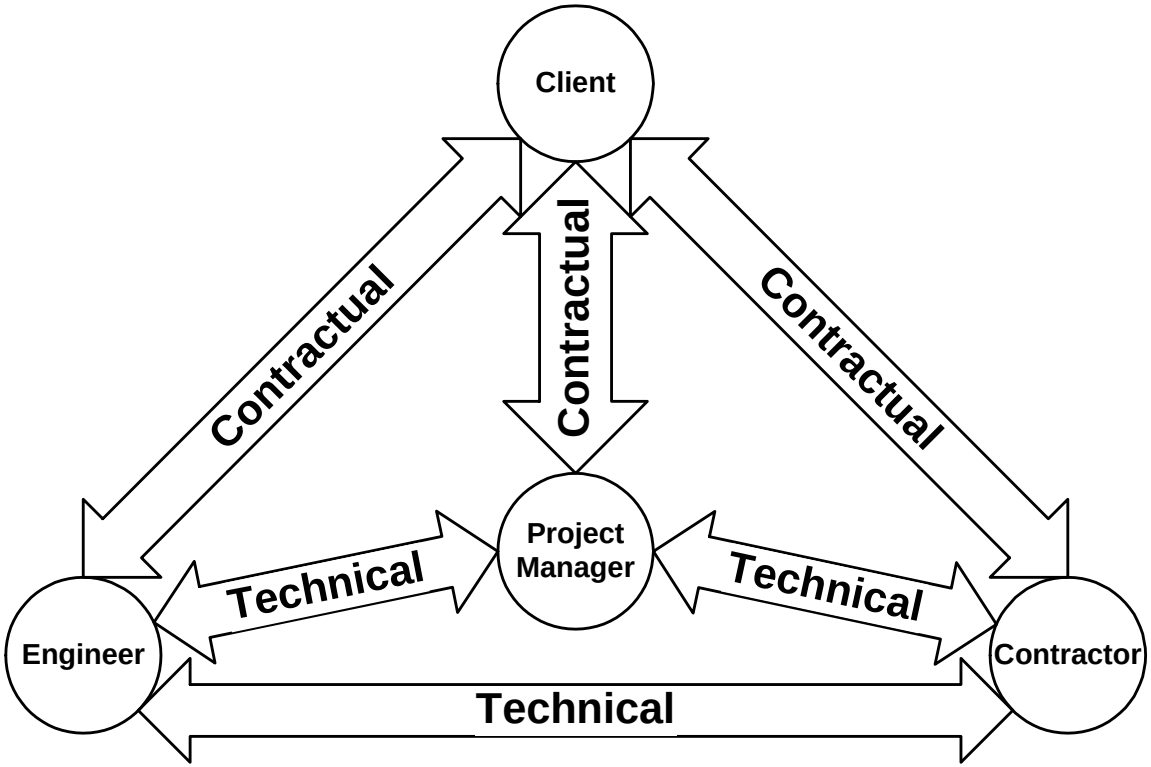
Potential interdependencies among all categories



Potential interdependencies among all categories

Risk Assessment (cont'd)

- Example: Project Risks for Warehouse Automation



Relationships Among the Four Parties Involved in a Project

Risk Assessment (cont'd)

- Example: Project Risks for Warehouse Automation (cont'd)
  - ABC grocery and supermarket outlets desires to automate its warehouse by installing a computer-controlled order-packing system, along with a conveyor system for moving goods from storage to the warehouse shipping area

Risk Assessment (cont'd)

- Example: Project Risks for Warehouse Automation (cont'd)
  - Four parties are involved in this project:
    - (1) client
    - (2) project manager
    - (3) engineer
    - (4) contractor
  - The risk events and scenarios associated with this project can be constructed based on the perspectives of the four parties as provided in Tables 2-4a, 2-4b, 2-4c, and 2-4d, respectively of your *textbook*

Risk Assessment (cont'd)

- Example: Project Risks for Warehouse Automation (cont'd)
  - Risk perspectives:
    - (1) Client (Table 2-4a) – contractor with weak cash flow
    - (2) Project manager (Table 2-4b) – contractor with weak planning procedures
    - (3) Engineer (Table 2-4c) – signing off on poor quality product
    - (4) Contractor (Table 2-4d) inadequate cash flow

Risk Assessment (cont'd)

- Identification of Risk Events and Scenarios
  - The risk assessment process starts with the question:

    "What can go wrong?"

  - The identification of *what can go wrong* entails defining:
    - *Hazards or threats*
    - *Risk events*
    - *Risk scenarios*

Risk Assessment (cont'd)

- Identification of Risk Events and Scenarios
  - Risk identification can be a difficult task because it is often subjective, and no unerring procedures available that may be used to identify risk events and scenarios other than relaying heavily on the experience and insight of key project personnel
  - Scenarios for risk evaluation can be created
    - Deductively (e.g., fault tree analysis (FTA))
    - Inductively (e.g., failure mode and effect analysis (FMEA) or event tree analysis (ETA))

Risk Assessment (cont'd)

- Identification of Risk Events and Scenarios
  - Precursor Event Analysis
  - A *precursor event* (PE) is an event that precedes an incident (such as, an accident relating to nuclear power plants, or a terrorist attack relating to homeland security) and substantially reduces safety margins

Risk Assessment (cont'd)

- **Precursor Event Analysis**

1. Screening using the *event trees*, i.e., identification of events with anticipated high conditional probabilities of severe incident p_i given precursor event i
2. Quantification, i.e., estimation of p_i and the observed rate of occurrence of severe incidents *as*

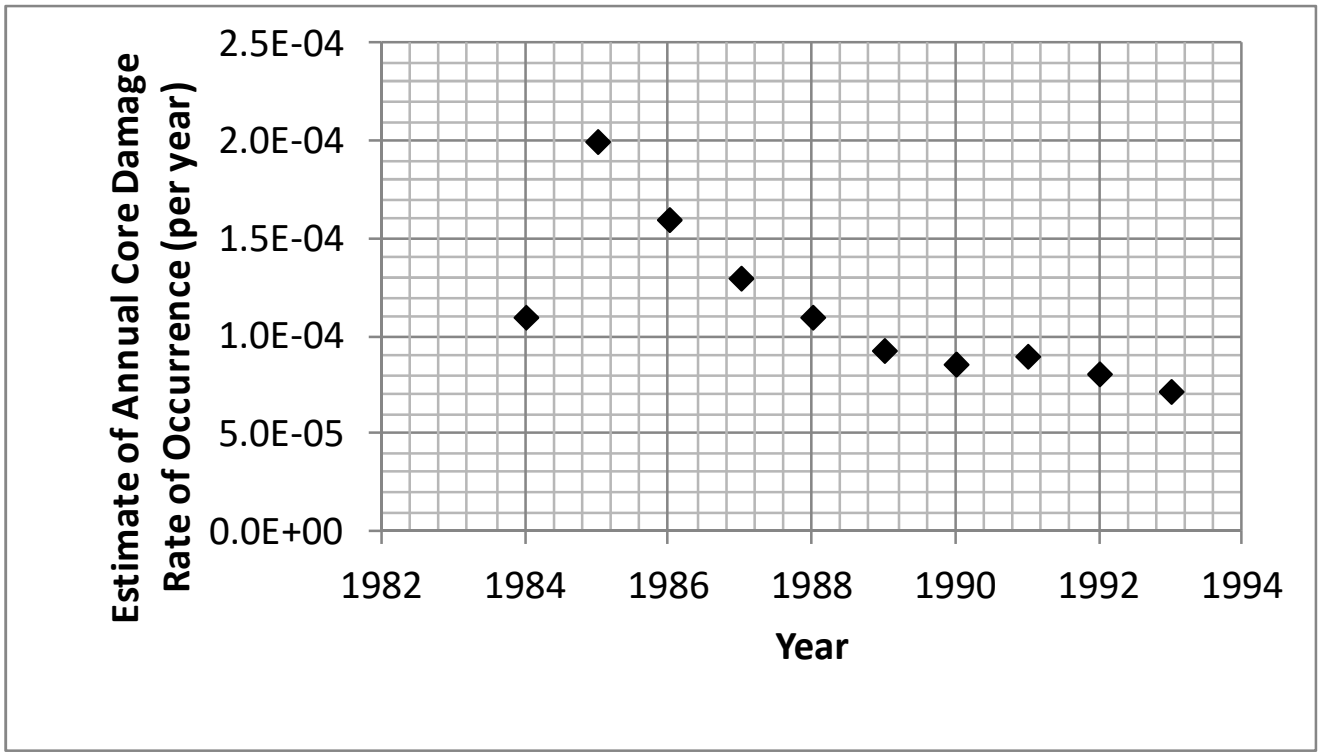
$$\hat{\lambda} = \left(\sum_i p_i \right) / t$$

3. Trend analysis to assess the overall system performance and prediction

Risk Assessment (cont'd)

- Precursor Event Analysis

$$\hat{\lambda} = \left(\sum_i p_i \right) / t$$



Risk Assessment (cont'd)

Table 4. Risk Assessment Methods

Method	Scope
Safety/Review Audit	Identifies equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts.
Checklist	Ensures that organizations are complying with standard practices.
What-If	Identifies hazards, hazardous situations, or specific accident events that could result in undesirable consequences.
Hazard and Operability Study (HAZOP)	Identifies system deviations and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations.
Preliminary Hazard Analysis (PrHA)	Identifies and prioritizes hazards leading to undesirable consequences early in the life of a system. It determines recommended actions to reduce the frequency and/or consequences of the prioritized hazards. This is an inductive modeling approach.

Risk Assessment (cont'd)

Table 4. (cont'd) Risk Assessment Methods

Method	Scope
Probabilistic Risk Analysis (PRA)	Methodology for quantitative risk assessment developed by the nuclear engineering community for risk assessment. This comprehensive process may use a combination of risk assessment methods.
Failure Modes and Effects Analysis (FMEA)	Identifies the components (equipment) failure modes and the impacts on the surrounding components and the system. This is an inductive modeling approach.
Fault Tree Analysis (FTA)	Identifies combinations of equipment failures and human errors that can result in an accident. This is an deductive modeling approach.
Event Tree Analysis (ETA)	Identifies various sequences of events, both failures and successes that can lead to an accident. This is an inductive modeling approach.

Risk Assessment (cont'd)

Table 4. (cont'd) Risk Assessment Methods

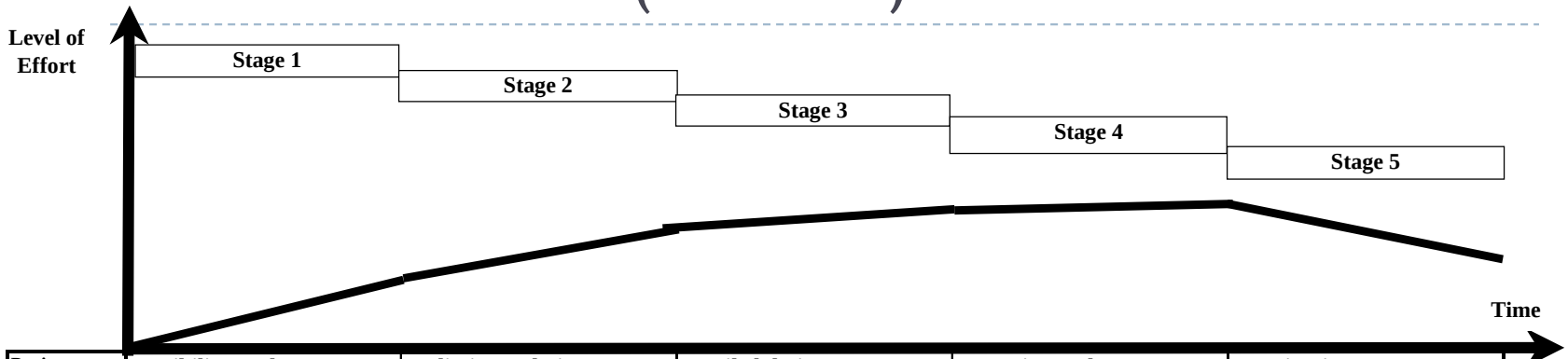
Method	Scope
The Delphi Technique	Assists to reach consensus of experts on an issue such as project risk while maintaining anonymity by soliciting ideas about the important project risks that are collected and circulated to the experts for further comment. Consensus on the main project risks may be reached in a few rounds of this process.
Interviewing	Identifies risk events by interviews of experienced project managers or subject-matter experts. The interviewees identify risk events based on experience and project information.
Experience-Based Identification	Identifies risk events based on experience including implicit assumptions.
Brain Storming	Identifies risk events using facilitated sessions with stakeholders, project team members, and support staff.

Method	Scope
Risk register (or Risk log)	Manages risk by acting as a central repository for all risks identified by the project staff, and, for each risk, tracks information such as risk factor, event, probability, impact, countermeasures, risk owner and so on.
Swiss cheese model	Organizes causes and used to analyze and represent the causes of systematic failures or accidents, and describes a scenario (or scenarios) leading to an accident as a series of events which must occur in a specific order and manner for an accident to occur.
Pareto analysis	Identifies and prioritizes the most significant items among many. This technique employs the 80-20 rule, which states that about 80 percent of the problems or effects are produced by about 20 percent of the causes.
Relative ranking/risk indexing	Assesses the attributes of a system or operation to calculate index numbers for making relative comparisons of various alternatives.
Change analysis	Looks systematically for possible risk impacts and appropriate risk management strategies in situations where change is occurring.
Event and causal factor charting	Describe graphically or textually the time sequence of contributing events associated with an accident.

Risk Assessment (cont'd)

- Example: Risk Assessment Methods for Warehouse Automation Project
  - This example identifies suitable risk assessment methods for various aspects of the warehouse automation project
  - Risk assessment methods include checklist, what-if-then analysis, FMEA, FTA, and ETA, and qualitative and quantitative risk assessments
  - The client risks identified in Example 2-1 (Text) are used herein to illustrate the use of checklists and what-if-then analysis

Risk Assessment (cont'd)



Project stages	Feasibility study	Preliminary design	Detailed design	Execution and implementation	Termination
what if	Feasibility stage is delayed for some reason.	The preliminary design is not approved for various reasons caused by the architect, engineer, project planner, or project manager.	The detailed design performed by the architect/engineer is delayed.	The execution and implementation stage is delayed or disrupted for one reason or more as provided in Example 2-1.	The termination stage is delayed or not scheduled.
then	The four stages of the project will be delayed causing problems to the client's financial and investment obligations.	The detailed design will not be ready for zoning and planning approval, and for the selection process of contractors causing accumulated delays in finishing the project leading to additional financial burdens on the client.	The project management activities cannot be performed efficiently, and the contractor (if selected at this stage) cannot start work properly causing delays in the execution of the project.	Definitely, the project will not be finished on time and will be completed over budget causing serious financial problems to the client.	The whole automation system will become unreliable and hazardous causing customer complaints and the increasing client's contractual obligation problems.

Example: What-if-then Analysis and Results for Various Project Stages

Risk Assessment (cont'd)

- Risk Breakdown Structure
  - Level 0
    Project Risks
  - Level 1
    Management, External, Technology
  - Level 2
    See next viewgraph

Risk Breakdown Structure

Level 0	Level 1	Level 2	Level 3
Project Risks	Management	Corporate	History, experiences, culture, personnel
			Organization structure, stability, communication
			Finances conditions
			Other projects
			M
		Customers & stakeholders	History, experiences, culture, personnel
			Contracts and agreements
			Requirement definition
			Finances and credit
			M
	External	Natural environment	Physical environment
			Facilities, site, equipment, materials
			Local services
			M
		Cultural	Political
			Legal, regulatory
			Interest groups
			Society and communities
			M
		Economic	Labor market, conditions, competition
			Financial markets
			M
	Technology	Requirements	Scope and objectives
			Conditions of use, users
			Complexity
			M
		Performance	Technology maturity
			Technology limitations
			New technologies
			New hazards or threats
			M
		Application	Organizational experience
			Personnel skill sets & experience
			Physical resources
			M

Risk Assessment (cont'd)

- Enterprise Risk Breakdown Structure
  - Strategic risk assessment
  - Operational risk assessment
  - Compliance risk assessment
  - Internal audit risk assessment
  - Financial statement risk assessment
  - Fraud risk assessment
  - Market risk assessment
  - Credit risk assessment
  - Customer risk assessment
  - Supply chain risk assessment
  - Product risk assessment
  - Security risk assessment
  - Information technology risk assessment
  - Project risk assessment
  - First-of-a-kind technology risk assessment
  - Portfolio risk assessment
  - Sector risk assessment
  - Logistics risk assessment

Enterprise Risk Breakdown Structure

Level 0 Enterprise	Level 1 Prospects	Level 2 Bidding	Level 3 Execution
1. Strategic:	Site	Site (as an example):	Site|Availability (as an example):
Reputational damage	Technology & Technical	Availability	Delay to ownership
Competition	Labor	Suitability	Delay to permits
Customer wants	Materials and Equipment	Transportation & Logistics	Adequacy of permits
Demographic	Equipment for construction	Utilities	Regulatory agency requirements
Social/cultural trends	Procurement sources	Communications	Restrictions and easements
Technological innovation	Subcontractors	Conceptual difficulty	Residual war risks (mines, unexploded ordinance)
Capital availability	Commercial	First of a kind	Seashore use rights
Regulatory and political trends	Hazards	Unmanaged assumptions	Air use rights
2. Financial:	External	Local codes and standards	
Price		Scope definition	
Liquidity		Technical interfaces	
Credit		Fabrication & construction	
Inflation/purchasing power		Mining processes	
Hedging/basis risk		Environmental restoration	
3. Operational:		Services	
Business operations		Hazardous aspects	
Empowerment			
Information			
Information/business reporting			
4. Hazards:			
Fire			
property damage			
Natural perils			
Theft and other crime			
Personal injury			
Business interruption			
Disease and disability			
Liability claims			
5. Assets:			
Physical and intellectual			
Financial			
Customer related			
Hires			
Organizational			
6. Environments:			
Markets			
Sovereign or political			
Legal or regulatory			
Attitudes or sentiments			
Acceptance or sensitivity			
Technological innovation			
Competition			
Catastrophic events			

Risk Assessment (cont'd)

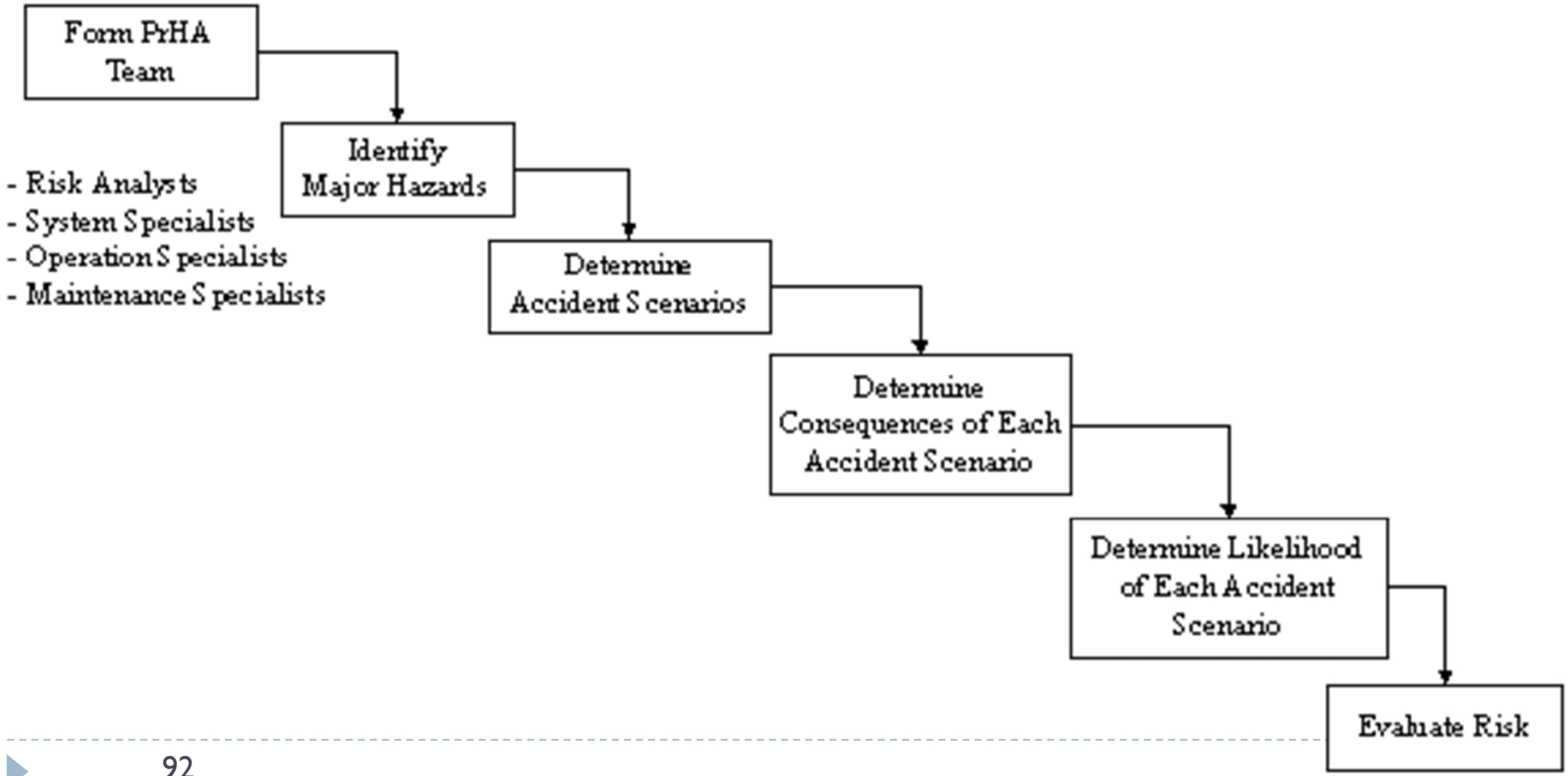
- System Definition for Risk Assessment
  - The system must be constructed in a well organized and repeatable fashion
  - The formation of system boundaries is based upon the objectives of the risk analysis. Delineating system boundaries can assist in developing the system definition.
  - Establishing the system boundary is partially based on what aspects of the system's performance are of concern

Risk Assessment (cont'd)

- System Definition for Risk Assessment (cont'd)
  - Along with identifying the boundaries, it is important to establish a resolution limit for the system
  - The system breakdown structure is the top-down division of a system into subsystems and components

Risk Assessment (cont'd)

- Selected Risk Assessment Methods
  - Preliminary Hazard Analysis



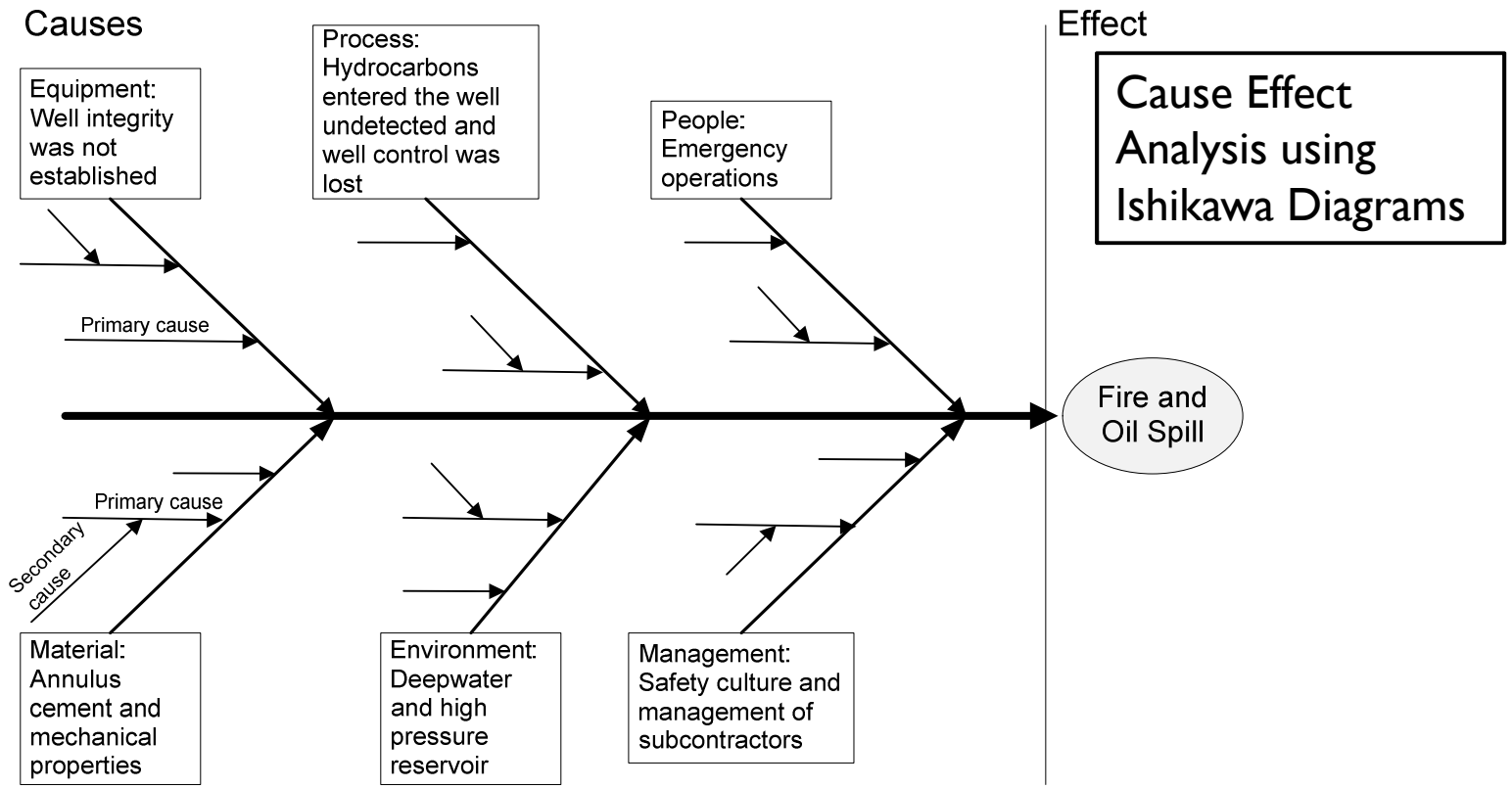
Risk Register

Risk Register

Risk Category	Risk Factor or Event	Identification Number	Probability (1 to 3)	Impact (1 to 3)	Risk Score	Mitigation or Countermeasure	Contingency	Risk Owner	Action Timing
Natural hazard	Strong wind	1.1.	2 (medium)	2 (medium)	4	Avail hardware to secure equipment, supplies & structure	Secure equipment, supplies & structure	Jim	within 2 hours
Natural hazard	High temperature	1.2.	1 (low)	2 (high)	2	Access and ice to water suppliers	Offer frequent breaks, provide water, etc.	John	within 2 hours
Materials	Delay in arrival	2.1.	2 (medium)	2 (medium)	4	Identify points of contacts of suppliers	Check with suppliers	Janet	within 2 hours
Labor	Strike	3.1	1 (low)	3 (high)	3	Monitor labor concerns and address early	Alternate labor providers	Everyone	According to plan
Labor	Low productivity	3.2	1 (low)	2 (medium)	2	Track and provide incentives	Increase or replace labor force	Susan Michael	Within a day
Startup check	Low power output	4.1	1 (low)	3 (high)	3	Perform component checks	Engage technical support	Mathew	within 6 hours

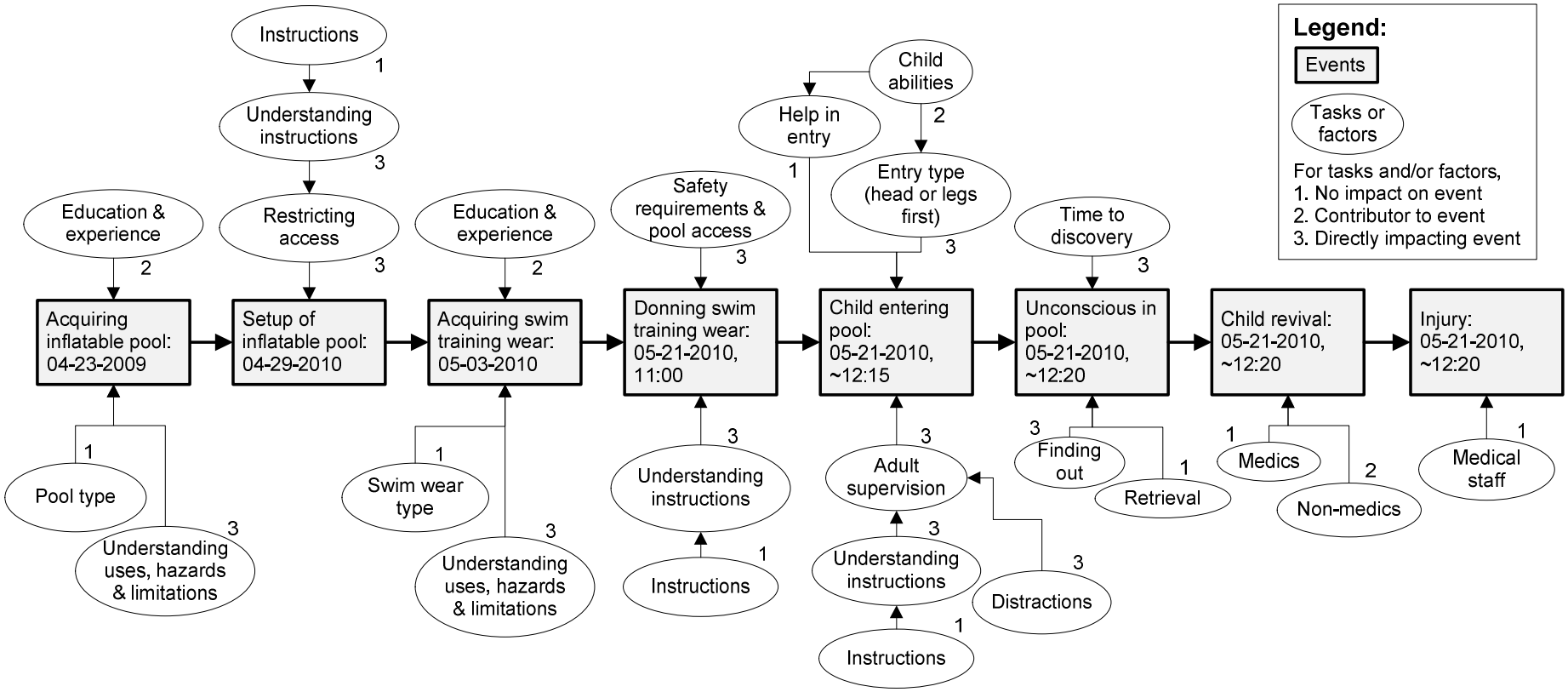
Risk Assessment (cont'd)

- Selected Risk Assessment Methods
  - Root Cause Analysis (oil spill)

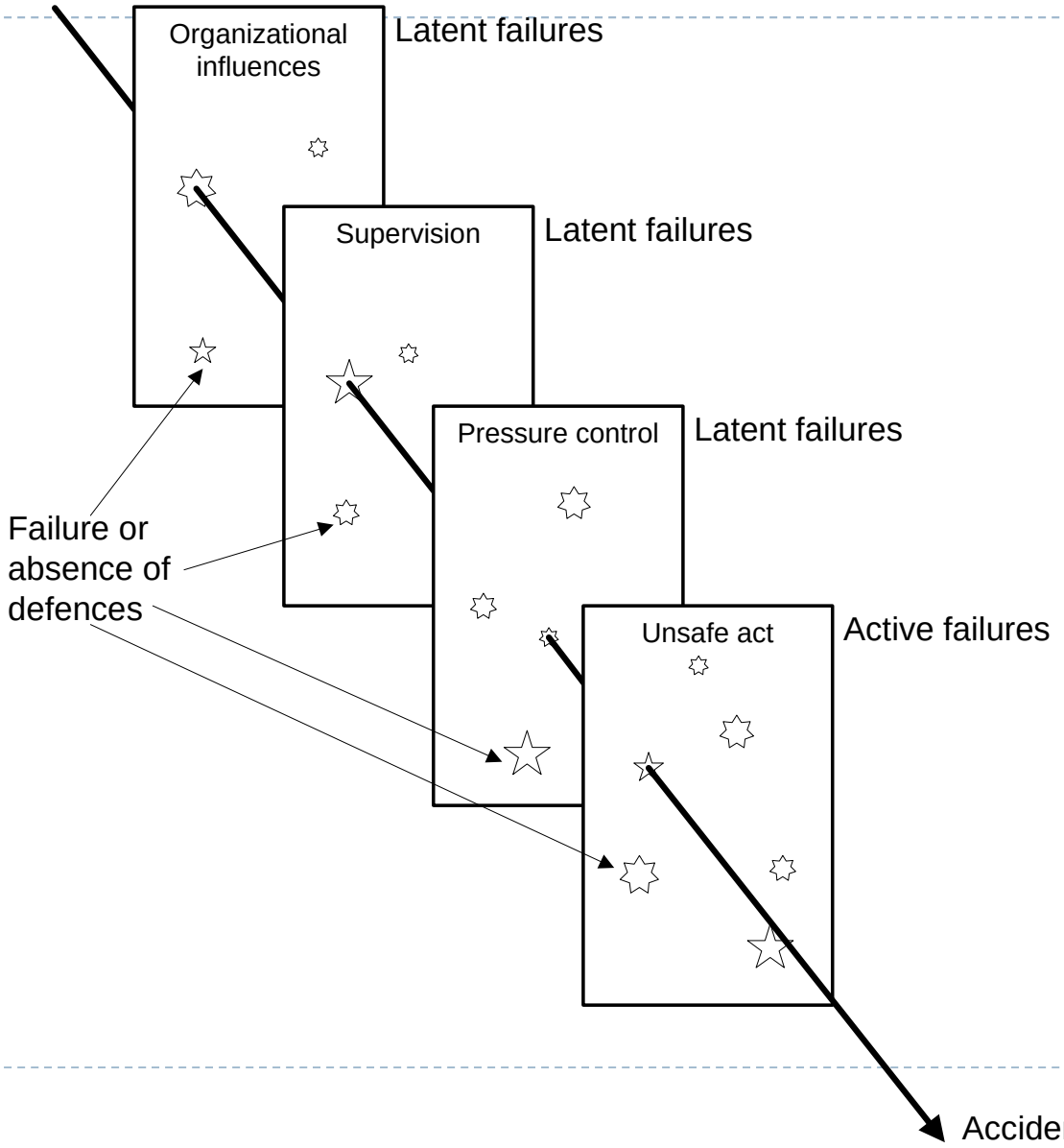


Risk Assessment (cont'd)

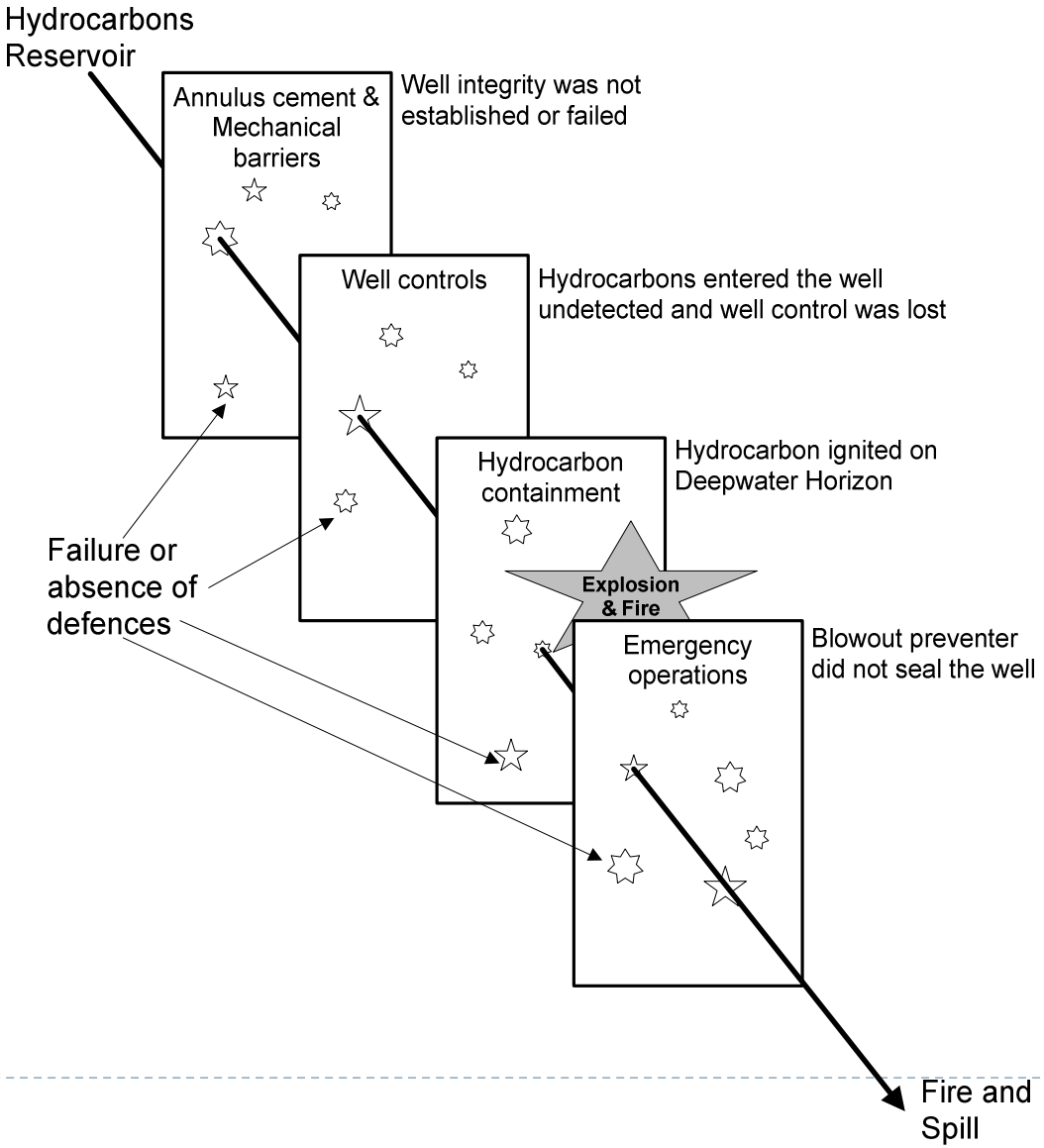
- Selected Risk Assessment Methods
  - Events and Causal Factors Diagram of Child Drowning



Swiss Cheese Model

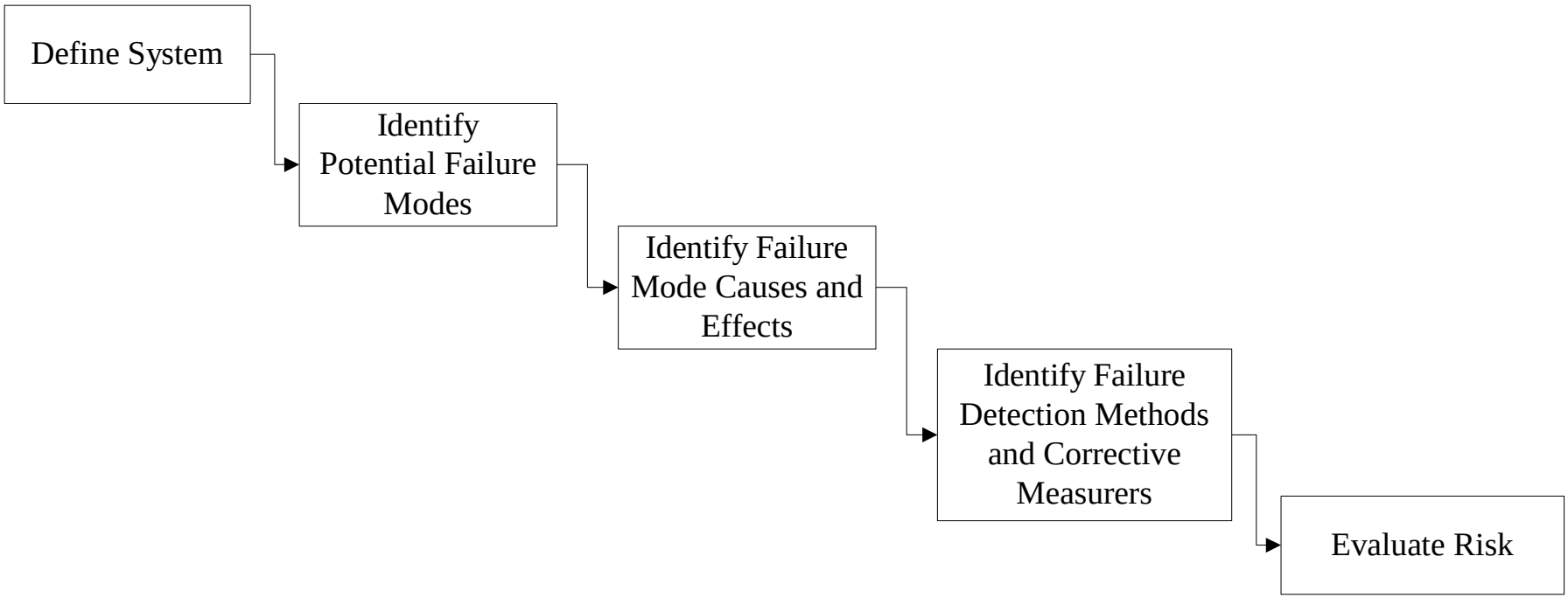


Example: Oil Spill



Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis



Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Failure Modes:** A failure mode is a way in which a specific process or product fails. It is a description of features that can be negatively affected by a process step or component
    - **Failure Effects:** Failure effects are the impact on end user or regulatory requirements. They are what the end user might experience or notice as a result of the failure mode. The effect is the outcome of the occurrence of the failure mode on the system

Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Severity Ratings:** The severity rating is the importance of the effect on end user requirements. It is concerned with safety and other risks if failure occurs. Severity rating is driven by failure effects and criticality and applies only to the effect. Severity rating should be the same each time the same failure effect occurs. A relative rating scale of 1 to 10 is commonly used (where 1 = not severe and 10 = extremely severe) as given in Table 5.

Risk Assessment (cont'd)

Table 5. Severity Rating Evaluation Criteria

Rating	Description
Minor:	
1	Not noticeable. No effect to the product and end user.
Low:	
2	Not noticeable. No effect.
3	Slightly noticeable, slight end user annoyance.
Moderate:	
4 – 6	End user will notice immediately upon receipt. Noticeable effects on sub-system, or product performance. Some end user dissatisfaction. End user is uncomfortable or annoyed by failure.
High:	
7 – 8	Effects on major system, but not on safety or government regulated compliance items. High degree of end user dissatisfaction due to nature of failure.
Extreme:	
9 – 10	Affects safety or involves noncompliance with government regulations. (9 with warning; 10 without warning)

Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Failure Causes:** Causes of failure are sources of process variation that causes the failure mode to occur. Potential causes describe how the failure could occur in terms of something that can be corrected or controlled. Potential causes should be thought of as potential root causes of a problem and point the way toward preventive / corrective action. Identification of causes should start with failure modes associated with the highest severity ratings.

Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Occurrence Rating:** The occurrence rating of a cause is the frequency with which a given cause occurs and creates the failure mode. Occurrence rating refers to the industry wide average likelihood or probability that the failure cause will occur. A rating scale of 1 to 10 is used as given in Table 6.
    - **Definition of Controls:** Current controls are those controls that either prevent the failure mode from occurring or detect the failure mode should it occur. Prevention controls consist of mistake-proofing and automated control. Controls also include inspections and tests which detect failures that may occur at a given process step or subsequently.

Risk Assessment (cont'd)

Table 6. Occurrence Rating Criteria

Rating	Failure Consequence Description	Failure Rate
Minor:		
1	Failure is unlikely. No failures ever associated with almost identical processes.	< 1 in 1,000,000
Low:		
2	Only isolated failures associated with almost identical processes.	1 in 20,000
3	Isolated failures associated with similar processes.	1 in 4,000
Moderate:		
4 5 6	Generally associated with similar processes that have experienced occasional failures, but not in major proportions.	1 in 1,000 1 in 400 1 in 80
High:		
7 8	Generally associated with similar processes that have often failed. Process is not in control.	1 in 40 1 in 20
Extreme:		
9 10	Failure is almost inevitable.	1 in 8 1 in 2

Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Detection Ratings:** The detection rating is a measure of the capability of current controls. A detection rating indicates the ability of the current control scheme to detect the causes before creating failure mode and/or the failure modes before causing effect. Detection rating provides the probability that current controls will prevent a defect from reaching the end user given that a failure has occurred as given in Table 7.

Risk Assessment (cont'd)

Table 7. Detection Rating Criteria for Likelihood Defect is caught by Current Controls

Rating	Description
Certainty of non-detection:	
10	Controls will not or cannot detect the existence of a defect.
Very low:	
9	Controls probably will not detect the existence of a defect.
Low:	
7 – 8	Controls have a poor chance of detecting the existence of a defect.
Moderate:	
5 – 6	Controls may detect the existence of a defect.
High:	
3 – 4	Controls have a good chance of detecting the existence of a defect. The process automatically detects failure.
Very high:	
1 – 2	Controls will almost certainly detect the existence of a defect. The process automatically prevents further processing.

Risk Assessment (cont'd)

- Selected Risk Assessment Methods (cont'd)
  - Failure Mode and Effects Analysis (cont'd)
    - **Risk Priority Number (RPN):** The Risk Priority Number (RPN) can be introduced as a weighted assessment number used for prioritizing the highest risk items. The RPN focuses efforts on factors that provide opportunities to make the greatest improvement. The RPNs are sorted and actions are recommended for the top issues. Risk assessment should be performed to determine when a corrective action is required:

$$\begin{aligned} RPN &= \text{Risk Priority Number} \\ &= (\text{Occurrence rating})\,(\text{Severity rating})\,(\text{Detection rating}) \end{aligned} \tag{4}$$

Refer to example 2.4 textbook (Personal Flotation Devices)

Risk Assessment (cont'd)

- Risk Matrices
  - Risk can presented and assessed using matrices for preliminary screening by subjectively estimating probabilities and consequences in a qualitative manner
  - A risk matrix is a two-dimensional presentation of likelihood and consequences using qualitative metrics for both dimensions

Risk Assessment (cont'd)

- Risk Matrices (cont'd)

  Table 8. Likelihood Categories for a Risk Matrix

Category	Description	Annual Probability Range
A	Likely	$\geq$ 0.1 (1 in 10)
B	Unlikely	$\geq$ 0.01 (1 in 100) but < 0.1
C	Very Unlikely	$\geq$ 0.001 (1 in 1,000) but < 0.01
D	Doubtful	$\geq$ 0.0001 (1 in 10,000) but < 0.001
E	Highly Unlikely	$\geq$ 0.00001 (1 in 100,000) but < 0.0001
F	Extremely Unlikely	< 0.00001 (1 in 100,000)

Risk Assessment (cont'd)

- Risk Matrices (cont'd)

Table 9. Consequence Categories for a Risk Matrix

Category	Description	Examples
I	Catastrophic	Large number of fatalities, and/or major long-term environmental impact.
II	Major	Fatalities, and/or major short-term environmental impact.
III	Serious	Serious injuries, and/or significant environmental impact.
IV	Significant	Minor injuries, and/or short-term environmental impact.
V	Minor	First aid injuries only, and/or minimal environmental impact.
VI	None	No significant consequence.

Risk Assessment (cont'd)

- Risk Matrices (cont'd)

Table 10. Example Consequence Categories for a Risk Matrix in 2003 Monetary Amounts (US$)

Category	Description	Cost
I	Catastrophic Loss	≥ $10,000,000,000
II	Major Loss	≥ $1,000,000,000 but < $10,000,000,000
III	Serious Loss	≥ $100,000,000 but < $1,000,000,000
IV	Significant Loss	≥ $10,000,000 but < $100,000,000
V	Minor Loss	≥ $1,000,000 but < $10,000,000
VI	Insignificant Loss	< $1,000,000

Risk Assessment (cont'd)

- Risk Matrices (cont'd)
  - Example: Risk Matrix

Refer also to the book for a figure that includes rewards

	A	L	M	M	H	H	H
	B	L	L	M	M	H	H
	C	L	L	L	M	M	H
Probability	**D**	L	L	L	L	M	M
Category	**E**	L	L	L	L	L	M
	F	L	L	L	L	L	L
		VI	**V**	**IV**	**III**	**II**	**I**
	Consequence Category						

Risk Assessment (cont'd)

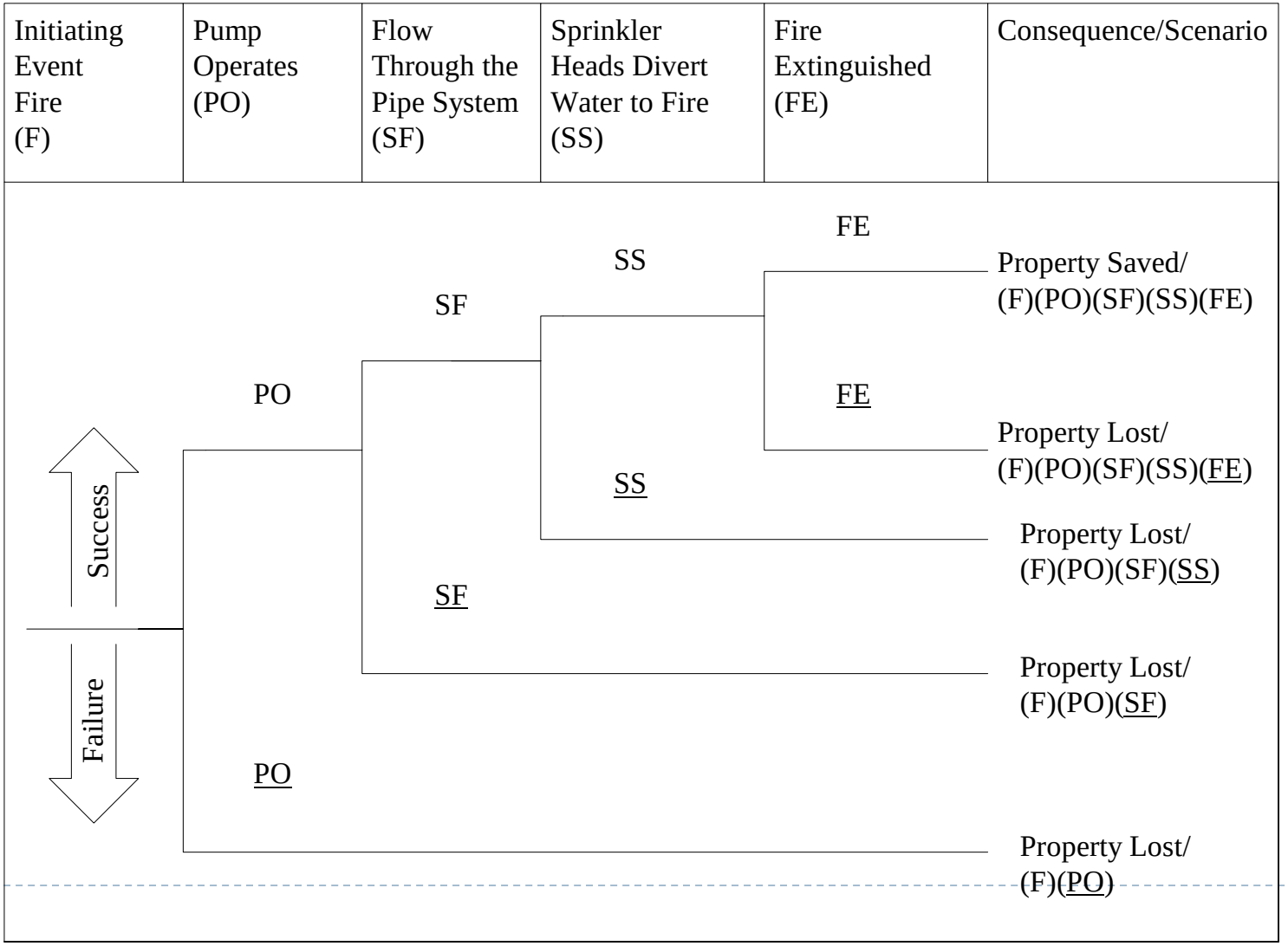
- Event Modeling, Event Trees, Success Trees, and Fault Tress
  - Event modeling is a systematic and often most complete way to identify accident scenarios and quantify risk for risk assessment
  - The combination of event-tree analysis (ETA), success-tree analysis (STA), and fault-tree analysis (FTA) can provide a structured analysis for defining scenarios

Logic Trees Compared

Logic Tree	Analysis Outcomes	Mathematical Foundation	Data Required	Advantages	Limitations
Fault Tree	Calculate the probability of failure Determine the cut sets	Boolean Logic Probability theory including reliability theory	System knowledge, Failure modes and probabilities	Focus on components and failure modes	Complex systems require the use of specialized software
Success Tree	Calculate the probability of success Determine the cut sets	Boolean Logic Probability theory including reliability theory	System knowledge Success modes and probabilities	Focus on success modes	Complex systems require the use of specialized software
Event Tree	Calculate the probability of scenarios and consequences	Probability theory	Events and sequencing Outcome spaces	Multiple outcomes Conceptually simple to develop and solve	Binary outcomes
Probability Tree	Calculate the probability of any uncertain event in a joint probability distribution	Probability theory Bayes Theorem	Events and sequencing Outcome spaces Probabilities Consequences	Multiple outcomes Conceptually simple to develop and solve	Large trees are difficult to understand, display, and solve
Decision Tree	Calculate the outcomes of a decision in order to determine the best decision strategy under uncertainty	Bayes Theorem Utility theory	Events and sequencing Outcome spaces Probabilities Alternatives Consequences	Conceptually simple to develop and solve	Large trees are difficult to understand, display, and solve

Risk Assessment (cont'd)

- **Event-Tree Example for Sprinkler System**



Risk Assessment (cont'd)

- **Fault-Tree and Success-Tree Analyses**
  - *Basic events*. These events cannot be decomposed further into lower level events. They are the lowest events that can be obtained. For these events, failure probabilities need be obtained
  - *Events that can be decomposed further.* These events can be decomposed further to lower levels. Therefore, they should be decomposed until the basic events are obtained

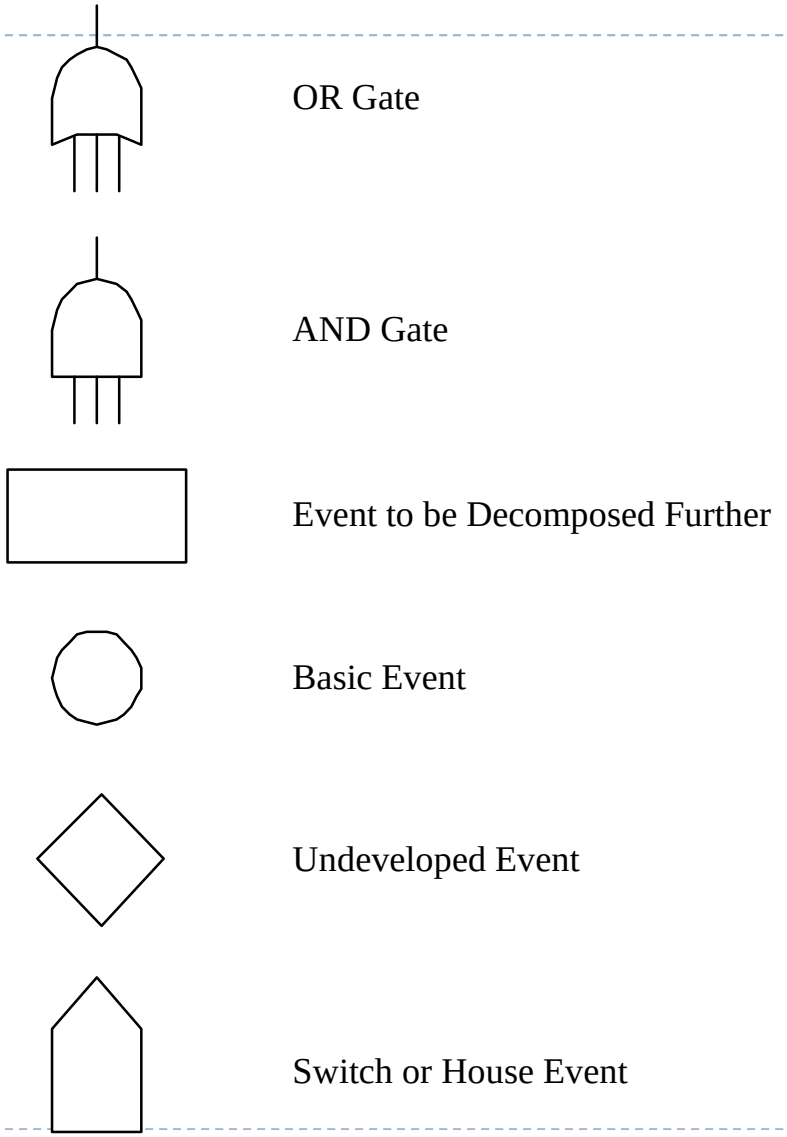
Risk Assessment (cont'd)

- *Undeveloped events*. These events are not basic and can be decomposed further; however, because they are not important, they are not developed further of these events are very small or the effect of their occurrence on the system is negligible, or can be controlled or mediated
- *Switch (or house) events.* These events are not random, and can be turned on or off with full control

The symbols shown in the following figure (Figure 2) are used for these events.

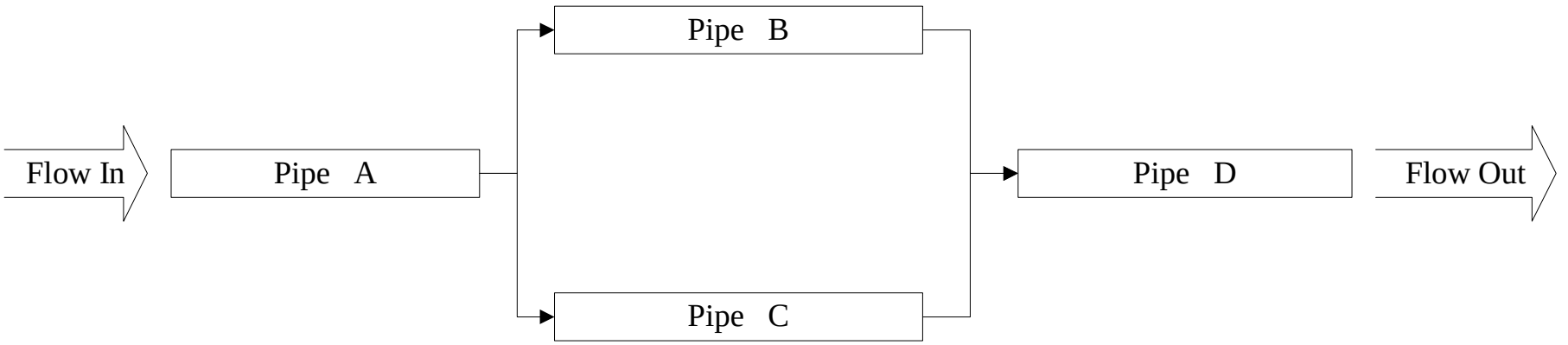
Risk Assessment (cont'd)

- Figure 2. Symbols Used in Fault-Tree Analysis



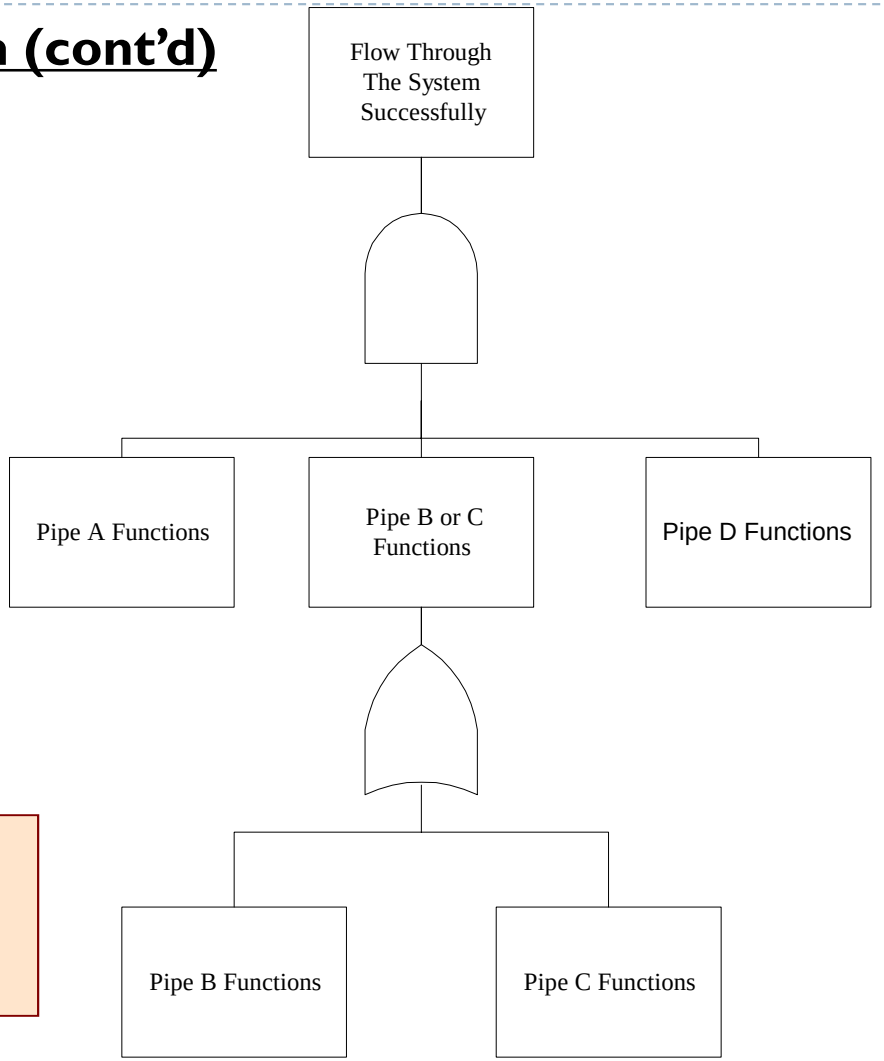
Risk Assessment (cont'd)

- FTA requires the development of a tree-looking diagram for the system that shows failure paths and scenarios that can result in the occurrence of a top event. The construction of the tree should be based on the building blocks and the Boolean logic gates
- **Example: Piping System**



Risk Assessment (cont'd)

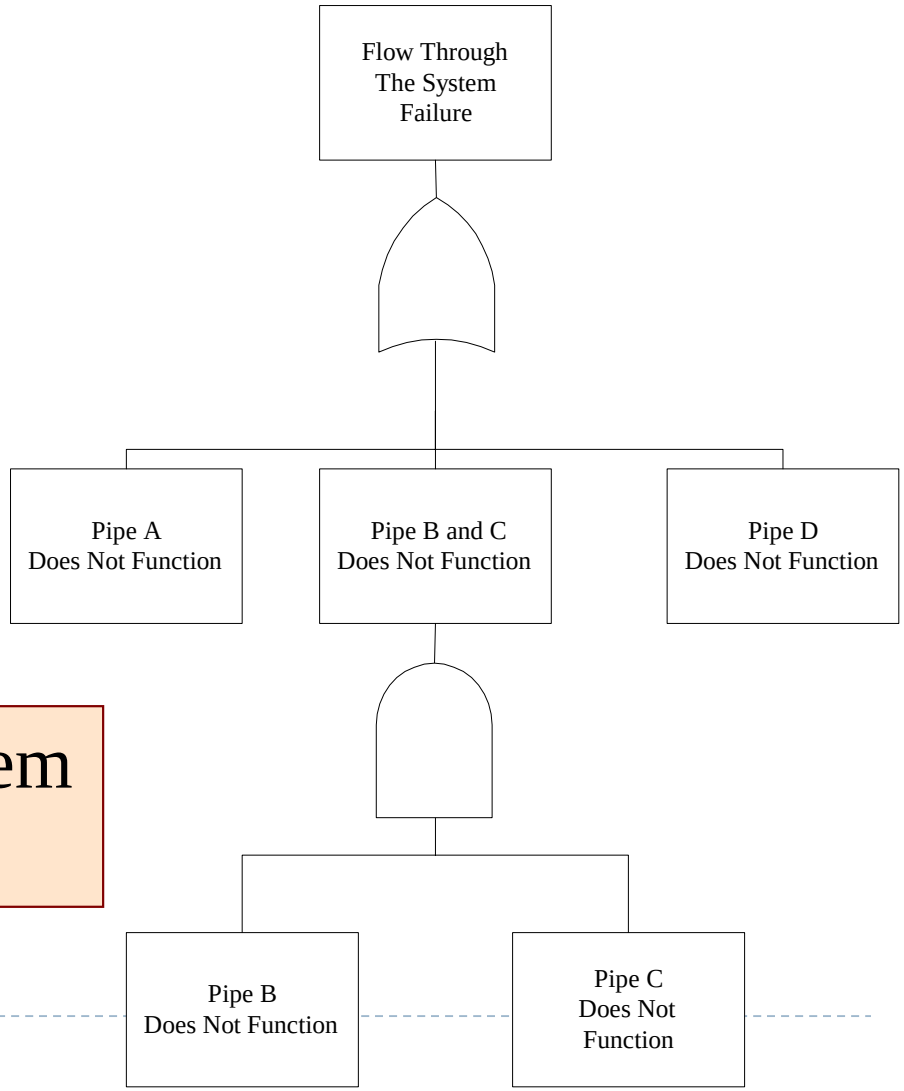
- **Example: Piping System (cont'd)**



Success Tree for the Pipe System Example

Risk Assessment (cont'd)

- **Example: Piping System (cont'd)**



Fault Tree for the Pipe System Example

Risk Assessment (cont'd)

- **Example: Piping System (cont'd)**
  - Using the fault tree model, the top event (T) can be given as

$$T = A \text{ or } (B \text{ and } C) \text{ or } D$$

  - Minimal cut sets:

$$A, BC, D \qquad (5)$$

  - Based on the theory of probability, the probability (P) of the top event can be computed as a function of pipe failure probabilities as follows (independent case and mutually exclusive case, respectively):

$$P(T) = 1 - [1 - P(A)][1 - P(B)P(C)][1 - P(D)] \qquad (6a)$$

$$P(T) = P(A) + P(B)P(C) + P(D) \qquad (6b)$$

See second edition for examples

Risk Assessment (cont'd)

- **Example: Piping System (cont'd)**
  - **The number of possible failure scenarios (assuming only two possible outcomes for each basic event) is bounded by:**

$$\text{Failure paths} = 2^n \qquad (7)$$

Risk Assessment (cont'd)

- Several methods for generating minimal cut sets are available. One of the methods is based on a top-down search of the Boolean logic
- Another algorithm for generating cut sets is based on a bottom up approach that substitutes the minimal cut sets from lower level gates into upper level gates
- According to Eq. 5, the minimal cut sets are

$$A \tag{8a}$$

$$D \tag{8b}$$

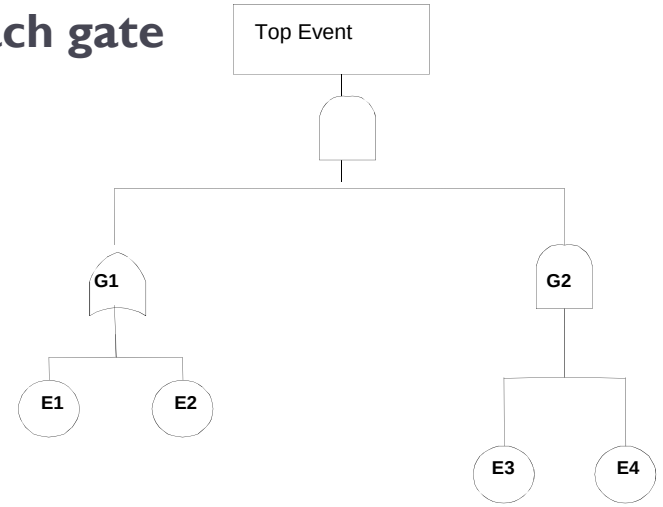
$$B \text{ and } C \tag{8c}$$

Risk Assessment (cont'd)

- A minimal cut set includes events that are all necessary for the occurrence of the top event. For example, the following cut set is not a minimal cut set:

A and B (9)

- The minimal cut sets can be systematically generated using the following algorithm:
  1. **Provide a unique label for each gate**
  2. **Label each basic event**
  3. **Set up a two cell array**



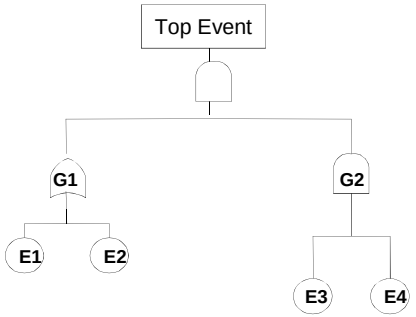
Risk Assessment (cont'd)

4. **Place the top event gate label in the first row, first column:**

Top	

5. **Scan each row from left to right replacing:**
   - **each OR gate by a vertical arrangement defining the input events to the gate, and**
   - **each AND gate by a horizontal arrangement defining the input events to the gate.**

For example, the following table sequence can be generated for an AND top gate with two gates below (Gate 1 of OR type, and Gate 2 of AND type):



Top (AND)	

Risk Assessment (cont'd)

Leading to the following:

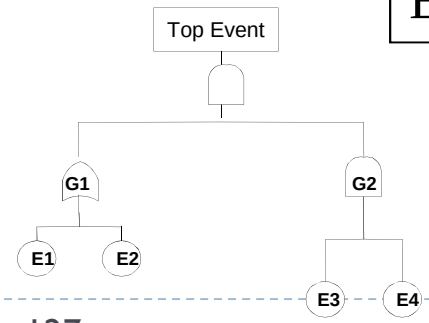
Gate1(OR)	Gate2(AND)

If Gate 1 has two events with OR Gate (1 and 2), then

Event 1	Gate2
Event 2	Gate2

If Gate 2 has two events with AND Gate (3 and 4), then

Event 1	Event 3	Event 4
Event 2	Event 3	Event 4



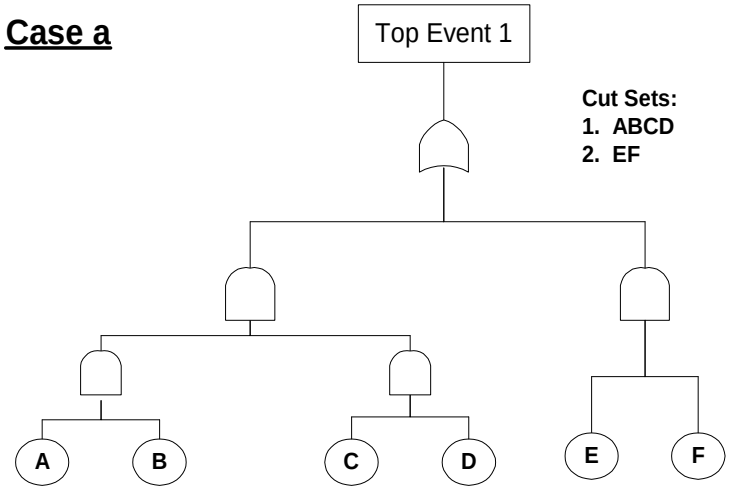
Risk Assessment (cont'd)

6. **When no gate events remain, each row is a cut set**
7. **Remove all non-minimal combinations of events such that only minimal cut sets remain**
8. **Compute the occurrence probability for each minimal cut set as the products of the probabilities of its underlying events**
9. **Compute the system (top event) occurrence probabilities as the sum of the occurrence probabilities of all the minimal cut sets (mutually exclusive)**

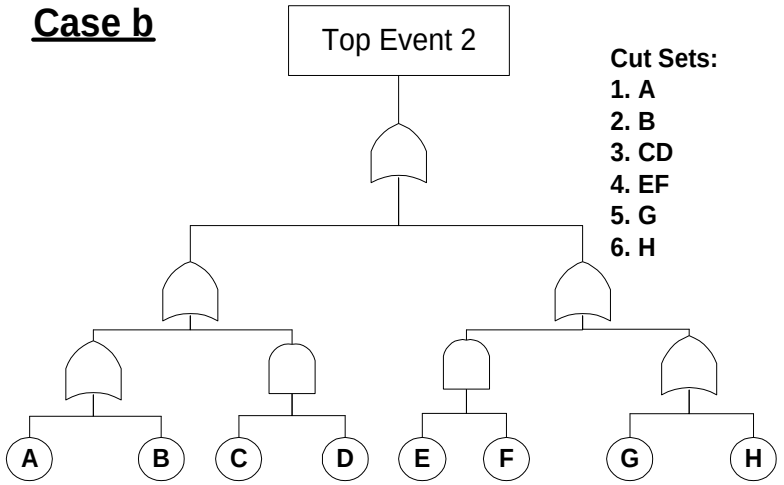
Risk Assessment (cont'd)

Trends in Fault Tree Models and Cut Sets

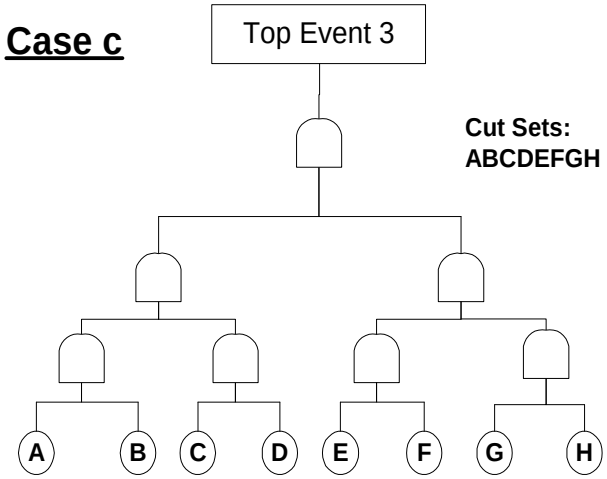
Case a



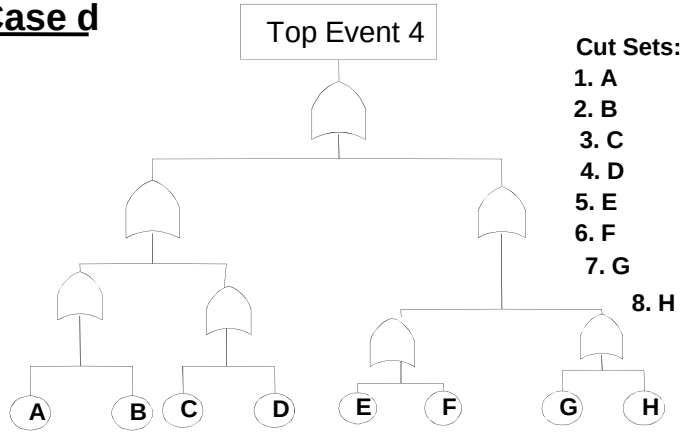
Case b



Case c



Case d



Risk Assessment (cont'd)

- Common Cause Scenarios
  - Common-cause scenarios are events or conditions that result in the failure of seemingly separate systems or components
  - Common-cause failures complicate the process of conducting risk analysis because a seemingly redundant system can be rendered ineffectively by common-cause failure
    - Physical
    - Logical
    - Human

Risk Assessment (cont'd)

- Sensitivity or Importance Factors:
  Needed for reducing the sizes of trees (tree pruning) and/or enhancing reliability
  - ***Fussell-Vesely Factor*.** For any event (basic or undeveloped) in a fault tree, the Fussell-Vesely factor (FVF) for the event is given by

$$FVF = \frac{\sum_{\text{all sets containing the event}} \text{occurrence probability of minimal cut set}}{\sum_{\text{all sets}} \text{occurrence probability of minimal cut set}} \qquad (10)$$

Risk Assessment (cont'd)

The FVF measures the contribution significance of the event to the failure probability of the system. Events of large FVF should be used to reduce failure probability of the system by reducing their occurrence probabilities

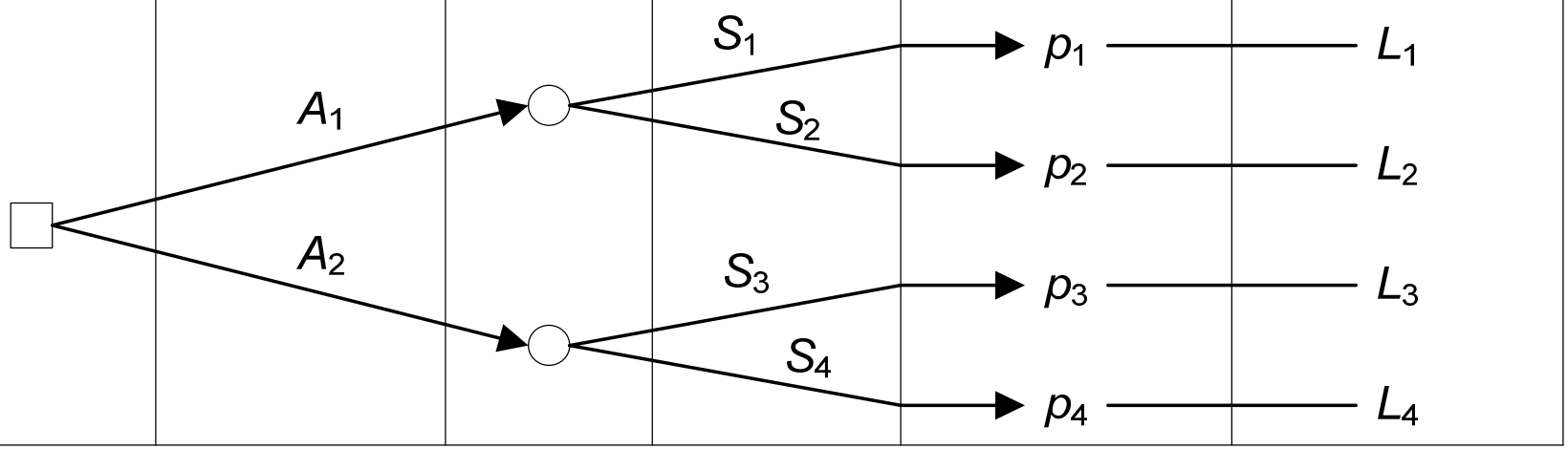
- ***Birnbaum Factor.*** For any event (basic or undeveloped) in a fault tree, the Birnbaum factor (BF) for the event is given by

$$BF = \frac{\sum_{\text{all sets containing the event}} \text{occurrence probability of minimal cut set}}{\text{occurrence probability of the event}} \qquad (11)$$

Risk Assessment (cont'd)

- The BF measures the sensitivity of the failure probability of the system to changes to the occurrence probability of the event. Events of large BF should be used to reduce failure probability of the system by reducing their occurrence probabilities

Decision Trees

A Decision Node	Alternatives (A)	Chance Nodes	System States (S)	Scenario Probability (p)	Loss or Consequence (L)
					

Risk Assessment (cont'd)

- Human-Related Risks
  - Human Error Identification
    - Human errors are unwanted circumstances caused by humans that result in deviations from expected norms that place systems at risk
    - It is important to identify the relevant errors to make a complete and accurate risk assessment
    - Human error identification techniques should provide a comprehensive structure for determining significant human errors within a system

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Human Error Modeling
    - Currently, there is no consensus on how to model human reliably. The human-error-rate estimates are often based on simulation tests, models, and expert opinion
  - Human Error Quantification
    - still a developing science requiring understanding of human performance, cognitive processing, and human perceptions

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Reducing Human Errors
    - Error reduction is concerned with lowering the likelihood for error in an attempt to reduce risk
    - The reduction of human errors may be achieved by human factors interventions or by engineering means
    - Engineering means of error reduction may include automated safety systems or interlocks

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Game Theory for Intelligent Threats
    - Rooted in economics, war gaming, defense, etc.
    - Mixes behavior, preferences, decision making and uncertainty
    - Game theory can be used to model human behavior, herein as a threat to a system

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Game Theory for Intelligent Threats
    - Each player seeks a utility, i.e., benefit, that is a function of the desired state of the system
    - A classical example used to introduce game theory is called the prisoners' dilemma. Payoff is in lowering prison years. Dominant strategy maximizes payoff. If all players select dominant strategies, the situations is called dominant strategy (Nash) equilibrium. Mixed strategies involve probabilities for choices

e.g., Action of S1 | S2=Confess

		Second Suspect	
		Confess	Don't Confess
First Suspect	Confess	(10, 10)	(0, 20)
	Don't Confess	(20, 0)	(1, 1)

Bilateral Stability: Payoffs and Preferences

- Define the **values** or **rankings**, respectively, of outcomes associated with all combinations of choices by players

Payoffs

		USSR: Disarm	USSR: Arm
US	Disarm	(6,6)	(-7,7)
US	Arm	(7,-7)	(-1,-1)

Preferences

		USSR: Disarm	USSR: Arm
US	Disarm	(2,2)	(4,1)
US	Arm	(1,4)	(3,3)

(a,b)

"Row" player — "Column" player

Preferences

1 = most preferred
4 = least preferred

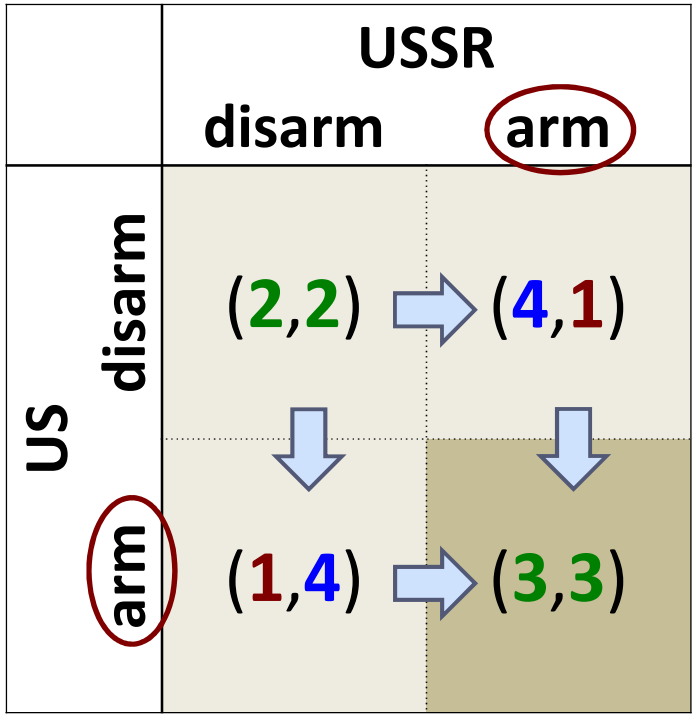
Preferences are more straightforward to develop and justify and, if consistent with payoffs, result in identical game play*

* for non-iterative, non-mixed strategy games with complete and "certain" information

2-Player Games

- Prisoners' Dilemma
- Chicken
- Deadlock
- Combinations
- Perceptual Dilemma

Prisoner's Dilemma



- **Both sides:**
  - **Most prefer to dominate**
  - **Prefer mutual disarming to mutual arming**
  - **Least like being dominated**
- **Arming is a *dominant* strategy for both sides**
- **Dilemma: Equilibrium exists at (arm, arm), yet better outcome for both sides is (disarm, disarm)**

The Prisoner's Dilemma has often been invoked to represent the Cold War US-USSR nuclear arms competition

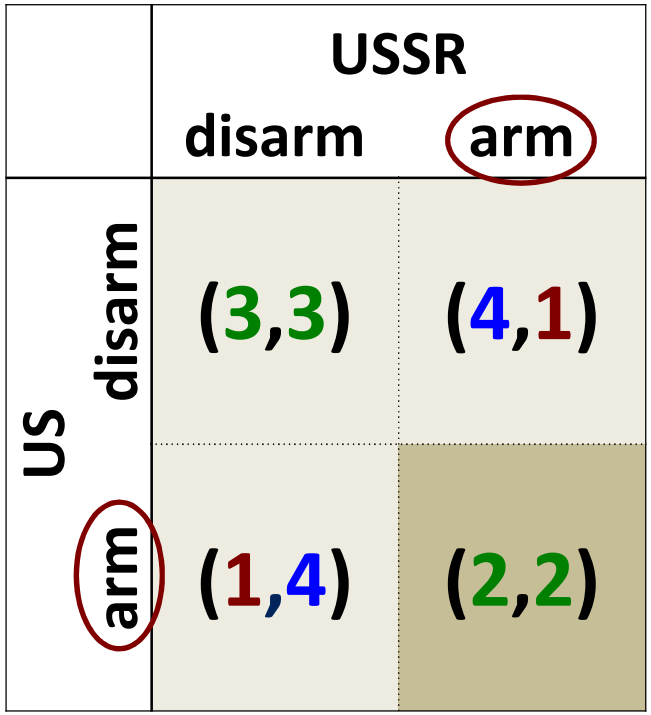
Chicken (aka Hawk-Dove)

		USSR: disarm	USSR: arm
US	disarm	(2,2)	(3,1)
US	arm	(1,3)	(4,4)

- **Both sides:**
  - **Most prefer to arm while the other side disarms**
  - **Prefer mutual disarming to sole disarming**
  - **Least like mutual arming**
- **Equilibria at both (arm, disarm) and (disarm, arm)**
- **No dominant strategy for either side**

Chicken has also been invoked to represent the Cold War US-USSR nuclear arms competition.

Deadlock (aka the Leader's Game)



- Both sides still
  - Most prefer to dominate
  - Least like being dominated
- Both sides prefer mutual arming to mutual disarming

Deadlock is also a reasonable representation of the Cold War US-USSR arms competition, but is less mentioned in the literature.

Stag Hunt (aka Assurance, Reciprocity)

		USSR: disarm	USSR: arm
US	disarm	(1,1)	(4,2)
US	arm	(2,4)	(3,3)

- **Both sides:**
  - **Most prefer mutual disarming**
  - **Prefer sole arming to mutual arming**
  - **Least like sole disarming**
- **Equilibria at both (arm, arm) and (disarm, disarm)**
- **No dominant strategy for either side**

Stag Hunt has also been invoked to represent the Cold War US-USSR nuclear arms competition, but has been overshadowed by Prisoner's Dilemma and Chicken. Game theorists generally dismiss it as trivial.

Game Comparison: US Preferences

Chicken

		USSR: disarm	USSR: arm
US	disarm	2	3
	arm	1	4

Prisoner's Dilemma

		USSR: disarm	USSR: arm
US	disarm	2	4
	arm	1	3

Stag Hunt

		USSR: disarm	USSR: arm
US	disarm	1	4
	arm	2	3

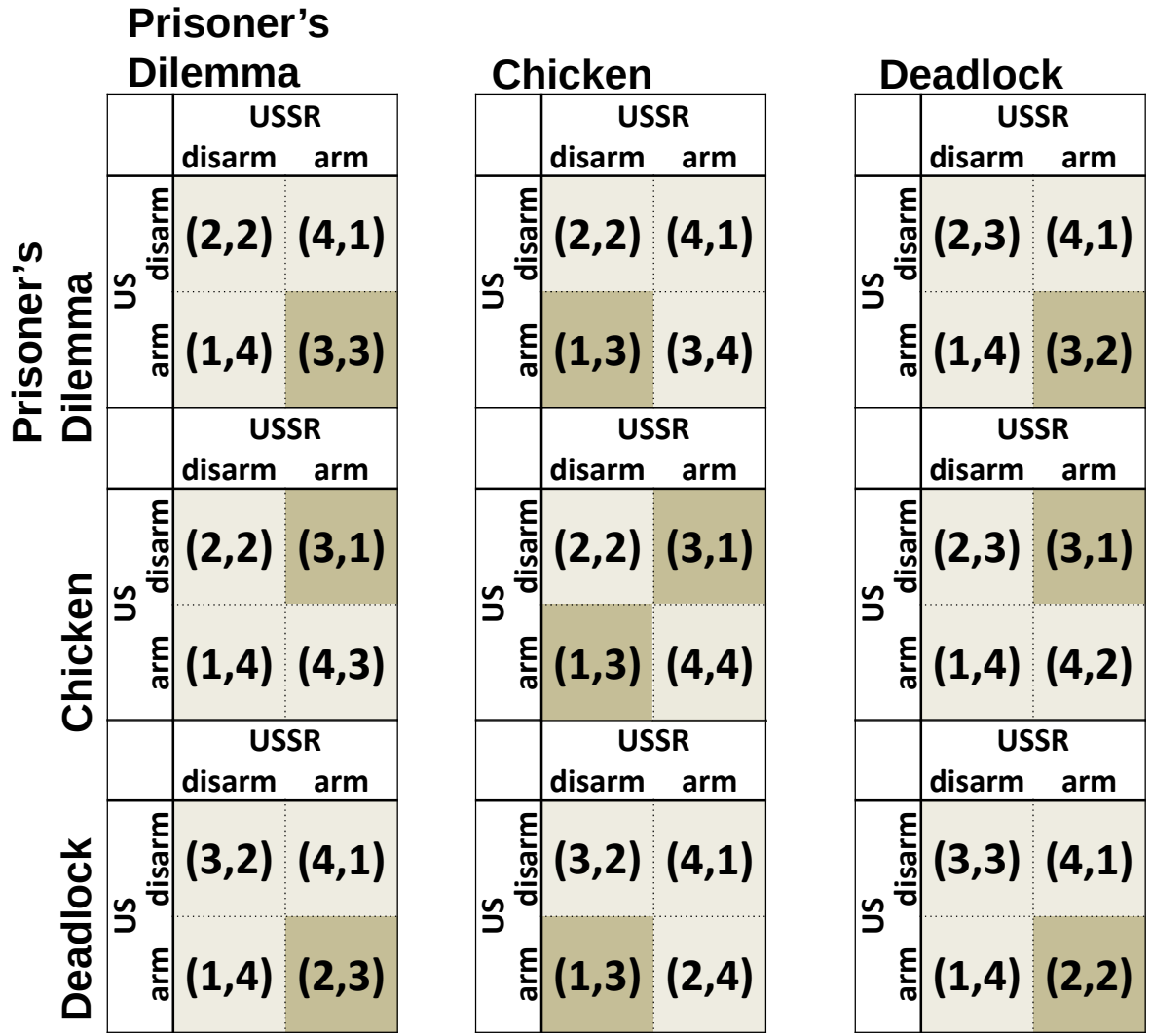
Deadlock

		USSR: disarm	USSR: arm
US	disarm	3	4
	arm	1	2

- All are defensible, and preferences can shift over time
- Rationales have generally been weak (or nonexistent)
- Implications of differences not well-studied

It is not within the domain of game theorists' expertise to develop such outcome preferences, but that is what has generally been done.

Some Combinations



- **Both sides need not be playing the same game**
- **Myriad defensible possibilities, but none compelling**
- **Combinations without "dilemmas" may be "boring" to game theorists**
- **Only a side playing Chicken is motivated to disarm**

Perceptual Dilemma

US Half of a Mutual Perceptual Dilemma

US: Stag Hunt

USSR: Prisoner's Dilemma

US \ USSR	disarm	arm
disarm	(1,2)	(4,1)
arm	(2,4)	(3,3)

USSR Half of a Mutual Perceptual Dilemma

US: Prisoner's Dilemma

USSR: Stag Hunt

US \ USSR	disarm	arm
disarm	(2,1)	(4,2)
arm	(1,4)	(3,3)

- **Each party most prefers mutual disarmament (but is prevented from disarming by the *perception* that the other side most prefers unilateral arming)**
- **Both sides still:**
  - **Prefer dominating to mutual arming**
  - **Least like unilaterally disarming**

Perceptual Dilemma has been offered as an alternative representation of latter stages of the Cold War US-USSR arms competition.*

*S. Plous, "Modeling the Nuclear Arms Race as a Perceptual Dilemma," *Philosophy and Public Affairs*, Vol. 17, No. 1 (1988)

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Game Theory for Intelligent Threats
    - Zero-Sum Payoff Table for Unit-Price (in Dollars) Competition

		Second Company	
		Price = $100	Price = $200
First Company	Price = $100	(0, 0)	(500, -500)
	Price = $200	(-500, 500)	(0, 0)

Risk Assessment (cont'd)

- Human-Related Risks (cont'd)
  - Game Theory for Intelligent Threats
    - Variable Sum-Game in Price Competition: Payoff Table (in Million Dollars) for Unit-Price (in dollars) Competition

		Second Company		
		Price = 100	Price = 200	Price = 300
First Company	Price = 100	(0, 0)	(50, -10)	(40, -20)
	Price = 200	(-10, 50)	(20, 20)	(90, 10)
	Price = 300	(-20, 40)	(10, 90)	(50, 50)

    - Continuous choices: Use linear programming for optimization purposes

Risk Assessment (cont'd)

- Economic and Financial Risks
  - Market Risks
    - Fluctuating Interest rates
  - Credit Risks
    - Credit risks are associated with potential defaults on notes or bonds, as examples, by corporations including subcontractors
    - Also, credit risks can be associated with market sentiments that determine a company likelihood of default that could affect its bond rating and ability to purchase money, and maintain projects and operations

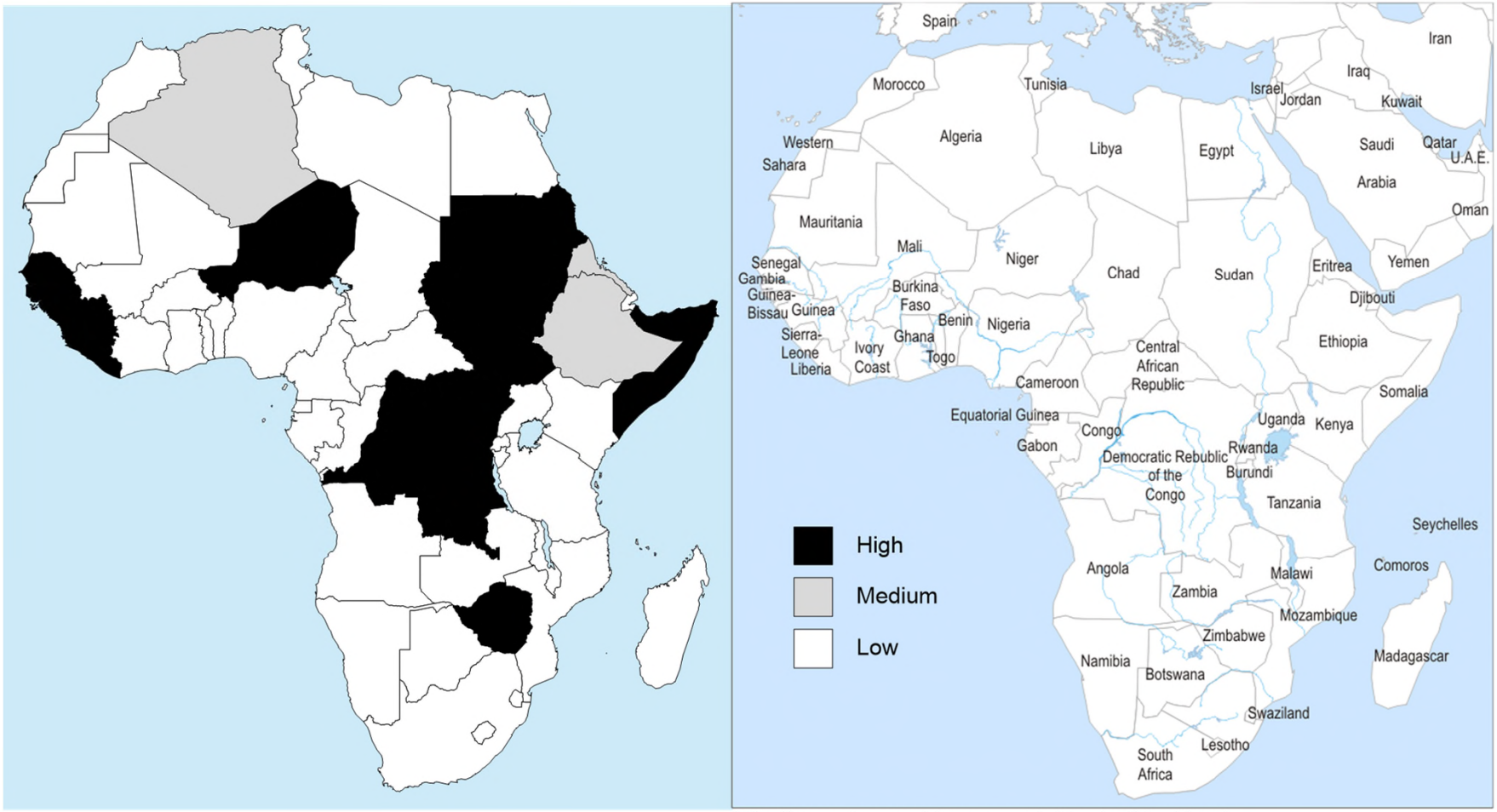
Risk Assessment (cont'd)

- Economic and Financial Risks (cont'd)
  - Operational Risks
    - Operational risks are associated with several sources that include out-of-control operations risk that could occur when a corporate branch undertake significant risk exposure that is not accounted for by a corporate headquarters leading potentially to its collapse
    - An example being the British Barings Bank that collapsed as a result of primarily its failure to control the market exposure being created within a small overseas branch of the bank

Risk Assessment (cont'd)

- Economic and Financial Risks (cont'd)
  - Reputation Risks
    - The loss of business attributable to decrease in a corporation's reputation can pose another risk source
    - This risk source can affect its credit rating, ability to maintain clients, workforce, etc.
    - This risk source usually occurs at a slow attrition rate
    - It can be an outcome of poor management decisions and business practices

Political and Country Risks



http://www.freeworldmaps.net/africa/political.html

Example

Risk Assessment (cont'd)

- Data Needs for Risk Assessment
  - Quality data are needed
  - Quality data lead to quality in results
  - Data can be classified as
    - "What can go wrong" data
    - Failure probability data
    - Failure consequence data
  - Data sources and reliability
  - Chapter 8

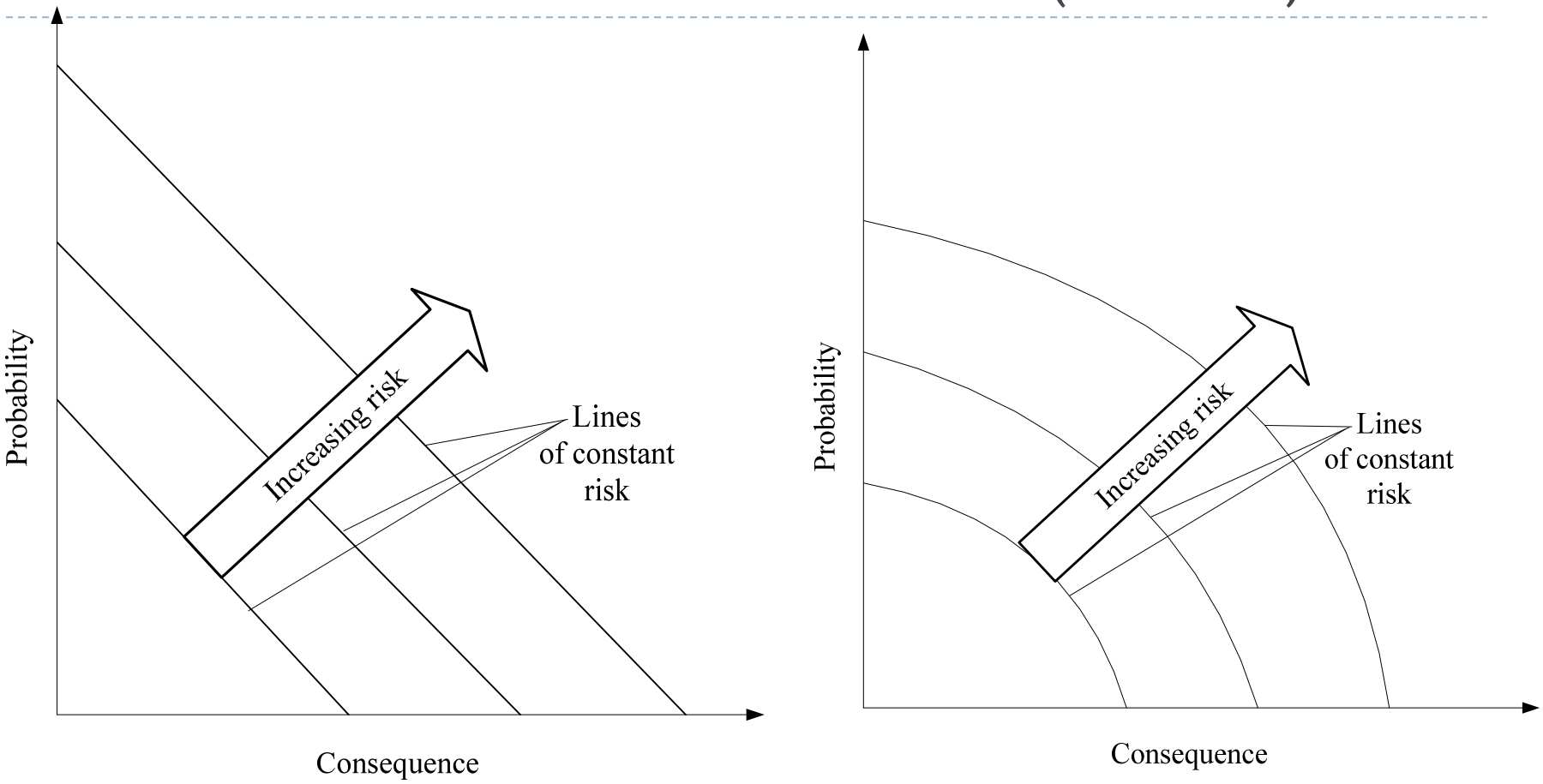
Risk Treatment and Control

- Adding risk control to risk assessment produces risk treatment or management
- Risk treatment is the process by which system operators, managers, and owners make safety decisions, regulatory changes, and choose different system configurations based on the data generated in the risk assessment

Risk Treatment and Control (cont'd)

- Risk management involves using information from the previously described risk assessment stage to make educated (informed) decisions about system safety
- Risk control includes
  - Failure prevention (countermeasures)
  - Consequence mitigation

Risk Treatment and Control (cont'd)



(A) Risk Neutral

(B) Risk Averse

Risk Treatment and Control (cont'd)

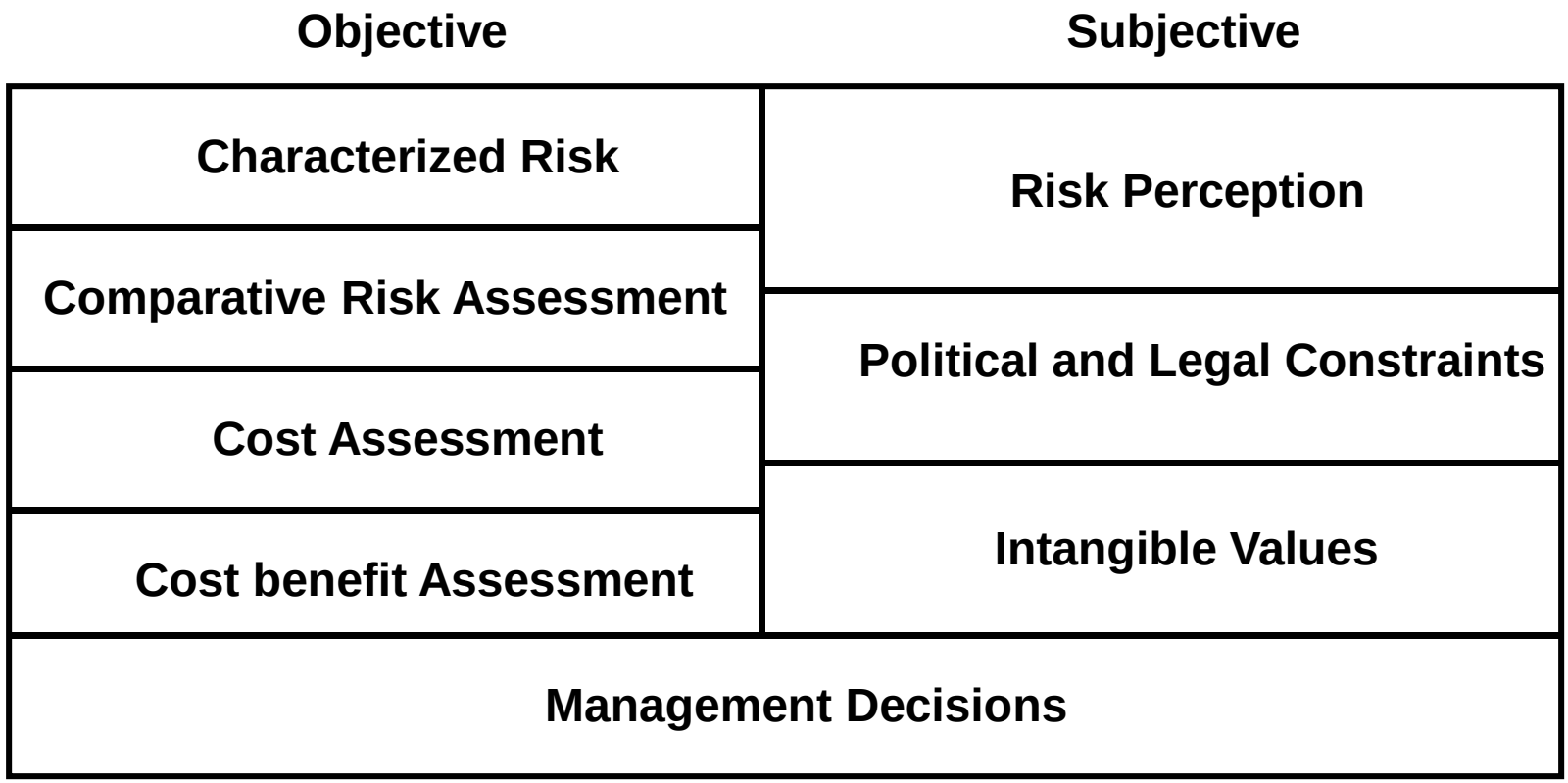
Assessing and Managing Risk

Since risk cannot be eliminated, the problem people face, individually and collectively, is how much risk should they live with and how should they go about managing the risk?

To answer the above questions, analytical tools must be built that enable understanding and modeling exposure, effects, human perception, and human evaluation processes

Risk Treatment and Control (cont'd)

Components of Risk Management



Risk Treatment and Control (cont'd)

- The cornerstone of risk management is risk assessment
- Under ideal conditions, the risk manager would decide a management option solely on the basis of a cost/benefit assessment whereby the benefit is expressed in reduction of risk
- In practice, there are significant obstacles for such a decision

Risk Treatment and Control (cont'd)

- Risk management is inherently complex and includes a large number of elements
- Contrary to the general opinion, risk management includes not only subjective but also objective elements
- Risk analysis can be used to make informed decisions

Risk Treatment and Control (cont'd)

Qualitative Risk Assessment Using Severity/Probability Factor Rating

High	2	2	3
Medium	1	1	2
Low	0	1	2
Severity Factor	Low	Medium	High
	Probability Factor		

Severity/Probability Factor Rating
3: Mitigation strategy and detailed contingency plan
2: Mitigation strategy and outlined contingency plan
1: Mitigation strategy
0: Treat as a project base assumption

Risk Treatment and Control (cont'd)

- Table 11. Methods for Determining Risk Acceptance

Risk Acceptance Method	Summary
Risk Conversion Factors	**This method addresses the attitudes of the public about risk through comparisons of risk categories. It also provides an estimate for converting risk acceptance values between different risk categories.**
Farmers Curve	**It provides an estimated curve for cumulative probability risk profile for certain consequences (e.g., deaths). It demonstrates graphical regions of risk acceptance/non-acceptance.**
Revealed Preferences	**Through comparisons of risk and benefit for different activities, this method categorizes society preferences for voluntary and involuntary exposure to risk.**
Evaluation of Magnitude of Consequences	**This technique compares the probability of risks to the consequence magnitude for different industries to determine acceptable risk levels based on consequence.**
Risk Reduction Effectiveness	**It provides a ratio for the comparison of cost to the magnitude of risk reduction. Using cost-benefit decision criteria, a risk reduction effort should not be pursued if the costs outweigh the benefits. This may not coincide with society values about safety.**
Risk Comparison	**The risk acceptance method provides a comparison between various activities, industries, etc., and is best suited to comparing risks of the same type.**

Risk Treatment and Control (cont'd)

- Risk Conversion Factors
  - The public is willing to accept voluntary risks roughly one hundred times greater than that for involuntary imposed risks
  - The statistical death rate appears to be a psychological yardstick for establishing the level of acceptability of other risks
  - The acceptability of risk appears to be crudely proportional to the third power of the benefits, either real or imaginary

Risk Treatment and Control (cont'd)

Table 12. Risk Conversion Values for Different Risk Factors

Risk Factors	Risk Conversion (RF) Factor	Computed RF Value
Origin	**Natural/human-made**	**20**
Severity	**Ordinary/catastrophic**	**30**
Volition	**Voluntary/involuntary**	**100**
Effect	**Delayed/immediate**	**30**
Controllability	**Controlled/uncontrolled**	**5 to 10**
Familiarity	**Old/new**	**10**
Necessity	**Necessary/luxury**	**1**
Costs	**Monetary/non-monetary**	**NA**
Origin	**Industrial/ Regulatory**	**NA**
Media	**Low profile/ high profile**	**NA**

NA = not available

Risk Treatment and Control (cont'd)

Table 13. Classification of Common Risks

		Voluntary		Involuntary	
Source	**Size**	**Immediate**	**Delayed**	**Immediate**	**Delayed**
Human Made	**Catastrophic**	**Aviation**		**Dam failure Building fire Nuclear accident**	**Pollution Building fire**
	Ordinary	**Sports Boating Automobiles**	**Smoking Occupation Carcinogens**	**Homicide**	
Natural	**Catastrophic**			**Earthquakes Hurricanes Tornadoes Epidemics**	
	Ordinary			**Lighting Animal bites**	**Disease**

Table 14. Individual Fatality Rates

Fatal Event	Total Number**	Fatalities/Year (10^{-4})**	Age-Adjusted Rate (10^{-4})
Total deaths	2,312,200	88.0	50.3
Disease			
Cardiovascular	952,500	36.3	17.5
Cancer	538,000	20.5	13.0
Pulmonary	188,300	7.2	3.4
AIDS	31,256	1.2	NA
Accidents			
Motor vehicle	41,800	1.6	1.6
Falls	13,450	0.52	NA
Poisons	8994	0.35	NA
Fires/electrical	4547	0.17	NA
Drowning	3404	0.13	NA
Firearms/handguns	1356	0.05	NA
Air/space	1075	0.04	NA
Water transport	723	0.03	NA
Railway	635	0.02	NA
Suicide	30,900	1.2	1.1
Homicide	21,600	0.8	0.8

*1994/1995 data

** 2003/2004 data show 2,398,365 deaths per year, and 81.7 Fatalities/Year (10^{-4})

Table 14. Individual Fatality Rates

Trends in Age-Adjusted Death Rate

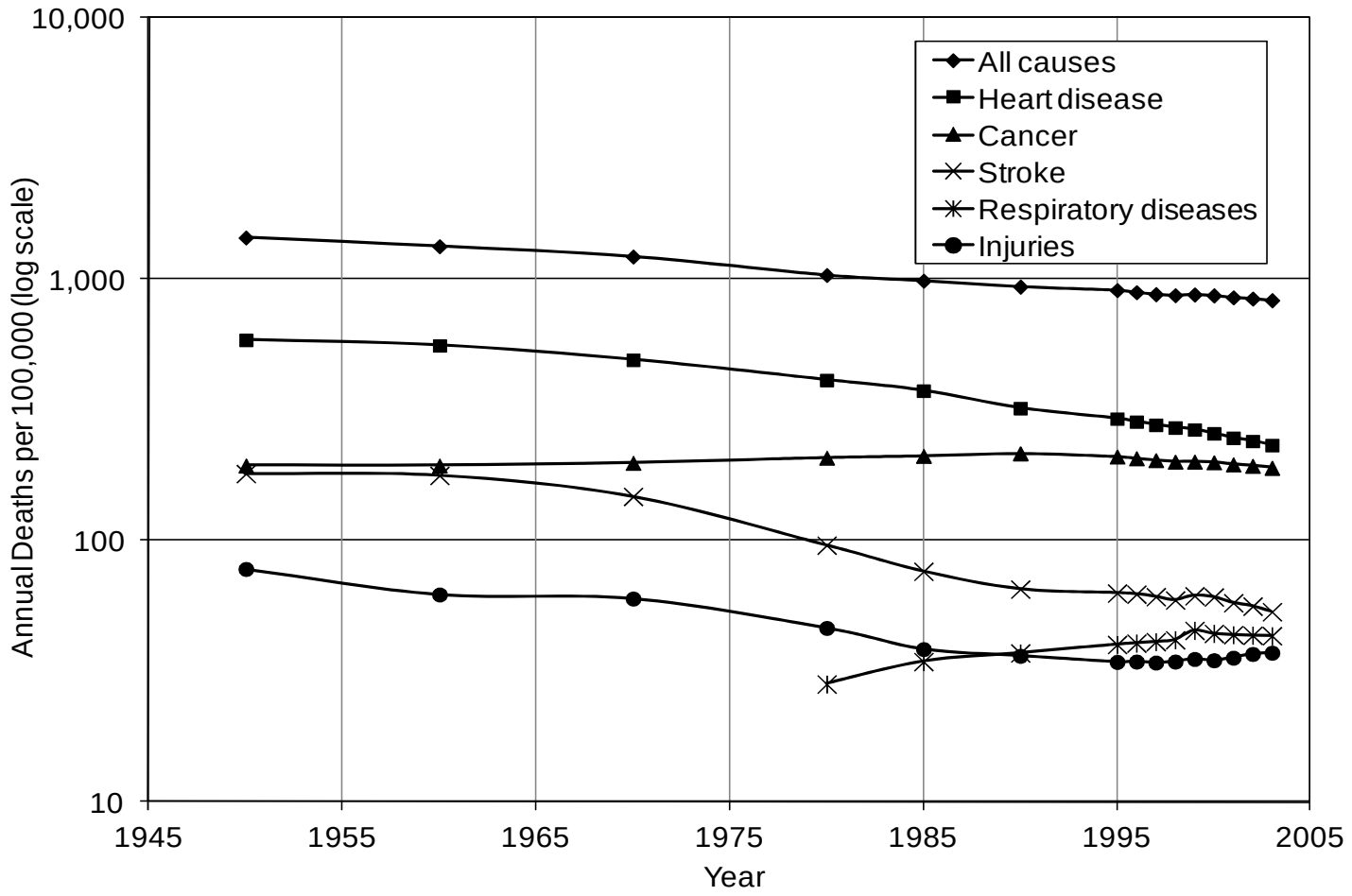


Table 14. Individual Fatality Rates

Trends in Life Expectancy

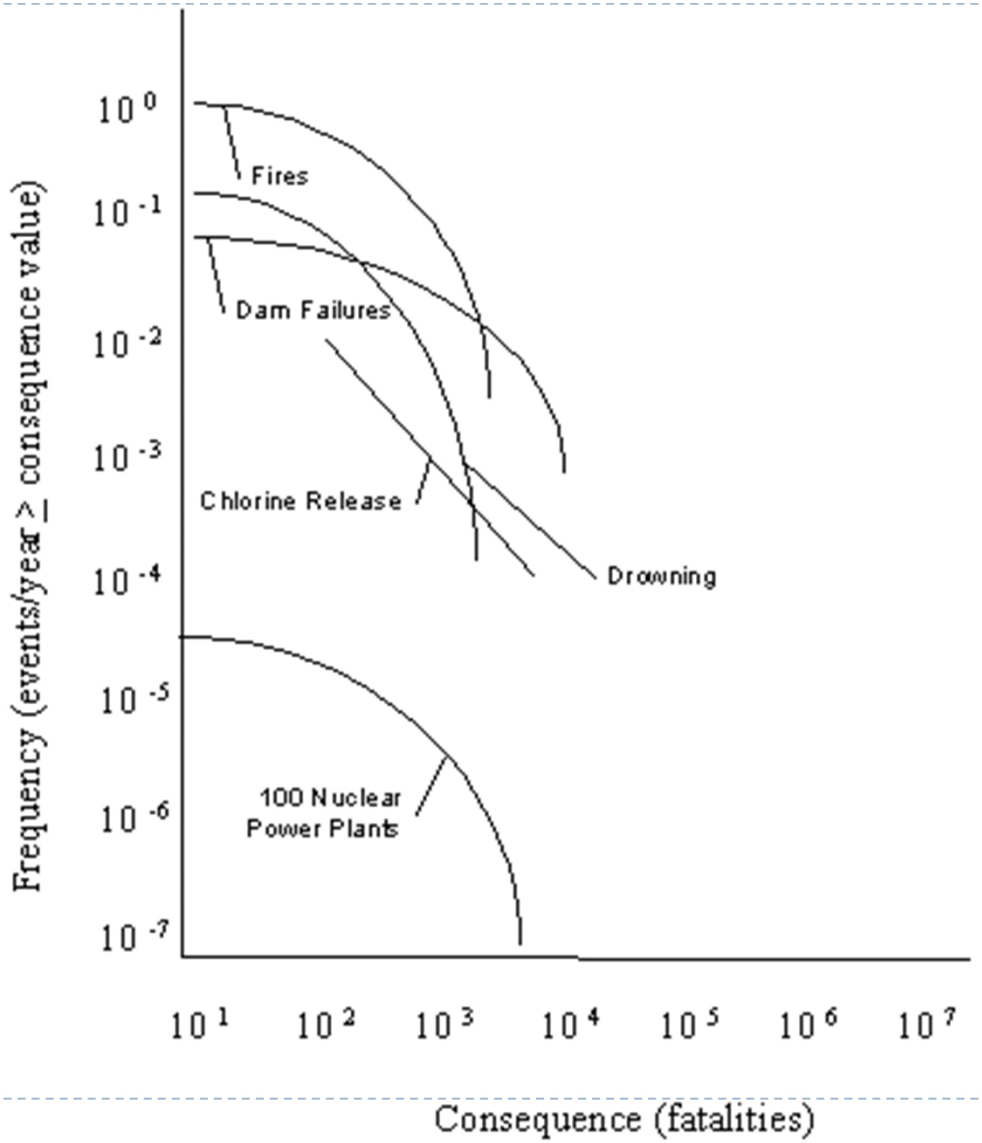
Risk Treatment and Control (cont'd)

Table 15. Natural Disaster Fatality Rates

Disaster	Years	Deaths	Rate (10^{-7})
Lightning	**1959 to 1993**	**91**	**4.2**
Tornadoes	**1995**	**30**	**1.1**
	1985 to 1994	**48**	**1.9**
Hurricanes/Tropical Storms	**1995**	**29**	**1.1**
	1985 to 1994	**20**	**0.8**
Floods	**1995**	**103**	**3.9**
	1985 to 1994	**105**	**4.2**

Risk Treatment and Control (cont'd)

- Farmer's Curve



Risk Treatment and Control (cont'd)

- Method of Revealed Preferences
  - This technique assumes that the risk acceptance by society is found in the equilibrium generated from historical data on risk versus benefit
  - The estimated lines for acceptance of different activities are separated by the voluntary/ involuntary risk categories

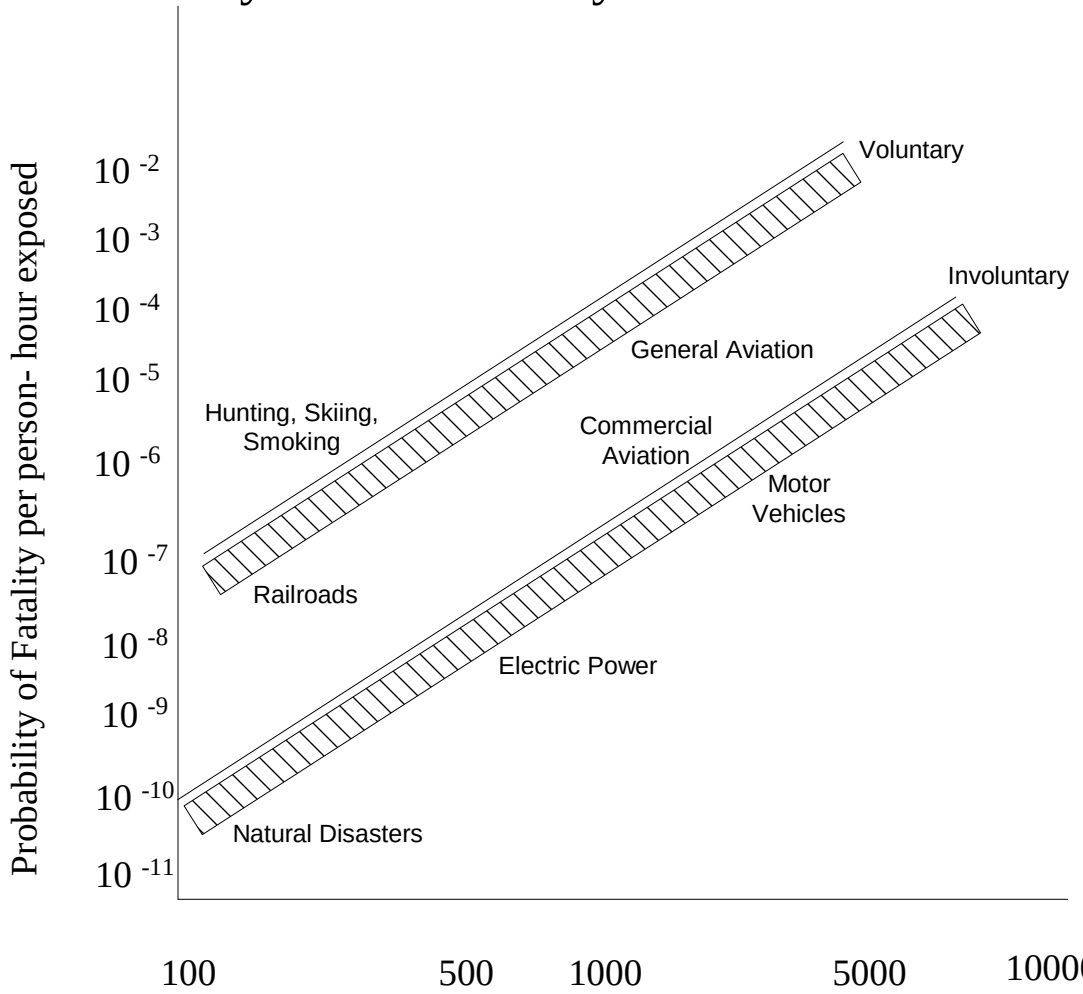
Risk Treatment and Control (cont'd)

- Method of Revealed Preferences (cont'd)
  - Further analysis of the data led to estimating the relationship between risk and benefit as follows:

$$Risk \sim Benefit^3 \qquad (12)$$

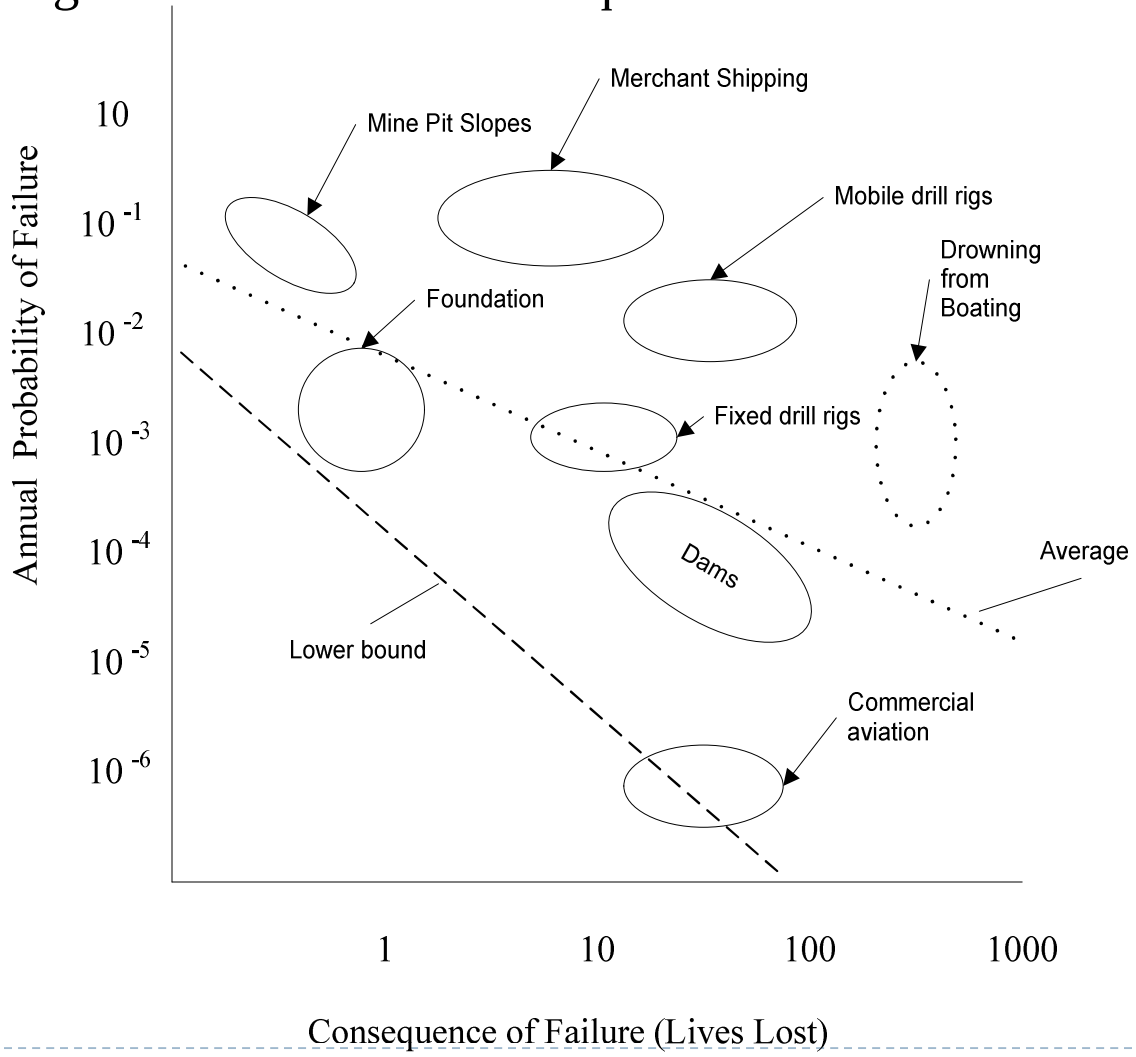
Risk Treatment and Control (cont'd)

Accepted Risk of Voluntary and Involuntary Activities



Risk Treatment and Control (cont'd)

Target Risk Based on Consequence of Failure for Industries



Risk Treatment and Control (cont'd)

- Magnitudes of Risk Consequence
  - The larger the consequence, the less the likelihood that this event may occur, CIRIA (lower bound):

$$P_f = 10^{-4}\frac{KT}{n} \qquad (13)$$

***Construction Industry Research and Information Association* (CIRIA)**

T = life of the structure
K = a factor regarding the redundancy of the structure
n = the number of people exposed to risk.

Risk Treatment and Control (cont'd)

- Magnitudes of Risk Consequence (cont'd)
  - Another estimate is Allen's equation (average) that is given by:

$$P_f = 10^{-7} \frac{TA}{W\sqrt{n}} \qquad (14)$$

T = the life of the structure
n = is the number of persons exposed to risk
A and W = factors regarding the type and redundancy of the structure

Risk Treatment and Control (cont'd)

- Risk Reduction Cost Effectiveness Ratio

$$Risk\ \text{Re}duction\ Effectiveness = \frac{Cost}{\Delta\ Risk} \qquad (15)$$

  - where the cost should be attributed to risk reduction, and *ΔRisk* is the level of risk reduction as follows:

$$\Delta\ Risk = \textbf{(Risk before mitigation action) – (Risk after mitigation action)} \qquad (16)$$

Risk Management and Control (cont'd)

Cost Effectiveness of Risk Reduction

Risk Treatment and Control (cont'd)

- Risk Comparisons

Ways to Identify Risk of Death	Summary
Number of Fatalities	**This measure shows the impact in terms of the number of fatalities on society. Comparison of these values is cautioned since the number of persons exposed to the particular risk may vary. Also, the time spent performing the activity may vary. Different risk category types should also be considered to compare fatality rates.**
Annual Mortality Rate/Individual	**This measure shows the mortality risk normalized by the exposed population. This measure adds additional information about the number of exposed persons; however, the measure does not include the time spent on the activity.**
Annual Mortality	**This measure provides the most complete risk value since the risk is normalized by the exposed population and the duration of the exposure.**
Loss of Life Exposure (LLE)	**This measure converts a risk into a reduction in the expected life of an individual. It provides a good means of communicating risks beyond probability values.**
Odds	**This measure is a layman format for communicating probability, for example, 1 in 4.**

Risk Treatment and Control (cont'd)

- Rankings Based on Risk Results
  - Another tool for risk management is the development of risk ranking
  - The elements of a system within the objective of analysis can be analyzed for risk and then ranked
  - This relative ranking may be based on the failure probabilities, failure consequences, risks, or other alternatives with concern towards risk

Risk Treatment and Control (cont'd)

- Rankings Based on Risk Results (cont'd)
  - Generally risk items ranked highly should be given high levels of priority; however, risk management decisions may consider other factors such as costs, benefits and effectiveness of risk reduction measures
  - The risk ranking results may be presented graphically as needed

Risk Treatment and Control (cont'd)

- Decision Analysis
  - Strategy tables (generation of alternatives for bio threats)

Detect	Warn	Protect	Respond
Patrols	Sirens	Containment	Citizens
Ground &Airborne Sensors	Television	Gas Masks	Emergency Medical Teams
Both	Multimedia	Both	National Guard

Risk Treatment and Control (cont'd)

- Decision Analysis

> "Decision Analysis is an analytic and systematic approach to studying decision making"

  - An appropriate decision is one that is based on logic, considers all available data and possible alternatives, and applies the qualitative and quantitative approaches to solve them

Risk Treatment and Control (cont'd)

- Decision Analysis (cont'd)
  - Decision Analysis is a method by which non-transparent situations can be made transparent so that every one knows what to do relative to their objectives
  - In fact, if situation were transparent enough, people probably would not make bad decisions

Risk Treatment and Control (cont'd)

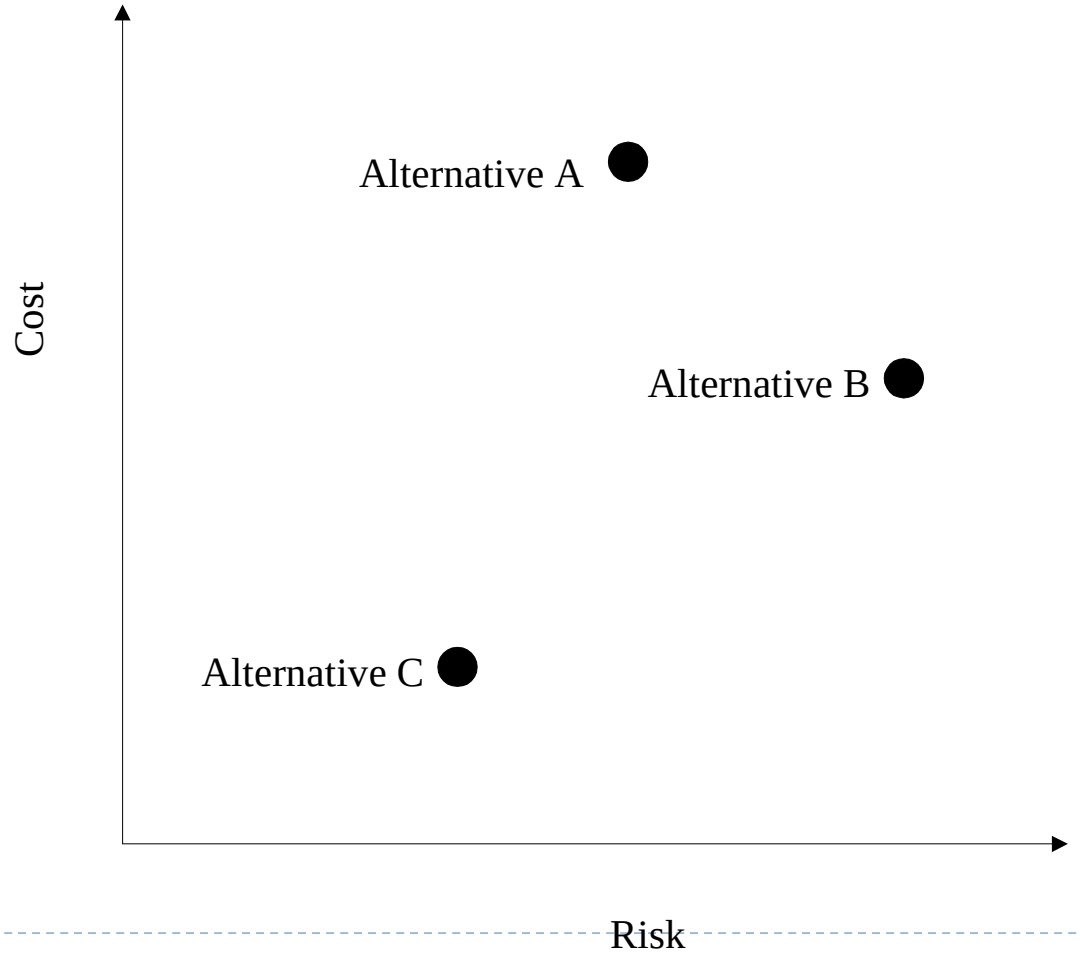
- Decision Analysis (cont'd)
  - Decision making is used to identify decision in three Environment/Cases:
    - Decision-making under certainty
    - Decision-making under uncertainty
    - Decision-making under risk
  - Benefit-cost analysis, decision trees, influence diagrams, utility theory, and the analytical hierarchy process are some of the tools to assist in decision analysis

Risk Treatment and Control (cont'd)

- Cost-Benefit Analysis
  - Risk managers commonly weigh various factors including cost and risk
  - The analysis of three different alternatives is shown graphically in the following figure (next slide) as an example
  - The graph shows that alternative (C) is the best choice since the level of risk and cost is less than alternatives (A) and (B)
  - However, if the only alternatives were A and B, the decision would be more difficult

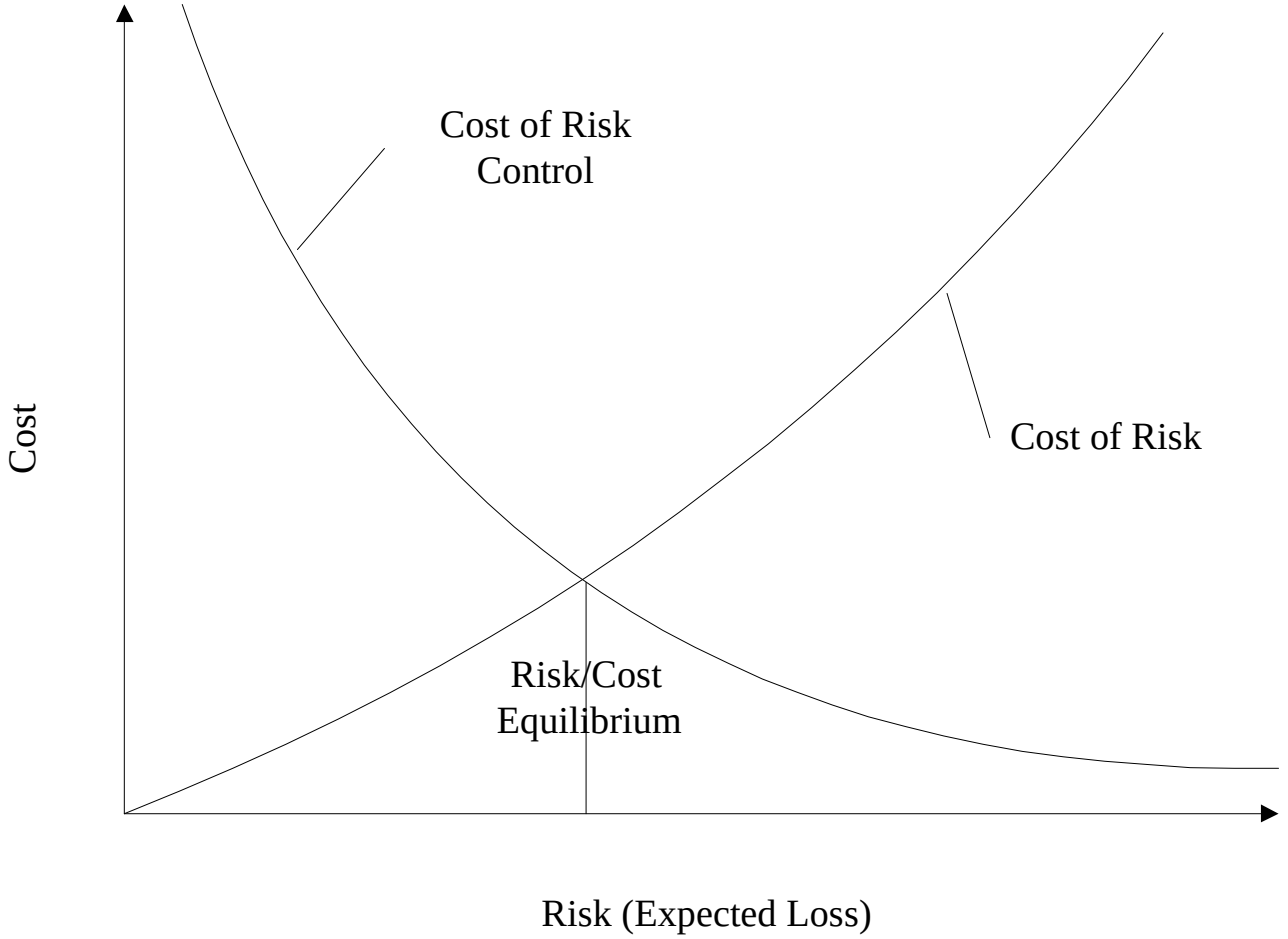
Risk Treatment and Control (cont'd)

Risk Benefit for Three Alternatives



Risk Treatment and Control (cont'd)

Comparison of Risk and Costs



Risk Treatment and Control (cont'd)

- Risk Mitigation
  - Four primary ways are available to deal with risk within the context of a risk management strategy as follows:
    - Risk reduction or elimination
    - Risk transfer, e.g., to a contractor or an insurance company
    - Risk avoidance
    - Risk absorbance or pooling

Risk Treatment and Control (cont'd)

- Risk Mitigation (cont'd)
  - *Risk reduction or elimination* is often the most fruitful approach. For example, could the design of a system be amended so as to reduce or eliminate either the probability of occurrence of a particular risk event or the adverse consequences if they occur?
  - *Risk transfer.* A general principle of an effective risk management strategy is that commercial risks in projects and other business ventures should be borne where-ever possible by the party that is best able to manage them and thus mitigate the risks. Most often, contracts and financial agreements are used to *transfer* risks.

Risk Treatment and Control (cont'd)

- Risk Mitigation (cont'd)
  - *Risk Avoidance.* A most intuitive way of avoiding a risk is not to undertake a project in a such a way that involves that risk
  - *Risk absorbance or pooling*. Cases where risks cannot (economically) be eliminated, transferred, or avoided, they must be absorbed if the project is to proceed. Pooling requires the collaboration of several entities

Risk Treatment and Control (cont'd)

- Example: Cost-Benefit Analysis for Selecting a Transport Method

Alternatives	Cost (in thousands of dollars)	Attributes (Scores 0-100)		
		Punctuality	Safety	Convenience
A1: Air	150	100	70	60
A2: Sea	90	0	60	80
A3: Road and Ferry	40	60	0	100
A4: Rail and Ferry	70	70	100	0
	Weight of Importance	30	60	10

Risk Treatment and Control (cont'd)

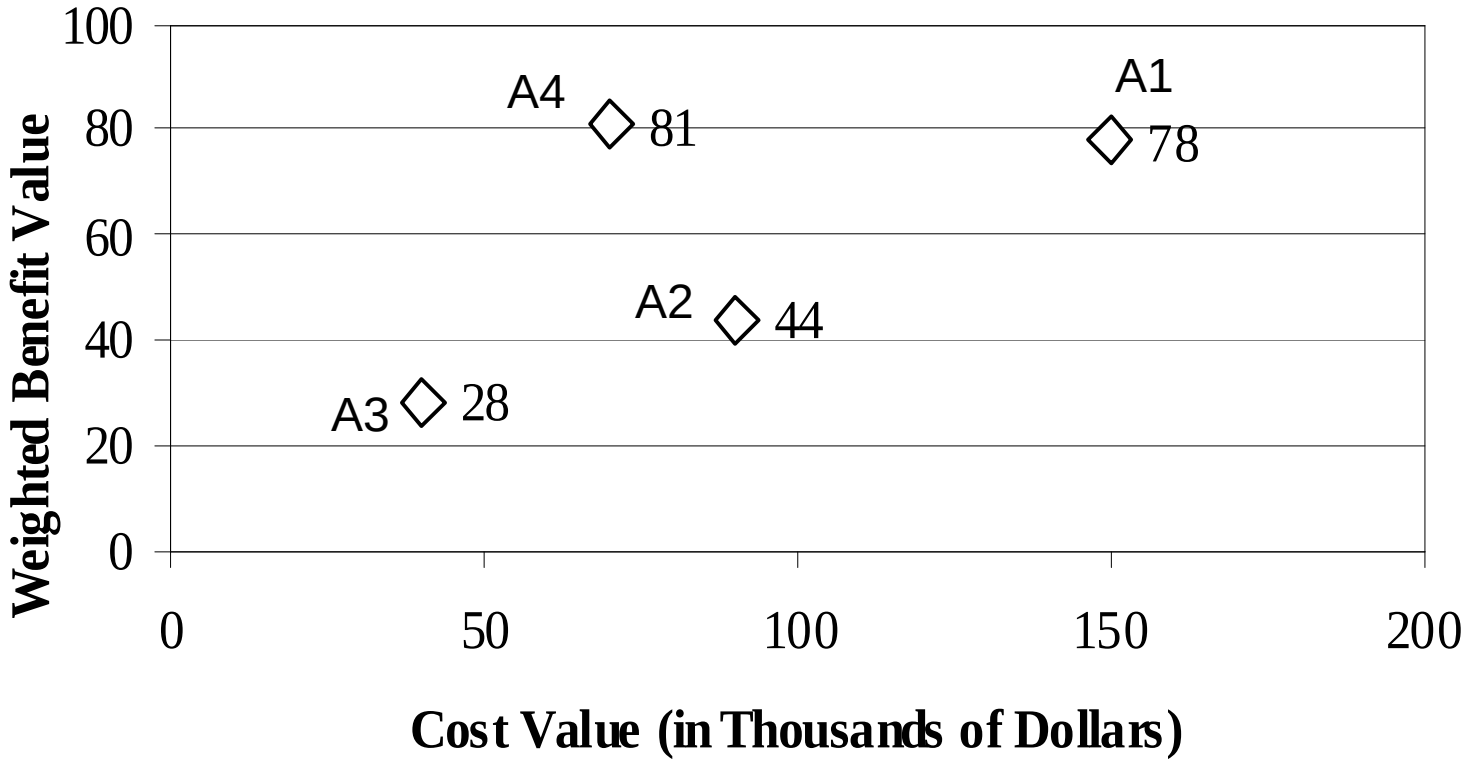
- Example (Cont.): Cost-Benefit Analysis for Selecting a Transport Method

Alternatives		Benefits scores [0-100]					
	Cost (in thousands of dollars)	Punctuality	Safety	Convenience	Weighted Benefit	(Weighted Benefit)/Cost	Rank
A1: Air	150	100	70	60	78	0.52	3
A2: Sea	90	0	60	80	44	0.49	4
A3: Road and Ferry	40	60	0	100	28	0.70	2
A4: Rail and Ferry	70	70	100	0	81	1.16	1
	Weight of Importance	30	60	10	100		
	Normalized Weight	0.3	0.6	0.1	1		

See figure/next page

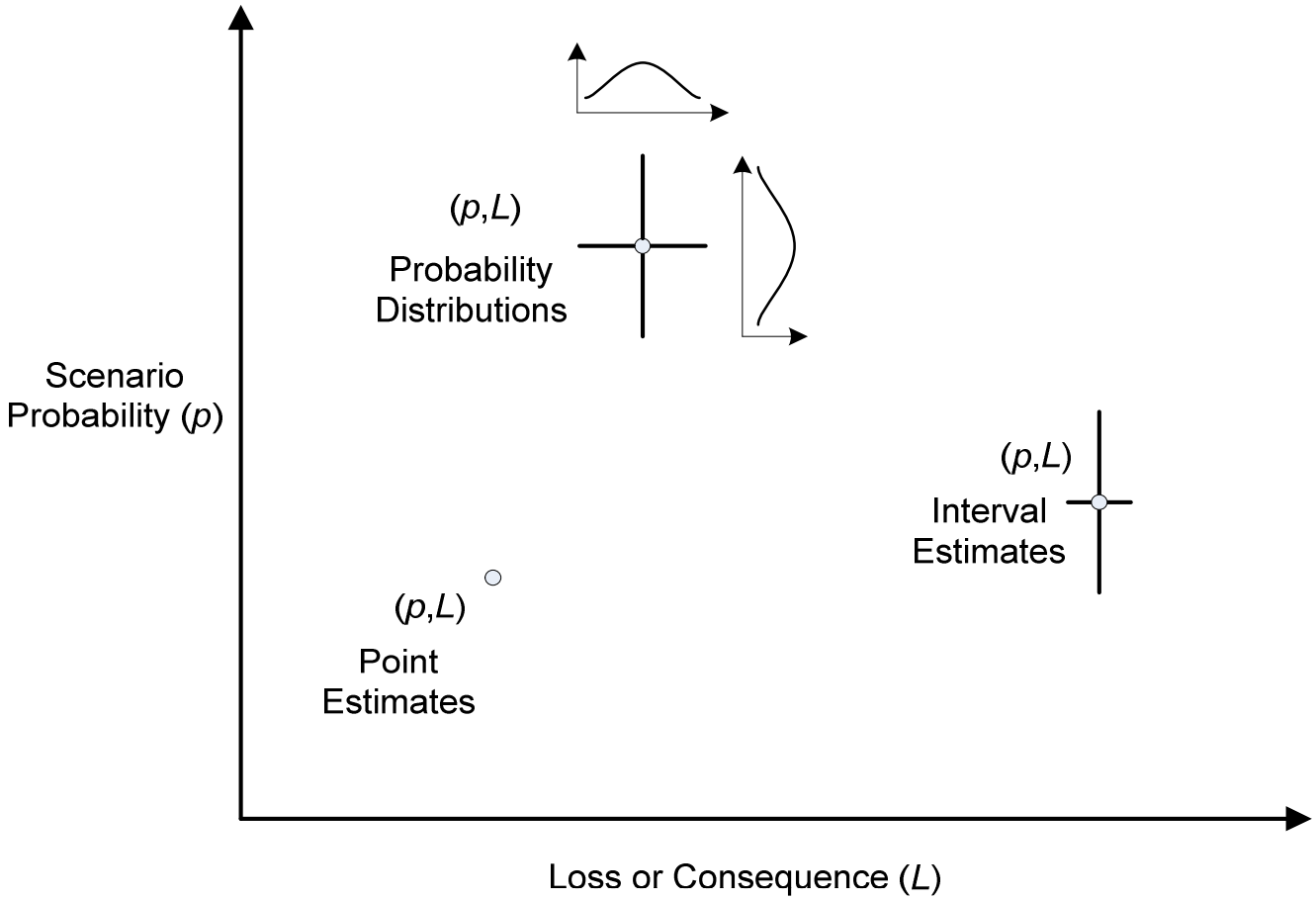
Risk Treatment and Control (cont'd)

- Example: Cost-Benefit Analysis for Selecting a Transport Method



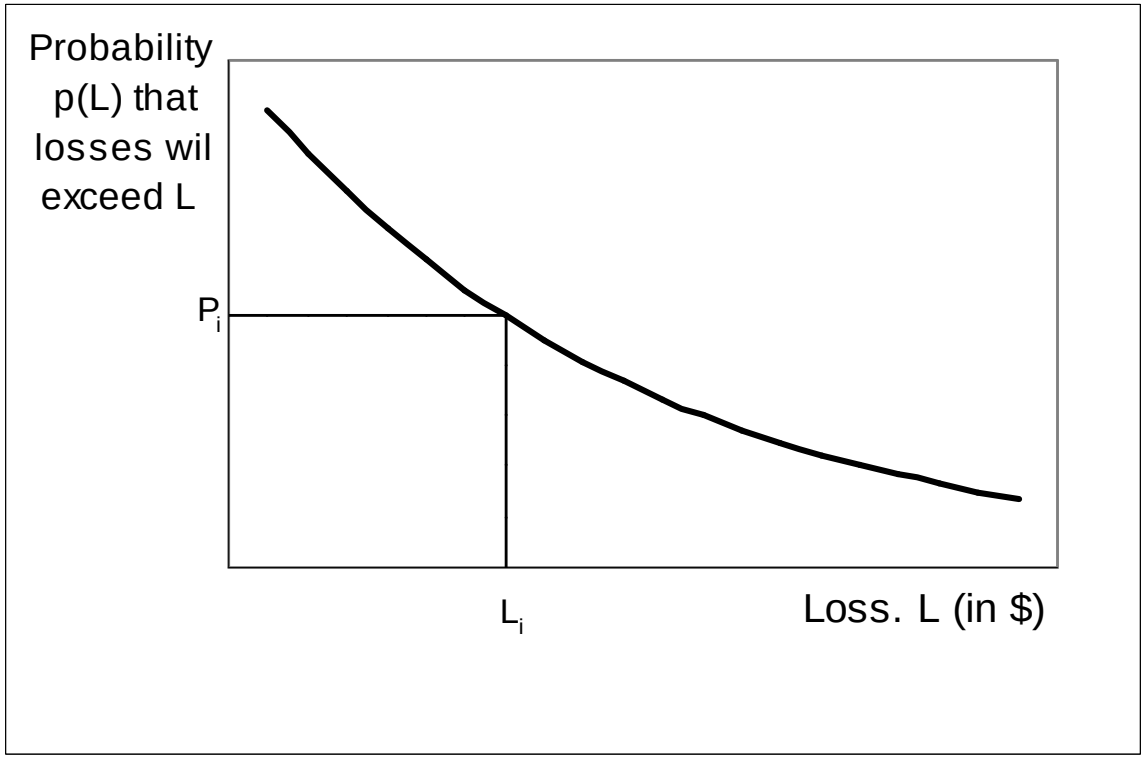
Risk Communication

- Risk representation



Risk Communication

- Risk representation



See example next page

$$EP(L_i) = P(L>L_i) = 1\text{-}P(L\leq L_i)$$

$$= 1 - \prod_{j=1}^{i} (1 - p_j)$$

Risk Communication

- Risk representation

Example: Constructing Exceedence Probability Curves

Event (E_i)	Annual Probability of Occurrence (p_i)	Loss (L_i)	Exceedence Probability ($EP(L_i)$)	$E(L) = (p_i L_i)$
$Event_1$	0.002	25,000,000	0.0020	50,000
$Event_2$	0.005	15,000,000	0.0070	75,000
$Event_3$	0.010	10,000,000	0.0169	100,000
$Event_4$	0.020	5,000,000	0.0366	100,000
$Event_5$	0.030	3,000,000	0.0655	90,000
$Event_6$	0.040	2,000,000	0.1029	80,000
$Event_7$	0.050	1,000,000	0.1477	50,000
$Event_8$	0.050	800,000	0.1903	40,000
$Event_9$	0.050	700,000	0.2308	35,000
$Event_{10}$	0.070	500,000	0.2847	35,000
$Event_{11}$	0.090	500,000	0.3490	45,000
$Event_{12}$	0.100	300,000	0.4141	30,000
$Event_{13}$	0.100	200,000	0.4727	20,000
$Event_{14}$	0.100	100,000	0.5255	10,000
$Event_{15}$	0.283	0	0.6597	0

EP(Li) = 1-(1-0.002)(1-0.005)(1-0.010)=0.0169 ~ 0.002+0.005+0.01

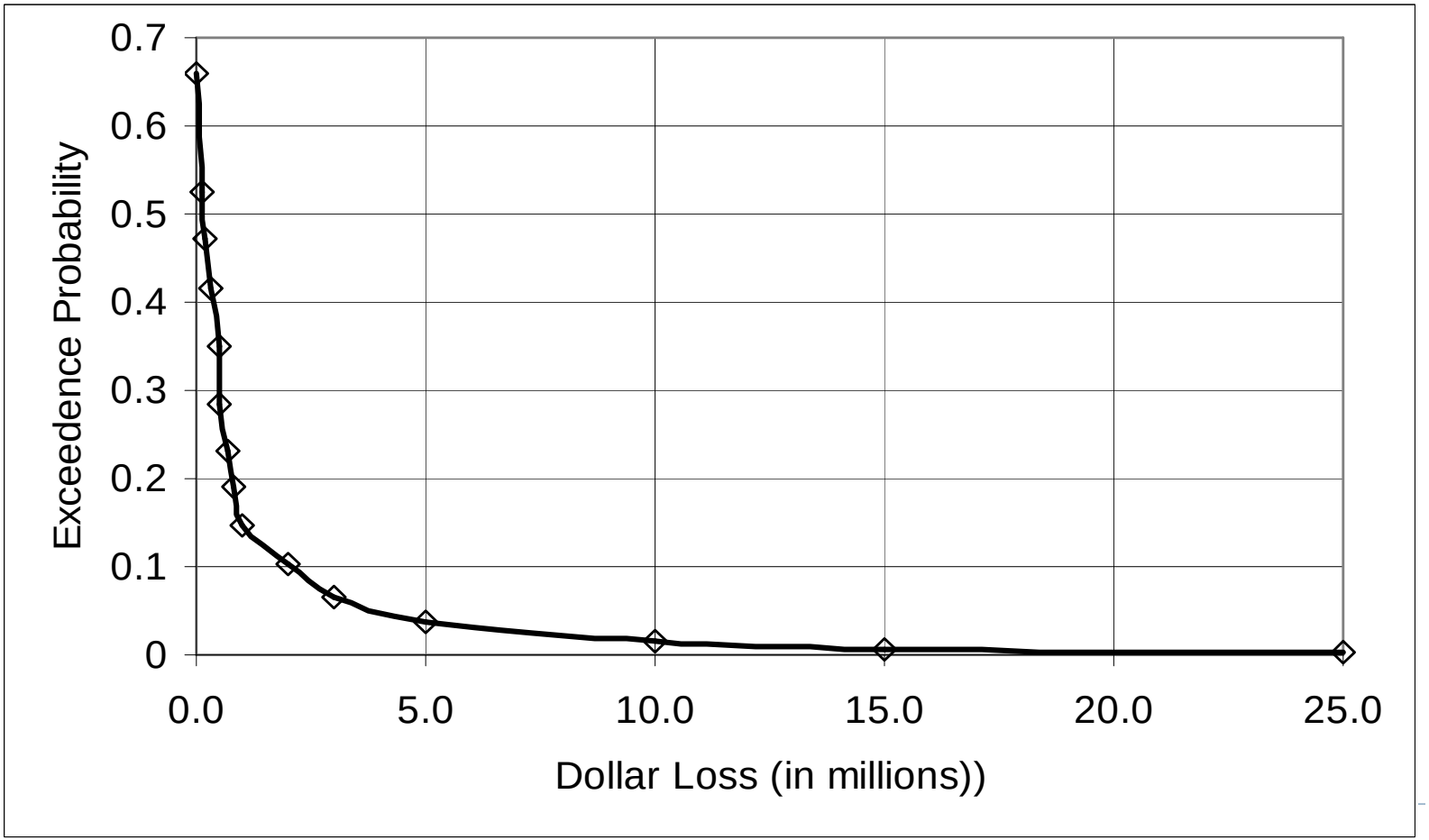
$$EP(L_i) = P(L>L_i) = 1\text{-}P(L\leq L_i)$$

Risk Communication

$$= 1 - \prod_{j=1}^{i} (1 - p_j)$$

- Risk representation

Example: Constructing Exceedence Probability Curves



Risk Communication

- Components of Risk Communication
- A Formula for Effective Risk Communication
  - Until the end of the seventies, it was assumed that once a risk management decision was made it was a matter of public education to inform the public of the final decision. If the decision were made logically, the public would understand and accept it. Numerous unfinished projects, significant problems in siting industrial plants and repeated inability to convince the public have demonstrated that risk communication is a distinct and important part of risk analysis. It requires the same level of understanding and research as the other segments of risk analysis.

Risk Communication (cont'd)

- Components of Risk Communication

The Message
The Source (of the message)
The Channel
The Recipient

Risk Communication (cont'd)

- The Message
  - The public has difficulty in
    - comprehending information expressed in probabilities and that a risk is often considered a reality
    - understanding scientific language
    - legitimate uncertainties by the scientific community that are often considered as a sign of disagreement

Risk Communication (cont'd)

- The Source
  - The public trust in social institutions has been eroded
  - Risk information originating from the government and industry is often considered biased and thus is mistrusted
  - The scientific community has had a limited role in providing relevant information to the public
  - Some scientific (including engineering professional) societies have chosen not to participate in the debate on the risk of various technologies
  - Congress and the media have not taken sufficient advantage of the availability of professional societies which constitute a reliable and often inexpensive resource

Risk Communication (cont'd)

- The Channel
  - The news media is the channel for the dissemination of risk information to the public
  - The news media makes its own independent judgment on what is newsworthy and how it is to be covered
  - One of the major reasons for the emergence of advocacy organizations as a trustworthy source-of information was that they were considered newsworthy and, after some initial mistakes, they learned how to deal with the news media
  - The news media can be bypassed by direct contact with the affected community. However, direct contact with a large community is laborious and expensive

The Web and social networks

Risk Communication (cont'd)

- The Recipient
  - Even if the message is properly prepared, the public trusts the messenger, and the news media chooses the technically correct message and messengers, the recipient of the risk message may misconstrue (or misunderstand) it
  - Contradictions among messages the public has received

Risk Communication (cont'd)

- The US Army Corps of Engineers has a 1992 Engineering Pamphlet (EP) on risk communication (EP 1110-2-8) with considerations in communicating risk:
  - Risk communication must be free of jargon
  - Consensus of experts needs to be established
  - Materials cited, and their sources must be credible
  - Materials must be tailored to audience

Risk Communication (cont'd)

- The information must be personalized to the extent possible
- Motivation discussion should stress a positive approach and the likelihood of success
- Risk data must be presented in a meaningful manner

Risk Communication (cont'd)

- Communication after a severe accident
  - Acknowledge the gravity of the events and the tragedy who have suffered
  - Recognize the public's concerns, emotions, and efforts to manage the risk
  - Assure the audience that the relevant officials are doing all that they can
  - Express a coherent, consistent communication philosophy for all risks

Risk Communication (cont'd)

- Communication after a severe accident
  - Provide quantitative risk estimates, including the uncertainties associated with the estimates
  - Provide summary analyses of possible protective actions considering all the expected effects
  - Lead by example, showing possible models for responsible bravery
  - Commit to earning and keeping the public trust

Risk Communication (cont'd)

- Documentation (ISO 31000)
  - Objectives and scope
  - Description of relevant parts of the system and their functions
  - A summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed
  - Risk criteria applied and their justification
  - Limitations, assumptions and justification of hypotheses

Risk Communication (cont'd)

- Documentation (ISO 31000)
  - Assessment methodology
  - Risk identification results
  - Data, assumptions and validation
  - Risk analysis results and their evaluation
  - Sensitivity and uncertainty analysis
  - Critical assumptions
  - Discussion of results
  - Conclusions and recommendations
  - References

Limitations and Pitfalls

- Confusion regarding the concept of risk
- Completely unavoidable human errors in subjective judgment of risk
- Entirely ineffectual but popular subjective scoring methods
- Misconceptions that block the use of better, existing methods
- Recurring errors in even the most sophisticated methods
- Institutional factors
- Unproductive incentive structure

Homework Assignments and Project

HW #2:

2.6

2.31

2.48

2.58

2.63