PROBABILISTIC RISK ASSESSMENT & MANAGEMENT

TOOLS, TECHNIQUES AND APPLICATIONS

LECTURE OUTLINE

1. Basic Definitions
2. Risk Assessment
   - Categories of Risk Analysis
   - Types of Risk Assessment
   - Elements of Risk Assessment
   - Probabilistic Risk Assessment
   - Strength of PRA
3. Risk management
   - Cost-Benefit Analysis
   - Decision Making Techniques Using Risk Information

DEFINITION OF RISK

- Consequences of human or natural actions result in losses and gains.
- Risk implies something unwanted or to be avoided.
- One takes risk for possible gains.
- Questions: "does the ***gain*** outweighs the ***risk***"?
- If we only associate risk with losses (not gains) then one can say that we are risk averse, i.e., we only control and reduce our risks (Note that actions taken to reduce a risk can be considered gain in the sense that possible losses are reduced.)
- Risk has two components

  (1) Unwanted consequence (or loss) expressed in magnitude

  (2) Uncertainty in the occurrence of that loss (expressed in probability or frequency)

DEFINITION OF RISK

- Risk is a measure of the
  - potential loss occurred due to natural or human activities.
  - Potential losses are the adverse consequences of such activities in form of loss of human life, adverse health effects, loss of property, and damage to the natural environment.
- Risk analysis is the process of
  - characterizing,
  - managing and
  - informing others about existence, nature, magnitude, prevalence, contributing factors, and uncertainties of the potential losses.
- From an engineering point of view, the risk or potential loss is associated with exposure of the recipients to hazards, and can be expressed as a combination of the *probability* or *frequency*

- the loss may be external to the system, caused by the system to one or more recipients (e.g., human, organization, economic assets, and environment).
- Also the loss may be internal to the system, only damaging the system itself. An engineering system is defined as an entity composed of hardware, software and human organization.

DEMAND FOR RISK ANALYSIS

- Morgan argue that we worry more about risk today exactly because we have more to lose and we have more disposable income to spend on risk reduction.

- A mechanism to control and avert risk has been to regulate manufacturing, operation and construction of complex systems.

- The conventional view of safety risk regulation is that the existence of risks is undesirable and, with appropriate technological interventions, we can eliminate those risks. However, this perspective does not recognize the risk reduction costs involved; the fact that a no-risk society would be so costly and infeasible.

- Risk analysis and especially Probabilistic Risk Assessment (PRA) can play pivotal roles in making design, manufacturing, operation, policy and regulatory decisions. Progress in the field of risk analysis and especially in PRA has been enormous.

CATEGORIES OF RISK ANALYSIS

- Health risk analysis

  Estimating potential diseases and losses of life affecting humans, animals and plants

- Safety risk analysis

  Estimating potential harms caused by accidents occurring due to natural events (climatic conditions, earthquakes, brush fires, etc.) or human-made products, technologies and systems (i.e., aircraft crashes, chemical plant explosions, nuclear plant accidents, technology obsolescence or failure);

- Security risk analysis

  Estimating access and harm caused due to war, terrorism, riot, crime (vandalism, theft, etc.) and misappropriation of information (national security information, intellectual property)

- Financial risk analysis

  Estimating potential individual, institutional and societal monetary losses such as currency fluctuations, interest rates, share market, project losses, bankruptcy, market loss, misappropriation of funds, and property damage;

- Environmental risk analysis

  estimating losses due to noise, contamination, and pollution in ecosystem (water, land, air and atmosphere) and in space (space debris)

TYPES OF RISK ANALYSIS

Risk analysis attempts to measure the magnitude of a loss (consequences) associated with complex systems, including evaluation, risk reduction and control policies. Generally there are three types of risk analysis:

- ✓Quantitative
- ✓Qualitative
- ✓A Mix of the two

ELEMENTS OF RISK ANALYSIS

Risk assessment is the process through which the chance or frequency of a loss and the magnitude of the loss (consequence) is measured or estimated.

Risk management is the process through which the potential (likelihood or frequency) of magnitude and contributors to risk are estimated, evaluated, minimized, and controlled.

Risk communication is the process through which information about the nature of risk (expected loss) and consequences, risk assessment approach and risk management options are exchanged, shared and discussed between the decision makers and other stakeholders.

RISK ASSESSMENT

- Risk assessment is the process of providing answer to four basic questions:

  1. What can go wrong?
  2. How likely is it?
  3. What are the losses (consequences)?

- Answering these questions could be simple or require a significant amount of analysis and modeling.

QUANTITATIVE DEFINITION OF RISK

Answers to:

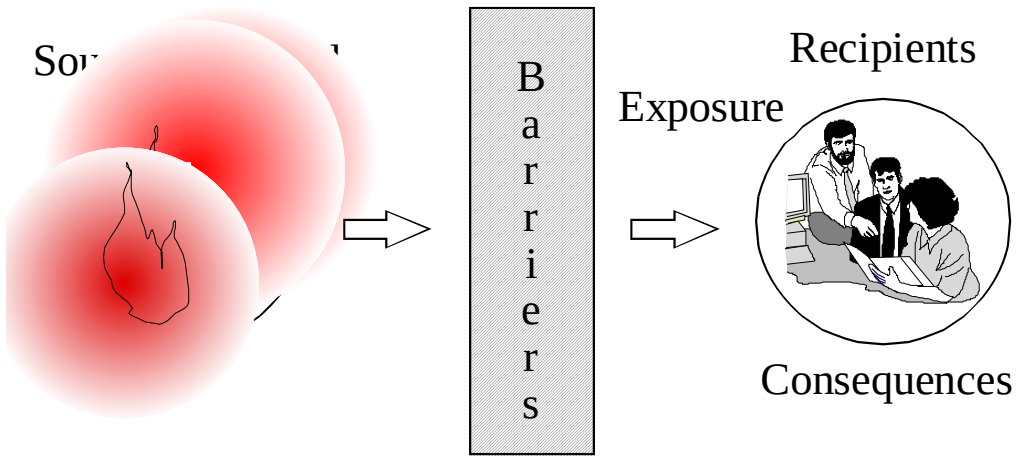
(1) What can go wrong?
(2) What is the likelihood?
(3) What is the damage (loss or consequence)?

Scenario	Likelihood	Damage
S_1	l_1	X_1
S_2	l_2	X_2
S_3	l_3	X_3
⋮	⋮	⋮
S_N	l_N	X_N

$$R = \text{RISK} = \{\langle S_1, l_1, X_1 \rangle\}$$

Risk "is" a set of triplets

Risk Assessment Concept



1. IDENTIFICATION OF HAZARDS

- Chemical (e.g., toxins, corrosive agents, smoke)
- Biological (e.g., viruses, microbial agents, bio-contaminants)
- Thermal (e.g., explosions, fire)
- Mechanical (e.g., impact from a moving object, explosions)
- Electrical (e.g., electromagnetic fields, electric shock)
- Ionizing radiation (e.g., x-rays, gamma rays)
- Nonionizing radiation (e.g., microwave radiation, cosmic rays)
- Information (e.g., propaganda, computer virus)

2. IDENTIFICATION OF CHALLENGERS TO BARRIERS

- Barrier strength or endurance degrades because of:
  - reduced thickness (due to deformation, erosion, corrosion, ware, etc.),
  - changes in material properties (e.g., fracture toughness, yield strength).
- Stress or Damage on the barrier increases by:
  - internal agents such as forces or pressure,
  - penetration or distortion by external objects or forces.

2. IDENTIFICATION OF CHALLENGERS TO BARRIERS (CONT)

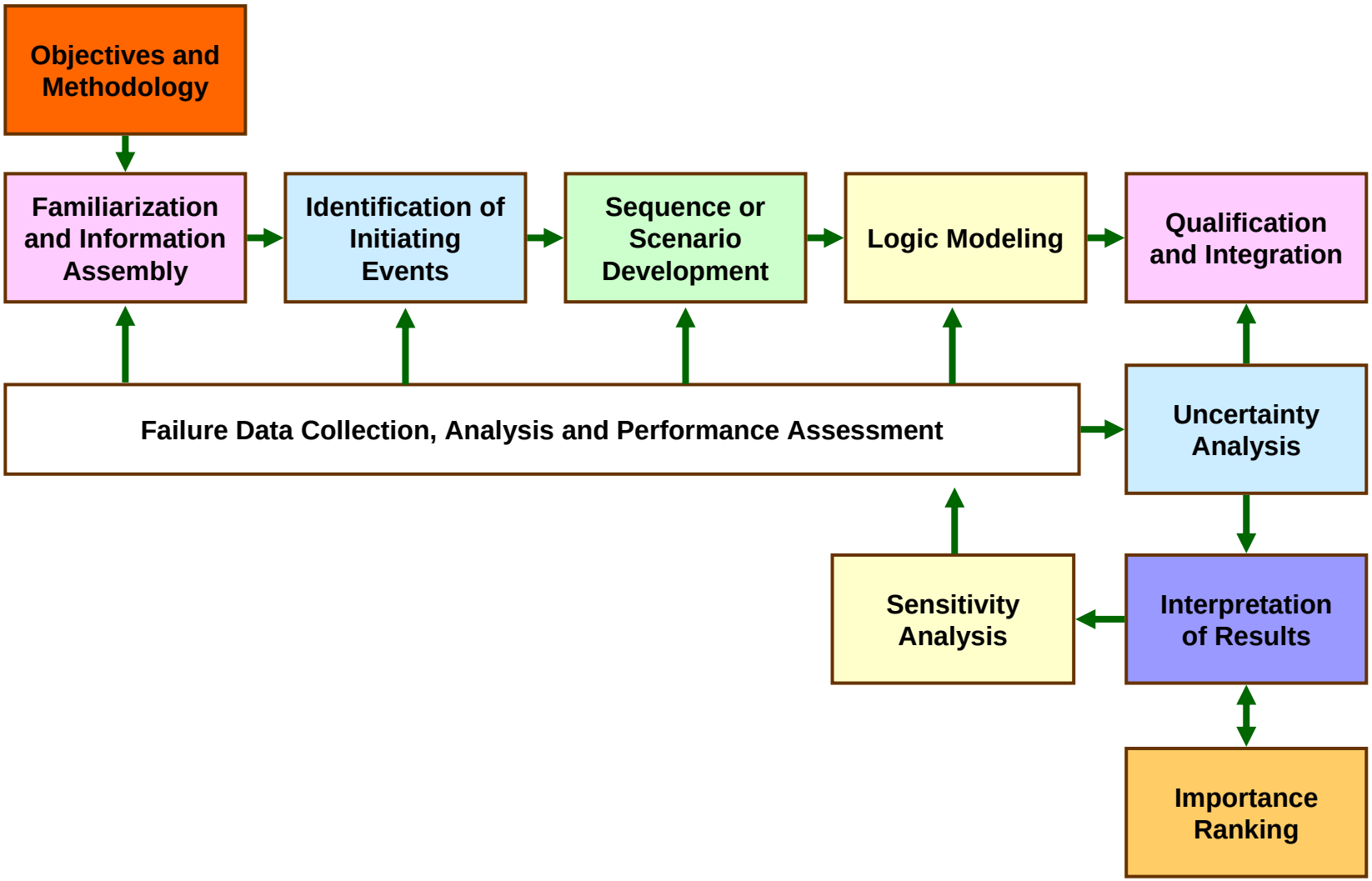
Above examples of causes of system degradation are often the results of one or more of the following conditions:

- Malfunction of process equipment (e.g., the emergency cooling system in a nuclear power plant)
- Problems with human-machine interface
- Poor design and maintenance
- Adverse natural phenomena
- Adverse human-made environments.

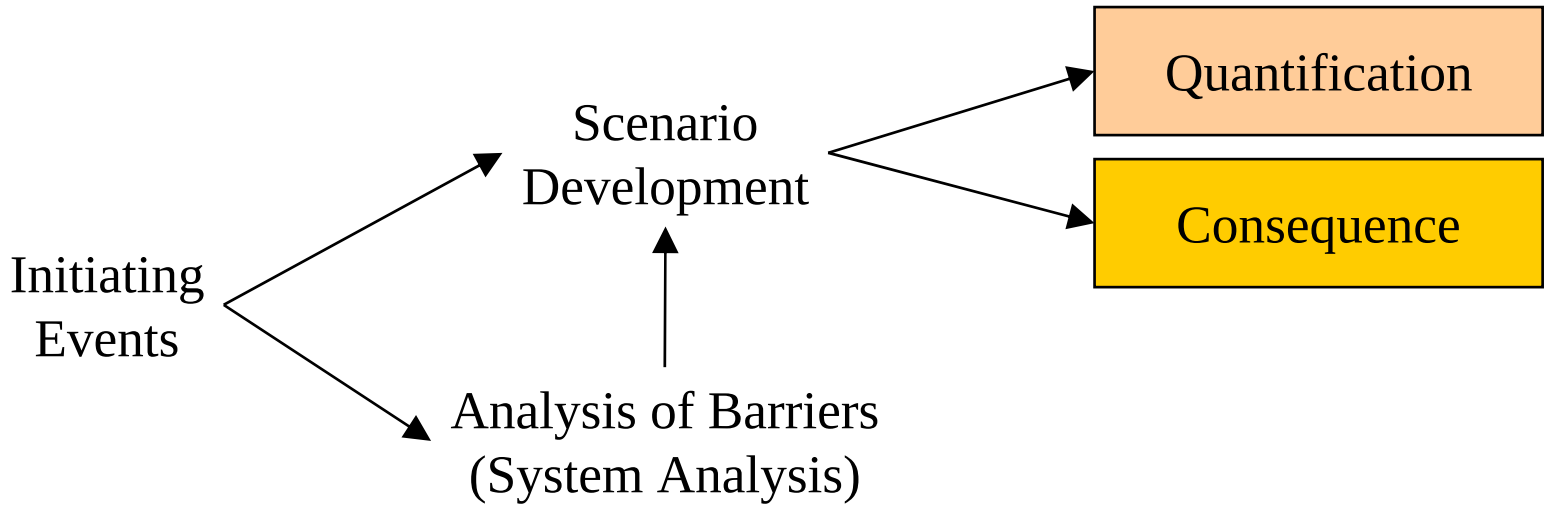
4. Estimation of Frequency or Probability of a Hazard Exposure

5. Consequences Evaluation

COMPONENTS OF THE OVERALL PRA PROCESS



PROBABILISTIC RISK ASSESSMENT (PRA)



FAMILIARIZATION AND INFORMATION ASSEMBLY

The following items should be performed in this step:

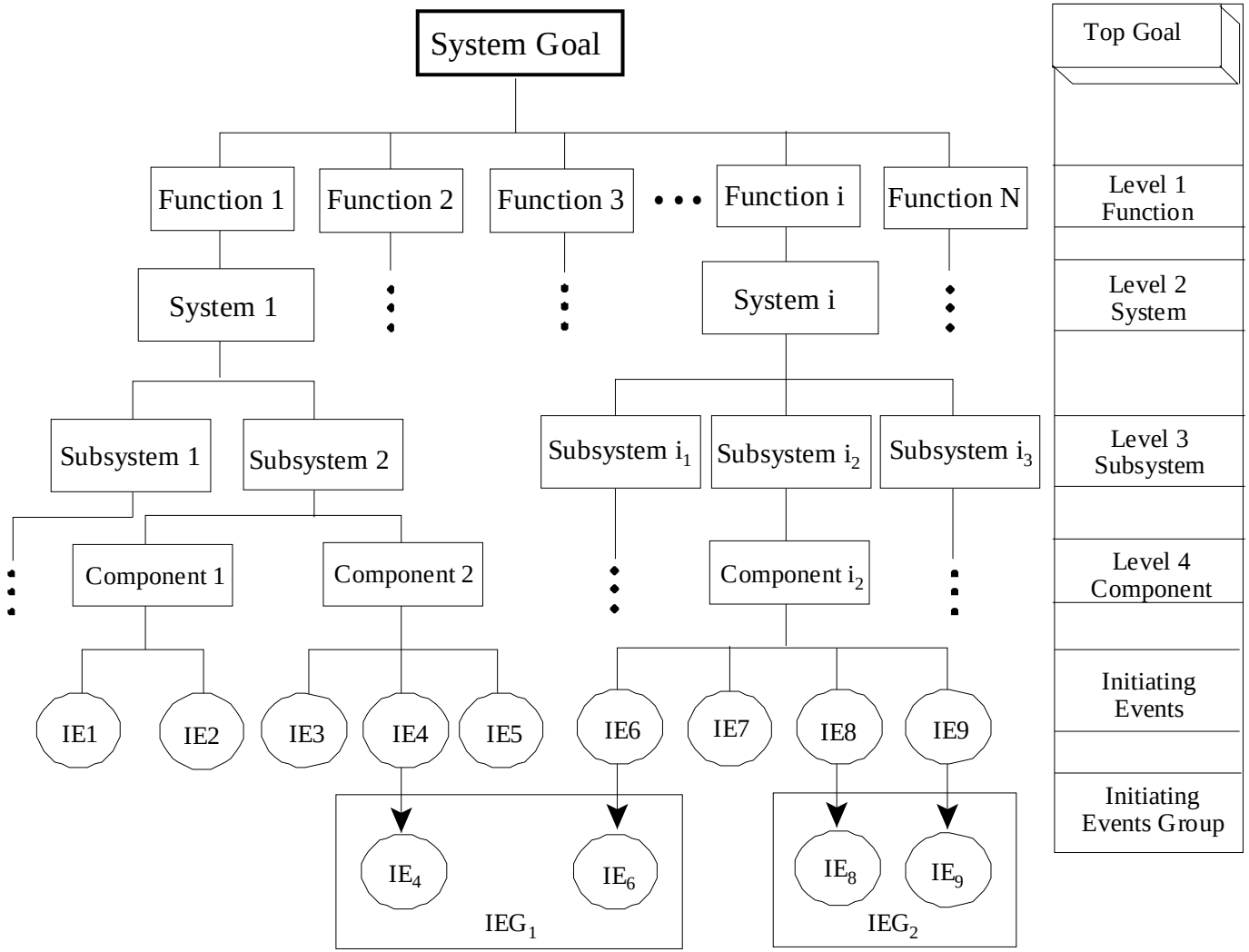
1. Major critical barriers, structures, emergency safety systems, and human interventions should be identified.
2. Physical interactions among all major subsystems (or parts of the system) should be identified and explicitly described. The result should be summarized in a dependency matrix.
3. Past major failures and abnormal events that have been observed in the facility should be noted and studied. Such information would help ensure inclusion of important applicable scenarios.
4. Consistent documentation is key to ensuring the quality of the PRA. Therefore, a good filing system must be created at the outset, and maintained throughout the study.

INITIATING EVENTS
(INTERNAL EVENTS INTERNAL TO THE PROCESS)

The following inductive procedures should be followed when grouping initiating events:

1. Combine the initiating events that directly break all hazard barriers.
2. Combine the initiating events that break the same hazard barriers (not necessarily all the barriers).
3. Combine the initiating events that require the same group of mitigating human or automatic actions following their occurrence.
4. Combine the initiating events that simultaneously disable the normal operation as well as some of the available mitigating human, software or automatic actions.

FUNCTION SYSTEM SUBSYSTEM INITIATING EVENT RELATIONSHIP



INITIATING EVENTS
(INTERNAL EVENTS INTERNAL TO THE PROCESS)

The following procedures should be followed in this step of the PRA:

1. Select a method for identifying specific operational and non-operational initiating events. Two representative methods are functional hierarchy and FMEA. If a generic list of initiating events is available, it can be used as a supplement.
2. Using the method selected, identify a set of initiating events.
3. Group the initiating events having the same effect on the system, for example those requiring the same mitigating functions to prevent hazard exposure are grouped together

SEQUENCE OR SCENARIO DEVELOPMENT

The following procedures should be followed in this step of the PRA:

1. Identify the mitigating functions for each initiating event (or group of events).
2. Identify the corresponding human actions, systems or hardware operations associated with each function, along with their necessary conditions for success.
3. Develop a functional event tree for each initiating event (or group of events).
4. Develop a systemic event tree for each initiating event, delineating the success conditions, initiating event progression phenomena, and end effect of each scenario.

LOGIC MODELING

The following procedures should be followed in this step of the PRA:

1. Develop a fault tree for each event in the event tree heading for which actual historical failure data does not exist.
2. Explicitly model dependencies of a subsystem on other subsystems and intercomponent dependencies (e.g., common cause failures that are described in Chapter 4).
3. Include all potential reasonable and probabilistically quantifiable causes of failure, such as hardware, software, test and maintenance, and human errors, in the fault tree.

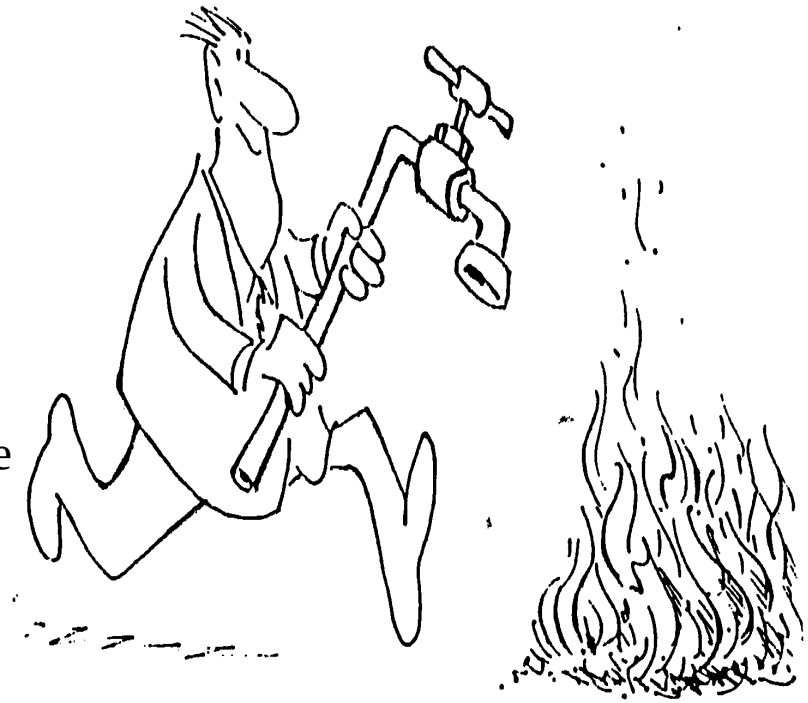
TREATMENT OF DEPENDENCIES

The following procedures should be followed in this step of the PRA:

1. Identify the hardware, software and human elements that are similar and could cause dependent or common cause failures. For example, similar pumps, motor-operated valves, air-operated valves, human actions, software routine, diesel generators, and batteries are major components in process plants, and are considered important sources of common cause failures.
2. Items that are potentially susceptible to common cause failure should be explicitly incorporated into the corresponding fault trees and event trees of the PRA where applicable.
3. Functional dependencies should be identified and explicitly modeled in the fault trees and event trees.

THE HUMAN ELEMENT

- **Nuclear** (Maintenance Error, Control Room Crew Error)
- **Aviation** (Maintenance Error, Flight Crew Error, Air Traffic Controller Error)
- **Chemical and Process** (Maintenance Errors)
- **Land and Sea Transportation** (Maintenance and Operator Errors)
- **Healthcare Industries** (Procedural Error, Operator Error)
- **Telecommunication** (Procedural Errors)



FAILURE DATA COLLECTION, ANALYSIS, AND PERFORMANCE ASSESSMENT

The following procedures should be followed in this step of the PRA:

1. Determine generic values of material strength or endurance, load or damage agents, failure times, failure occurrence rate and failures on demand for each item (hardware, human action, or software) identified in the PRA models. This can be obtained either from facility-specific or system-specific experiences, from generic sources of data, or both (see Chapter 4 for more details on this subject)
2. Gather data on hazard barrier tests, repair, and maintenance data primarily from experience, if available. Otherwise use generic performance data.
3. Assess the frequency of initiating events and other probability of failure events from experience, expert judgment, or generic sources. (See Chapter 4).
4. Determine the dependent or common cause failure probability for similar items, primarily from generic values. However, when significant specific data are available, they should be primarily used (see Chapter 4.)

QUANTIFICATION AND INTEGRATION

The following procedures should be followed as part of the quantification and integration step in the PRA:

1. Merge corresponding fault trees associated with each failure or success event modeled in the event tree scenarios (i.e., combine them in a Boolean form). Develop a reduced Boolean function for each scenario (i.e., truncated minimal cut sets).
2. Calculate the total frequency of each sequence, using the frequency of initiating events, the probability of barrier failure including contributions from test and maintenance frequency (outage), common cause failure probability, and human error probability.
3. Use the minimal cut sets of each sequence for the quantification process. If needed, simplify the process by truncating based on the cut sets or probability.
4. Calculate the total frequency of each scenario.
5. Calculate the total frequency of all scenarios of all event trees.

UNCERTAINTY ANALYSIS

Steps in uncertainty analysis include:

1. Identify models and parameters that are uncertain and the method of uncertainty estimation to be used for each.
2. Describe the scope of the PRA and
3. Estimate and assign probability distributions depicting model and parameter uncertainties in the PRA.
4. Propagate uncertainties associated with the hazard barrier models and parameters to find the uncertainty associated with the risk value.
5. Present the uncertainties associated with risks and contributors to risk in an easy way to understand and visually straightforward to grasp.

RISK RANKING AND IMPORTANCE ANALYSIS

Applications of importance measures may be categorized into the following areas:

1. (Re)Design: To support decisions of the system design or redesign by adding or removing elements (barriers, subsystems, human interactions, etc.)
2. Test and Maintenance: To Address questions related to the plant performance by changing the test and maintenance strategy for a given design.
3. Configuration and Control: To measure the significance or the effect of failure of a component on risk or safety or temporarily taking a component out of service.
4. Reduce uncertainties in the input variables of the PRAs.

RISK RANKING AND IMPORTANCE ANALYSIS

The following are the major steps of importance ranking:

1. Determine the purpose of the ranking and select appropriate ranking importance measure that has consistent interpretation for the use of the ranked results.
2. Perform risk ranking and uncertainty ranking, as needed.
3. Identify the most critical and important elements of the system with respect to the total risk values and total uncertainty associated with the calculated risk values.

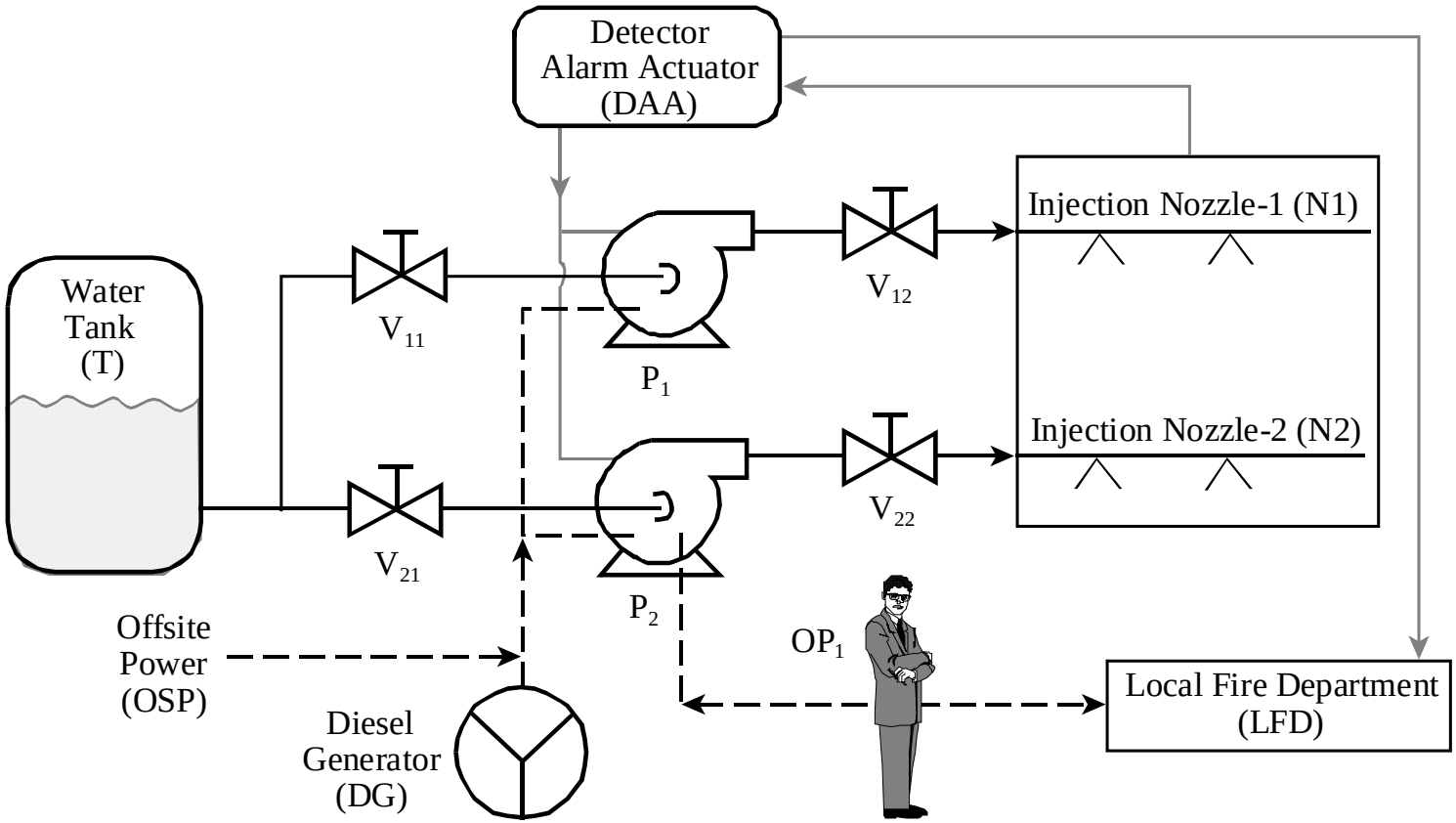
STRENGTH OF PRA

The most important strengths of the PRA, as the formal engineering approach to risk assessment are:

1. Provides an integrated and systematic examination of a broad set of design and operational features of an engineered system.
2. Incorporates the influence of system interactions and human-system interfaces.
3. Provides a model for incorporating operating experience with the engineered system and updating risk estimates.
4. Provides a process for the explicit consideration of uncertainties.
5. Permits the analysis of competing risks (e.g., of one system vs. another or of possible modifications to an existing system).
6. Permits the analysis of (assumptions, data) issues via sensitivity studies.
7. Provides a measure of the absolute or relative importance of systems, components to the calculated risk value.
8. Provides a quantitative measure of overall level of health and safety for the engineered system.

A SIMPLE EXAMPLE OF PRA

Risk Assessment of Fire Protection System



Example of PRA: Steps

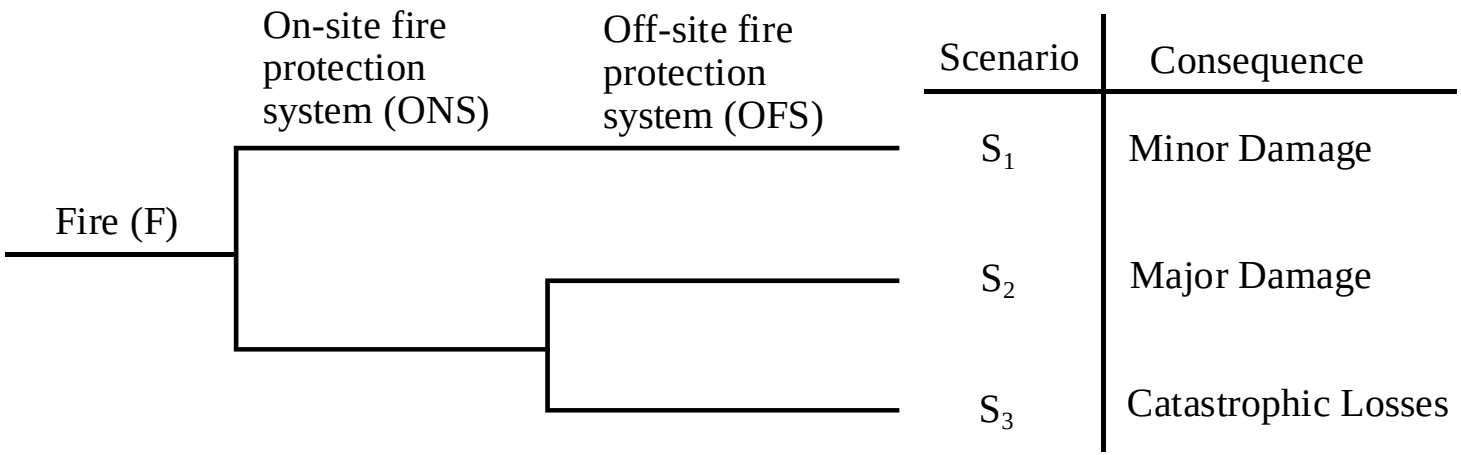
- Identification of Initiating Events
- Scenario Development
- Logic Modeling
- Failure Data Analysis
- Quantification
- Consequences
- Risk Value Calculation and Evaluation

EXAMPLE OF PRA (cont)

Initiating Events

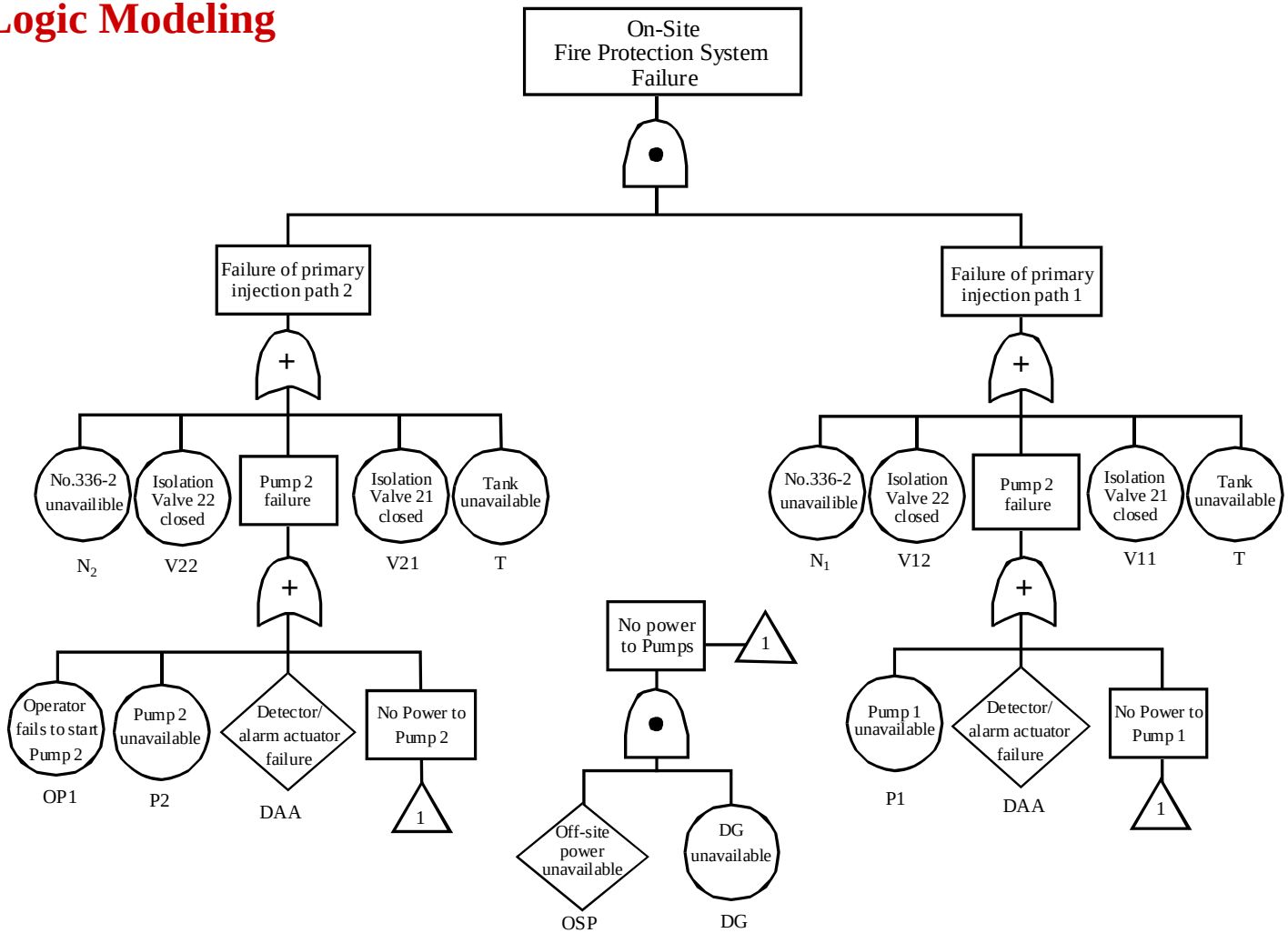
– Fire in Plant

Scenario Development



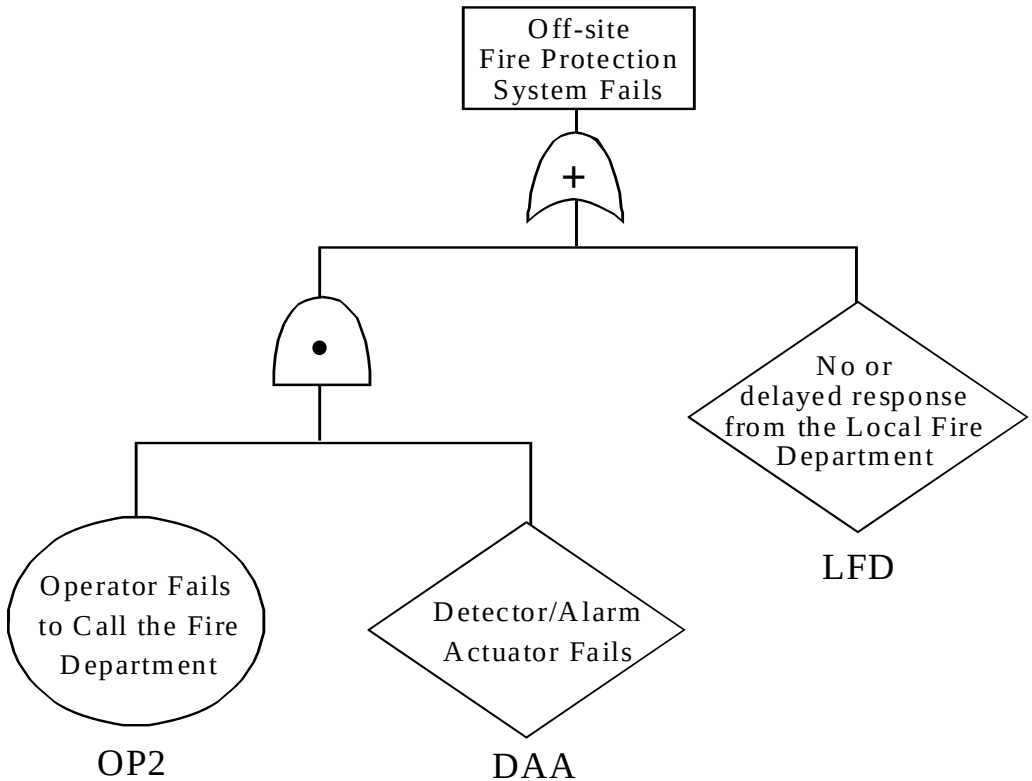
EXAMPLE OF PRA (cont)

Logic Modeling



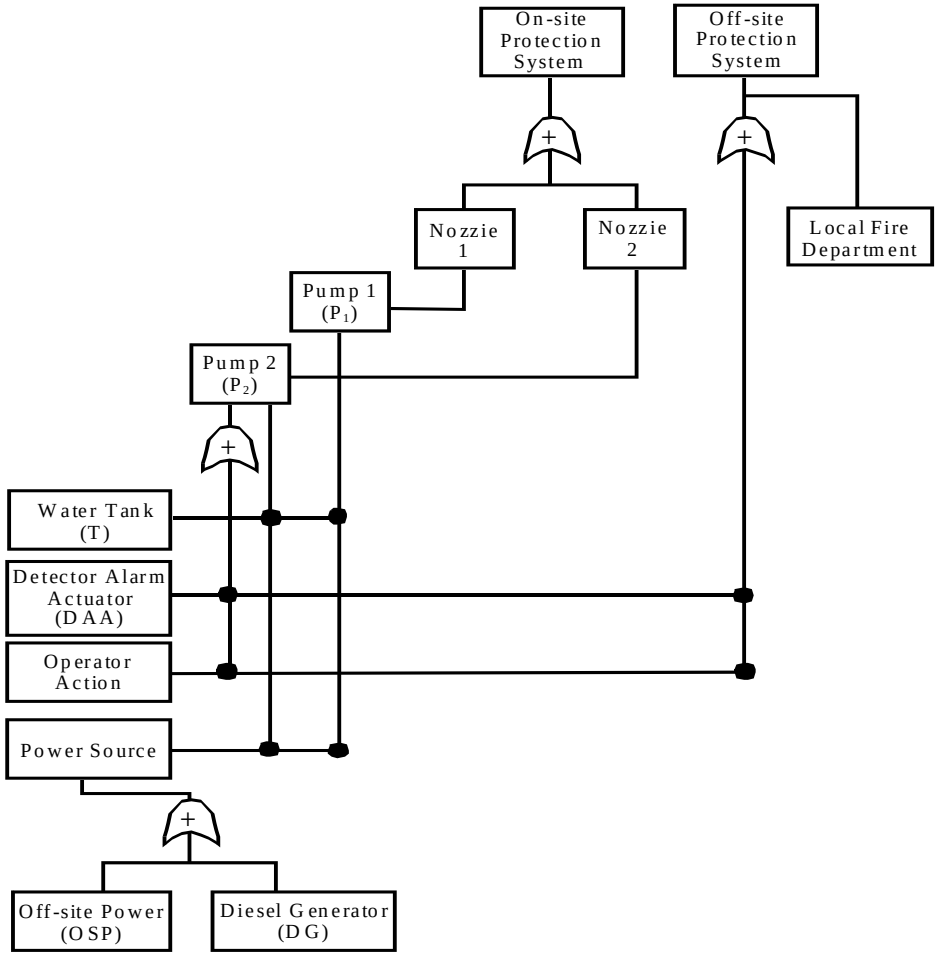
EXAMPLE OF PRA (cont)

Logic Modeling



A SIMPLE EXAMPLE OF PRA (cont)

Logic Modeling



EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Fire initiation frequency	No such experience in 10 years of operation.	5 fires in similar plants. There are 70,000 plant-years of experience.	F = 5/70,000 = 7.1E-4/yr.	Use generic data.
Pump 1 and Pump 2 failure	4 failures of two pumps to start per year each having an average of 10 demands (tests) per month. Repair time takes about 2.5 hours. No experience of failure to run.	Failure to run = 1×10^{-5} hr^{-1}.	$\frac{4}{2(12)(10)} = 1.7\times10^{-2}$/demand Unavailability $= 1.7\times10^{-2} + \frac{2.5(4)}{8760}$ $= 1.8\times10^{-2}$/demand $P_1 = P_2 = 1.8\times10^{-2}$	Failure to start is facility-specific. For failure to run is generic.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Common cause failure between Pump 1 and Pump 2	No such experience	Using the β-factor method, β = 0.1 for failure of pumps to start.	Unavailability due to common cause failure: $CCF = 0.1 \times 1.8 \times 10^{-2}$ $= 1.8 \times 10^{-3}/\text{demand}$	Assume no significant common cause failure exists between valves and nozzles.
Failure of isolation valves	2 failure to leave the valve in open position following 10 pump tests in one year.	Not used.	$v_{11} = v_{12} = v_{21} = v_{22}$ $= \frac{2}{10(12)(4)}$ $= 4.2 \times 10^{-3}/\text{demand}$	Facility-specific data used.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Failure of nozzles	No-such experience	1×10^{-5}/demand	$N_1 = N_2$ $= 1.0\times10^{-5}$/demand	Generic data used.
Diesel generator failure	3 failures in tests. 40 hours of repair per year.	3.0×10^{-2}/demand 3.0×10^{-3}/hr 40 run	failure on demand $= \frac{3}{12(10)}$ failure on demand = 2.5×10^{-2}/demand failure on run = 3.0×10^{-3}/hr Total failure of DG $= 2.5\times10^{-2} + 3.0\times10^{-3}$ $= 5.5\times10^{-2}$	Facility-specific data used for demand failure.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Loss of off-site power	No experience.	0.1/yr.	$\text{OSP} = 0.1 \times \frac{10}{8760} = 1.1 \times 10^{-4}/\text{demand}$	Assume 104 hours of operation for fire extinguisher and use generic data.
Failure of DAA	No Experience.	No data available.	DAA = 1×10^{-4}/demand.	This estimate is based on expert judgment.

EXAMPLE OF PRA (cont)

(Sources of Data and Failure Probabilities)

Failure Data Analysis

Failure Event	Plant-Specific Experience	Generic Data	Probability Used	Comments
Failure of operator to start Pump 2	No such experience	Using the THERP method	OP1 = 1×10^{-2}/demand	The method is discussed in Chapter 4
Failure of opera-tor to call the fire department	No such experience	1×10^{-3}	OP2 = 1×10^{-3}/demand	This is based on experience from no response to similar situations. Generic probability is used.
No or delayed response from fire department	No such experience	1×10^{-4}	LFD = 1×10^{-4}/demand	This is based on response to similar cases from the fire department. Delayed/no arrival is due to accidents, traffic, communication problems, etc.
Tank failure	No such experience	1×10^{-5}	T = 1×10^{-5}/demand	This is based on date obtained from rupture of the tank or insufficient water content.

EXAMPLE OF PRA (cont)

Quantification

These steps are described below:

1. The cut sets of the On-Site Fire Protection System Failure are obtained using the technique described in the section on Strength of PRA. These cut sets are listed in Table below.

Cut Sets of the On-Site Fire Protection System Failure

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
1	T	1.0×10^{-5} (0.35)
2	DAA	1.0×10^{-4} (3.5)
3	OSP · DG	6.0×10^{-6} (0.21)
4	$N_2 \cdot N_1$	1.0×10^{-10} (~ 0)
5	$N_2 \cdot V_{12}$	4.2×10^{-8} (~ 0)
6	$N_2 \cdot P_1$	1.7×10^{-7} (~ 0)

EXAMPLE OF PRA (cont)

Cut Sets of the On-Site Fire Protection System Failure (cont)

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
7	$N_2 \cdot V_{11}$	4.2×10^{-8} (~ 0)
8	$V_{22} \cdot N_1$	4.2×10^{-8} (~ 0)
9	$V_{22} \cdot V_{12}$	1.8×10^{-5} (0.64)
10	$V_{22} \cdot P_1$	7.1×10^{-5} (2.5)
11	$V_{22} \cdot V_{11}$	1.8×10^{-5} (0.64)
12	$V_{21} \cdot N_1$	4.2×10^{-8} (~ 0)
13	$V_{21} \cdot V_{12}$	1.8×10^{-5} (0.35)
14	$V_{22} \cdot P_1$	7.1×10^{-5} (2.5)
15	$V_{21} \cdot V_{11}$	1.8×10^{-5} (0.64)

EXAMPLE OF PRA (cont)

Cut Sets of the On-Site Fire Protection System Failure (cont)

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
16	$OP_1 \cdot N_1$	1.0×10^{-7} (~ 0)
17	$OP_1 \cdot V_{12}$	4.2×10^{-5} (1.5)
18	$OP_1 \cdot P_1$	1.7×10^{-4} (6.0)
19	$OP_1 \cdot V_{11}$	4.2×10^{-5} (1.5)
20	$P_2 \cdot N_1$	1.7×10^{-7} (~ 0)
21	$P_2 \cdot V_{12}$	7.1×10^{-5} (2.5)
22	$P_2 \cdot P_1$	2.9×10^{-4} (0.3)
23	$P_2 \cdot V_{11}$	7.1×10^{-5} (2.5)
24	CCF	1.8×10^{-3} (63.8)
$Pr(ON) = \Sigma_i C_i = 2.8\times10^{-3}$		

EXAMPLE OF PRA (cont)

Quantification

These steps are described below (cont):

2. The cut sets of the Off-Site Fire Protection System Failure are similarly obtained and listed below.

Cut Sets of the Off-Site Fire Protection System

Cut Set No.	Cut Set	Probability (% contribution to the total probability)
1	LFD	1×10^{-4} (100)
2	$OP_2 \cdot DAA$	1×10^{-7} (~0)
Total $Pr^{(OFF)} \approx 1\times10^{-4}$		

EXAMPLE OF PRA (cont)

Quantification

These steps are described below (cont):

3. The cut sets of the three scenarios are obtained using the following Boolean equations representing each scenario:

$$\text{Scenario}-1 = \text{F}\cdot\overline{\text{ONS}}$$

$$\text{Scenario}-2 = \text{F}\cdot\text{ONS}\cdot\overline{\text{OFS}}$$

$$\text{Scenario}-3 = \text{F}\cdot\text{ONS}\cdot\text{OFS}$$

4. The frequency of each scenario is obtained using data listed in Tables (Slide 185 to 188). These frequencies are shown in the Table "Dominant Minimal Cut-Sets of the Scenarios".

5. The total frequency of each scenario is calculated using the rare event approximation. These are also shown in the Table "Dominant Minimal Cut-Sets of the Scenarios".

EXAMPLE OF PRA (cont)

Consequences

In the scenario development and quantification tasks, we identified three distinct scenarios of interest, each with different outcomes and frequencies. The consequences associated with each scenario should be specified in terms of both economic and/or human losses. This part of the analysis is one of the most difficult for several reasons:

- Each scenario poses different hazards and methods of hazard exposure.
- The consequence of the scenario can be measured in terms of human losses.

Economic Consequences of Fire Scenarios

Scenario Number	Economic Consequence
1	$ 1,000,000
2	$ 92,000,000
3	$ 210,000,000

EXAMPLE OF PRA (cont)

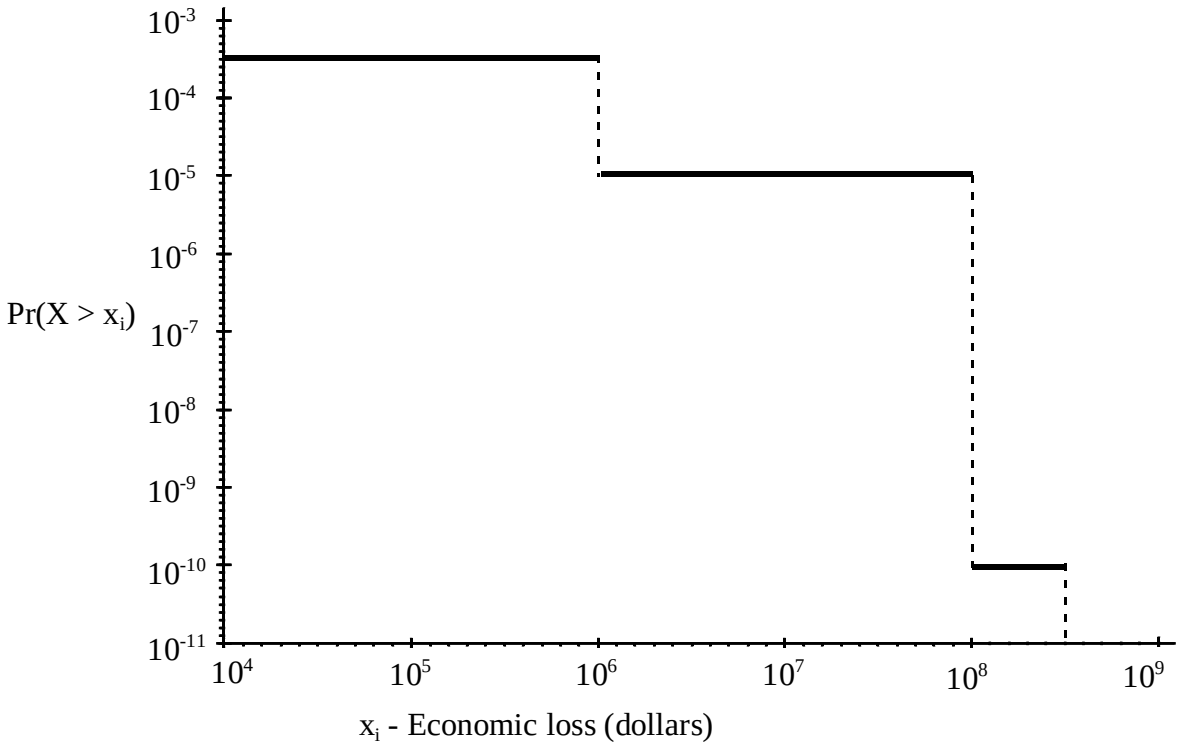
Risk Value Calculation and Evaluation

Using values from Table (Slide 190), we can calculate the risk associated with each scenario. These risks are shown in the Table below.

Scenario Number	Economic Consequence (expected loss)
1	(7.1×10^{-4}) ($1,000,000) = $ 710.000
2	(2.5×10^{-6}) ($92,000,000) = $ 230.000
3	(8.6×10^{-11}) ($210,000,000) = $ 0.018

EXAMPLE OF PRA (cont)

Risk Value Calculation and Evaluation



RISK MANAGEMENT

&

DECISION MAKING TECHNIQUES

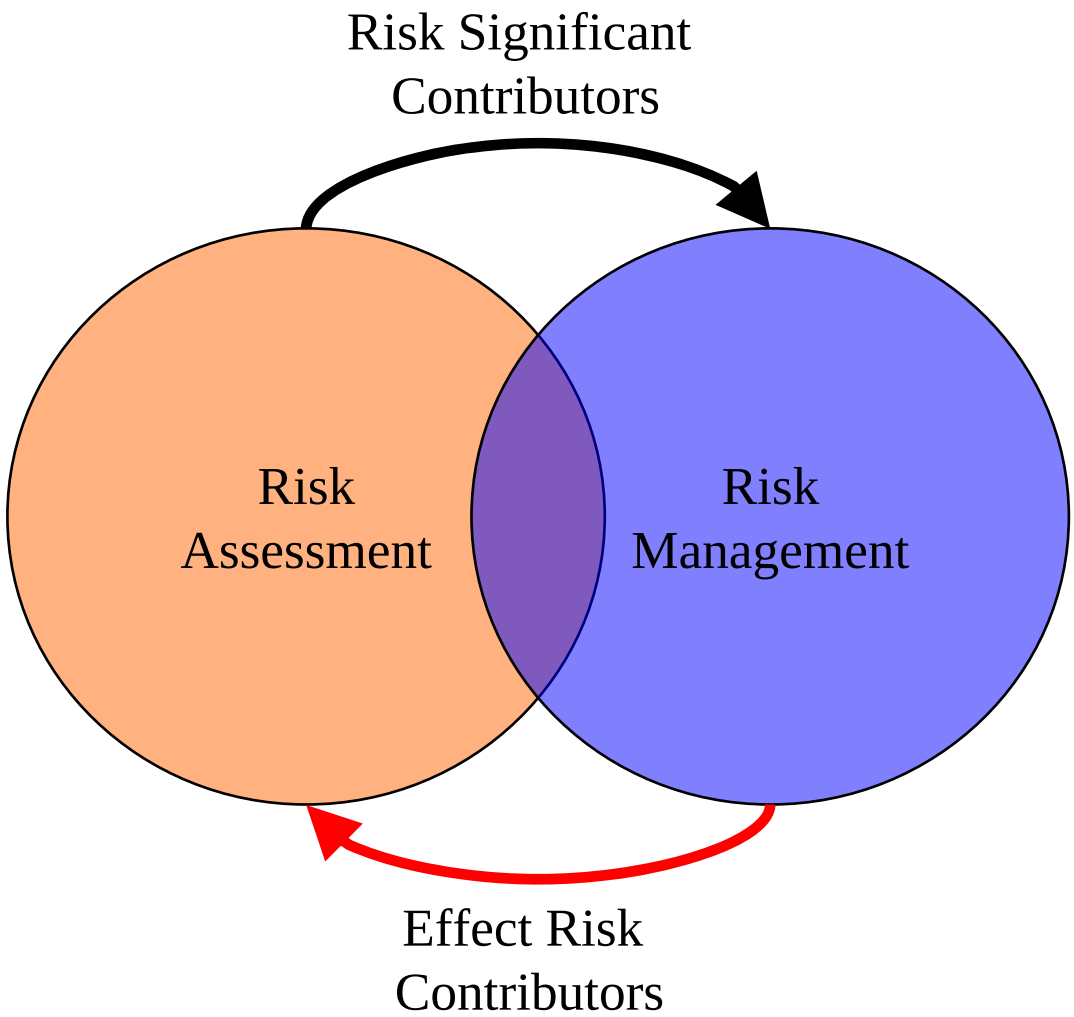
RISK MANAGEMENT

Is a practice involving coordinated activities to prevent, control and minimize losses incurred due to a risk exposure, weighing alternatives, and selecting appropriate actions by taking into account risks values, economic, technology constraints, legal and political issues.

- Continually assess the risk (what could go wrong?)
- Decide which risks are significant to deal with.
- Employ strategies to avert, control or minimize risks.
- Continually assess effectiveness of the strategies and revise them, if needed.

Risk management involves identifying the prime contributors to risk. Complex systems follow the 80:20 rules or the "Pareto's Principle“: more than 80% of the risk is contributed by less than 20% of risk scenarios or elements of the complex system. Risk management identify ways to avert control and minimize the 20%. That is, to achieve the highest risk reduction with the limited resources available

RISK ASSESSMENT-RISK MANAGEMENT SYNERGY



ECONOMIC METHODS IN RISK ANALYSIS

- **Cost-Benefit**
- Cost-Effectiveness
- Risk-Effectiveness Analysis

COST-BENEFIT METHOD

(As applied to Risk Management)

Risks are controlled (risk aversion) by reducing probability that a causative event will occurs or by minimizing exposure pathways.

Causative Control - quit smoking to avoid cancer, or use filtered cigarettes to hopefully reduce amount of cancer causing agent.

On the other hand smoking for example has both voluntary (smoker) and involuntary (premature death of the smoker or potential injuries to the passive smokers) risks.

Should risks and risk causing activities be regulated? When?

Cost-Benefit: (a measure of acceptability of risk)

Loss-Gain: So as to have one scale of measurement (for example $ or FLU)

COST-BENEFIT METHOD (cont)

Benefits: direct and indirect (can be voluntarily avoided)

Direct: profits from a new manufactured product

Indirect: benefit to the stores selling this product to the society gets the benefit of having a new product

Cost: direct loses are explicit and can not be voluntarily avoided when an activity is undertaken

A new plant commitment → investment of capital funds

Indirect costs or loses

Example: environmental pollution because of plant iteration

BALANCING GAINS AND LOSSES

Case	Direct Balance	Indirect Balance	Decision
1	$C_D < B_D$	$C_I < B_I$	Acceptable
2	$C_D > B_D$	$C_I > B_I$	Unacceptable
3	$C_D < B_D$	$C_I > B_I$	Unacceptable (unless allowed by Regulation)
4	$C_D > B_D$	$C_I < B_I$	Unacceptable (unless subsidized)

C_I - illegal drug operation in certain cause allowed under regulation (for example gambling operation) - nuclear power - between 2 and 4

B_I - since indirect societal benefit exceeds - direct balance so direct balance can be under written (development a new drug for curing cancer) - train subsidies

For comparing the effectiveness of multiple risk control measures, sometimes the benefit-cost ratio is used. The ratio is defined as

$$R_{b\text{-}c} = B/C$$

where, B is the benefit (direct, indirect or total) and C is the cost (direct, indirect or total).

COST-BENEFIT METHOD (cont)

Problem arises when using only analytical balance instead of subjective balance combination of both would be desirables

Example: Benefits are not ***always*** transferred to those receiving risk. So involuntary risk exist. For example, people near airport bear a high level of noise but they usually use airport least.

Therefore groups receiving risk and benefit must be clearly identified.

- short term benefits and long terms loses. Difficult to consider not good techniques exist for discounting future risk. On the other hand the reverse (short term risk and long term benefits) are more recognized to the society and more favorably accepted.

EXAMPLE 1: COST-BENEFIT METHOD

The case in question involves a scenario involving fuel tank side impacts in traffic accidents involving a particular design of pickup truck that may lead to explosions and fire-related injuries. The manufacturer is considering three risk reduction options. Determine the benefit-to-cost ratios for each design option. The data apply to reduction or prevention. The following risk reduction options are considered:

Option 1: Install a protective steel plate. Cost $14. This will effectively prevent all explosions.

Option 2: Install a Lexan plastic plate. Cost $4. This will prevent 95% of explosions.

Option 3: Install a plastic lining inside the fuel tank. Cost $2. This will prevent 85% of explosions.

EXAMPLE 1: COST-BENEFIT METHOD (cont)

The following risk and cost data apply to this vehicle when no risk-reduction option is implemented:

- Possible fatalities from vehicles already shipped: 180
- Expected cost per fatality: $500,000
- Number of injuries expected (no fatality): 200
- Cost per injury: $70,000
- Expected number of vehicles damaged (no injury): 3,000
- Cost to repair the vehicle: $1200
- Number of vehicles to be manufactured: 6,000,000

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Solution:

The cost for each option is the cost of implementing the change. The benefits are in terms of lives saved and avoidance of injury and damage.

Option 1:

Cost = $14 x 6,000,000 vehicles = $84,000,000

Benefits = (180 lives saved)($500,000) + (200 injuries prevented)

x ($70,000) + (3000 damaged vehicles prevented)($1200)

= $107,600,000

R = $107,600,000/ $84,000,000 = 1.28

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Option 2:

Cost = $4 x 6,000,000 = $24,000,000

Benefits = (95% accidents prevented) x [(180 fatalities)($500,000)

+ (200 injuries) x ($70,000) + (3000 vehicles)($1200)]

Benefits = 0.95 x $107,600,000

= $102,220,000

R = $102,220,000 /$24,000,000 = 4.25

EXAMPLE 1: COST-BENEFIT METHOD (cont)

Option 3:

Cost = \$2 x 6,000,000 = \$12,000,000

Benefits = (85% accidents prevented)[(180 fatalities)(\$500,000)

+ (200 injuries) x (\$70,000) + (3000 vehicles damage)

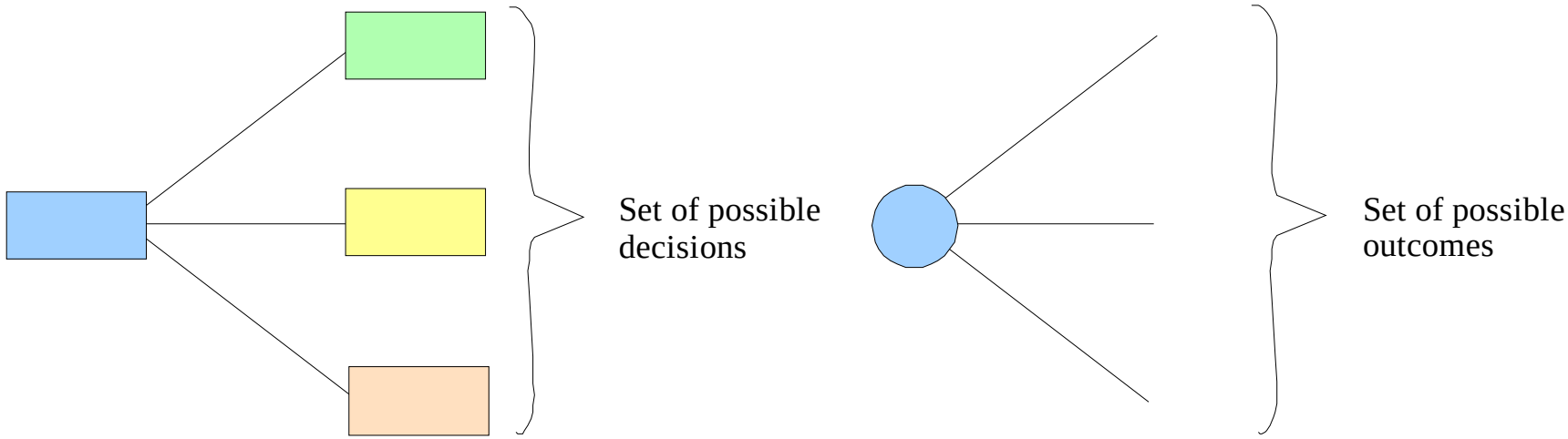
= 0.85 x \$107,600,000 = \$91,460,000

R = \$91,460,000/\$12,000,000 = 7.62

Option 3 has the highest benefit/cost ratio (R). As noted earlier, the decision should not be solely based on this figure of merit, as other indirect factors such as the manufacturer's reputation should also be considered.

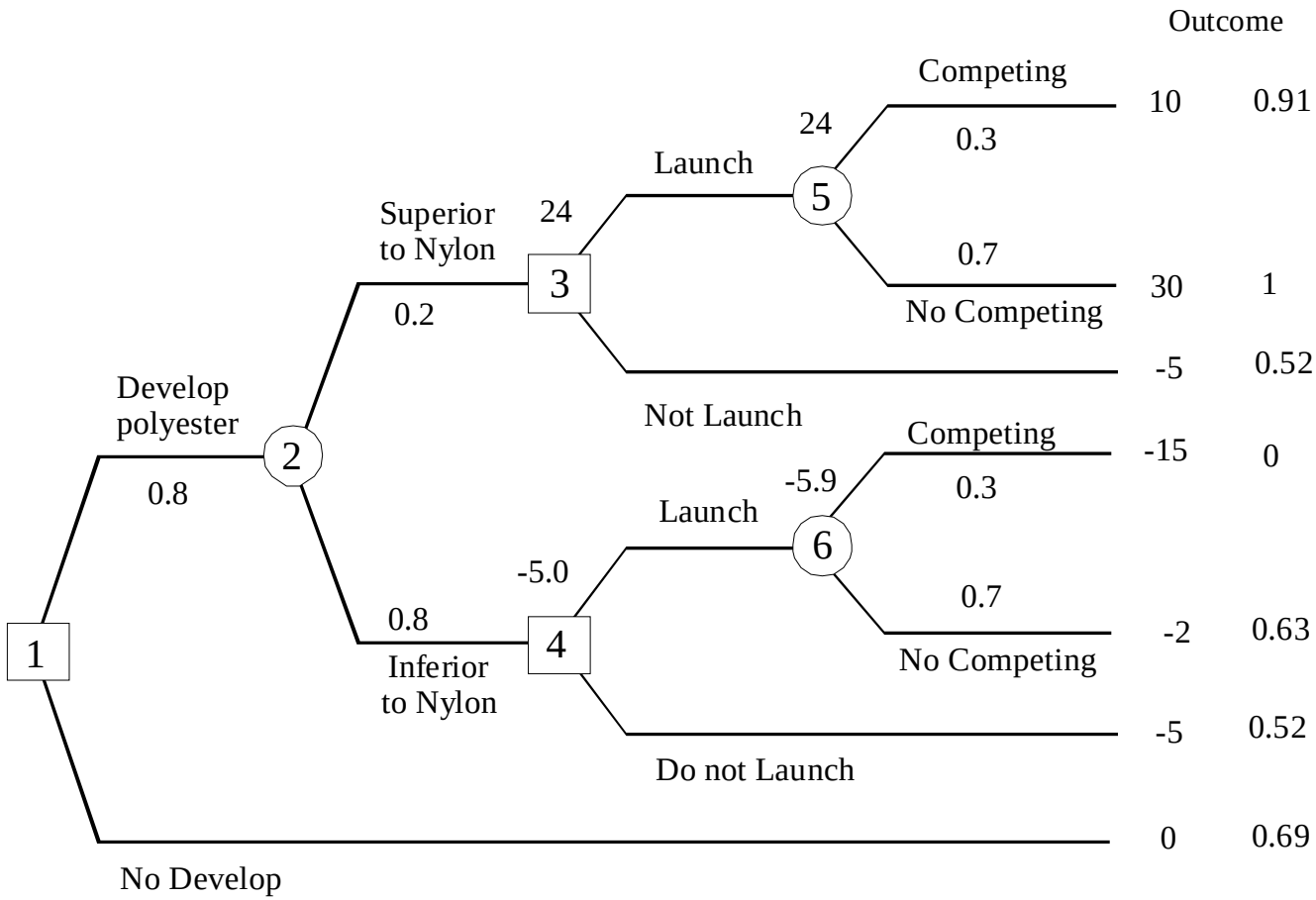
DECISION TREE ANALYSIS

Decision Trees are good for helping a risk manager to choose between several courses of risk control actions. They are highly effective structures within which one can lay out risk control solutions and investigate the possible outcomes of choosing such solutions



EXAMPLE 1: DECISION TREE

The tree below shows the developed decision tree and all sub-decisions and events involved



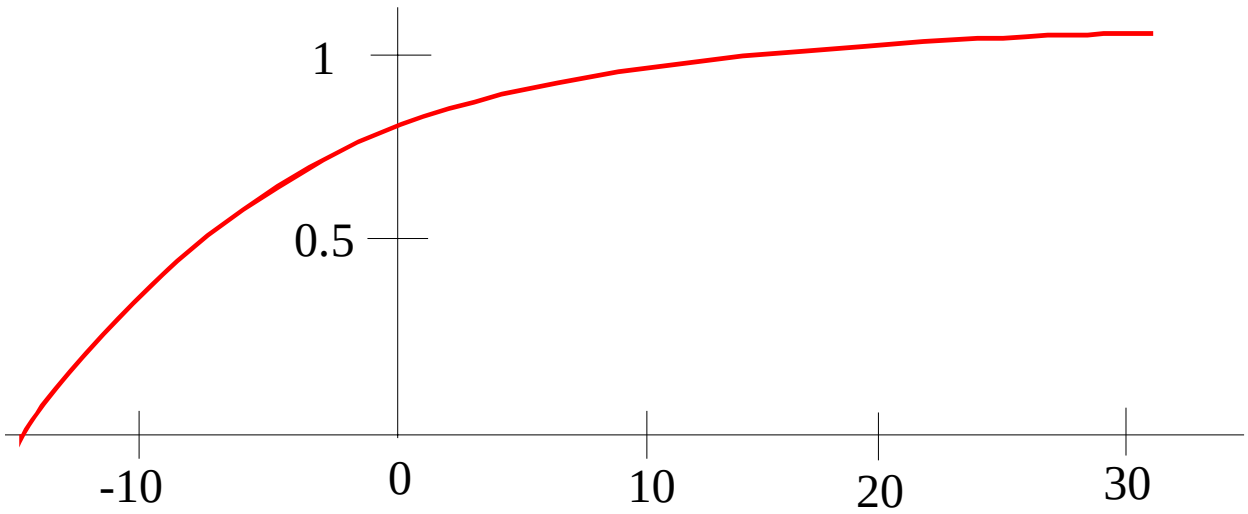
EXAMPLE 1: DECISION TREE (cont)

Risk = expected monetary value (EMV)

EMV

node 5 = 0.3 x 10 + 0.7 x 30 = 24

node 6 = 0.3 x -15 + 0.7 x -2 = -5.9



Utility Function for Payoff

EXAMPLE 1: DECISION TREE (cont)

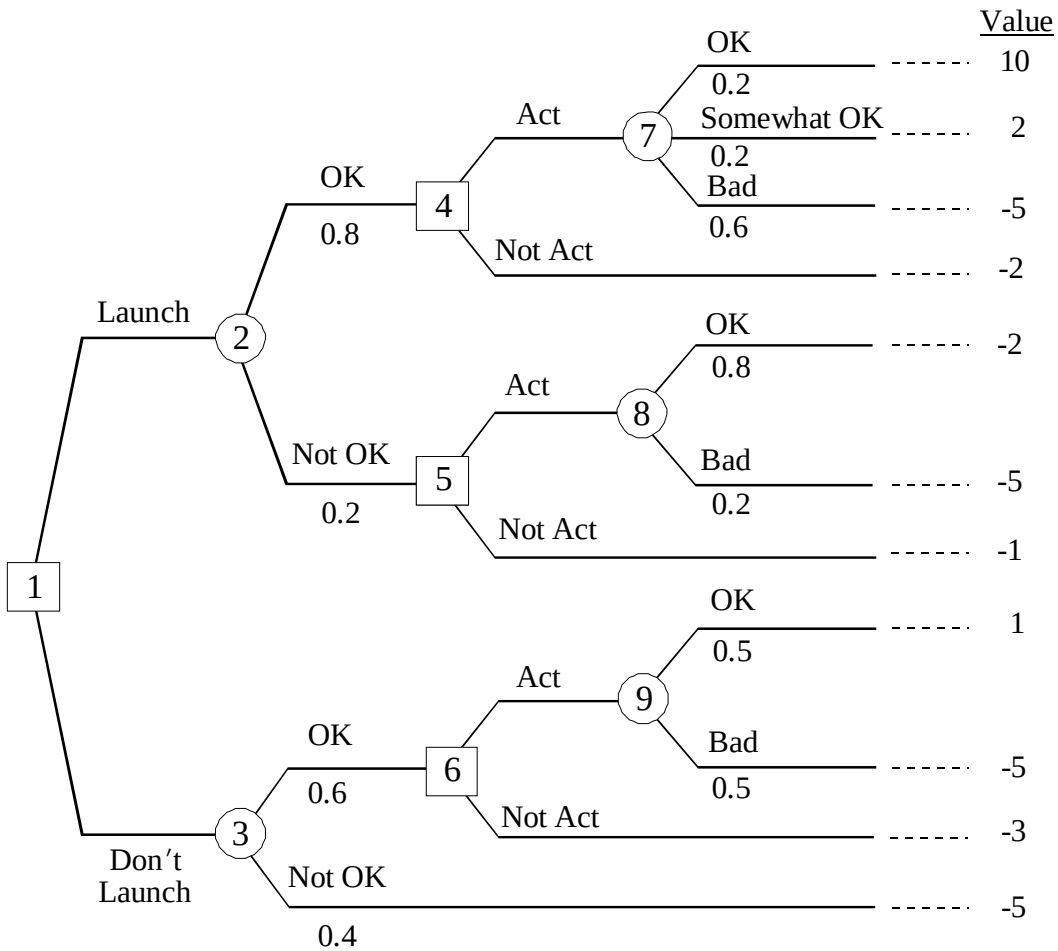
Based on the value function above, the value of each node is summarized.

Node	Expected Value Based on Actual Outcomes	Expected Value Based on the Value Judgment
1	0.8	0.69
2	0.8	0.61
3	24	0.97
4	-5	0.52
5	24	0.97
6	-5.9	0.44

Clearly in both evaluations, the value of node 1 (the main decision) is positive and, therefore, proceeding with the implementation of the proposed risk control solution is warranted.

EXAMPLE 2: DECISION TREE

For the following decision tree describe the outcome and the best decision



EXAMPLE 2: DECISION TREE (cont)

Solution:

The decision nodes (□) are 1, 4, 5, 6 and the chances nodes (o) are 2, 3, 7, 8, 9. For this decision tree, the outcome and the best decision are calculated according to the following:

Multiplying the payoff values by probability for chances nodes 7, 8 and 9:

Node 7: $(0.2 \times 10) + (0.2 \times 2) + (0.6 \times -5) = -0.6$
Node 8: $(0.8 \times -2) + (0.2 \times -5) = -2.6$
Node 9: $(0.5 \times 1) + (0.5 \times -5) = -2.0$

EXAMPLE 2: DECISION TREE (cont)

Using the above values and choosing the maximum at the decision nodes 4, 5 and 6:

At **Node 4** (maximum) between -0.6 and -2.0, choose -0.6.
At **Node 5** (maximum) between -2.6 and -1.0, choose -1.0.
At **Node 6** (maximum) between -2.0 and -3.0, choose -2.0.

Then, the values at chance nodes 2 and 3 will be:

Node 2: $(-0.6 \times 0.8) + (-1.0 \times 0.2) = -0.68$
Node 3: $(-2.0 \times 0.6) + (0.4 \times -5) = -3.2$

Therefore, the best decision is to "Launch" even though it has a negative payoff it is still greater than "Do Not Launch" negative payoff.

REMARKS ON DECISION TREES

Decision trees provide an effective method for policy and other decision making problems because they:

- clearly lay out the problem so that all options can be evaluated,
- analyze fully the possible consequences of a decision,
- provide a framework to quantify the values of outcomes and the probabilities of achieving them, and
- help to make the best decisions on the basis of existing information and best guesses.

As with all decision making methods, decision tree analysis should be used in combination with common sense, as decision trees are just one part of the actual risk management and control decision.

END OF LECTURE