ENRE 447/602 Reliability Analysis

Module 9: Risk Analysis

Katrina M. Groth

Associate Professor

Mechanical Engineering Department

Center for Risk and Reliability

University of Maryland

kgroth@umd.edu

Module 9 Objectives

- Understand how the previous modules combine to form a cohesive process for **quantitative risk assessment (QRA)**
- Understand the connection between risk analysis, risk assessment, risk management, and risk communication

Risk assessment methods

Type	Example Methods
Qualitative to Semi-quantitative	▪ FMEA (Failure Modes & Effects Analysis) ▪ FMECA (Failure Modes, Effects, & Criticality Analysis) ▪ PHA (Process Hazard Analysis) ▪ HAZOP (Hazards & Operability Analysis)

Quantitative	▪ QRA (Quantitative Risk Assessment) or PRA (Probabilistic Risk Assessment), including:
	  ▪ Fault trees
	  ▪ Event trees
	  ▪ Bayesian networks
	  ▪ Simulation
	  ▪ Hazard models

- Categories of risk analysis applications:
  - **Safety**: estimate potential harms due to natural or anthropogenic causes
  - **Security**: estimating access and harm due to intentional malicious actions
  - **Health**: estimate potential disease, injury, and mortality
  - **Financial:** estimating potential monetary losses
  - **Environmental:** estimate losses due to noise, contamination, pollution, etc.

Definition: QRA

- **Risk** is defined as a triplet:
  - What can go wrong? (**Scenario** – S_i)
  - How likely is it to happen? (**Probability** – P_i)
  - If it does happen, what are the consequences? (**Consequence** – C_i)
- Thus, **Quantitative Risk Assessment (QRA)** QRA has three main pieces:
  1. Identifying the scenarios S_i that comprise sequences of events, root causes, and outcomes of challenges to the system.
  2. Determining the probability P_i or frequency of occurrence F_i for each event E_i in each scenario S_i.
  3. Evaluating the consequences C_i of each scenario S_i occurrence.
- The **total expected risk value** R is the expected consequence summed over possible scenarios:

$$R = \sum_{S_i} P_i \times C_i$$

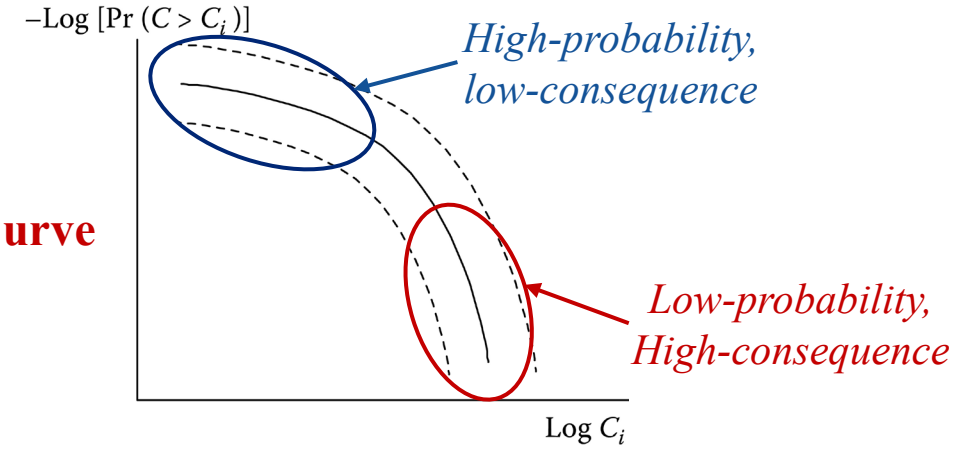
QRA results interpretation

- The total risk value R can mask qualitative aspects of the risk.
- **Example:** Scenario 1 occurs with a frequency $f_1 = 0.01\ \text{yr}^{-1}$ and a \$1,000,000 loss. Scenario 2 occurs with $f_2 = 1\ \text{yr}^{-1}$ and a \$10,000 loss. Thus, the total risk values are equal:

$$R_1 = f_1 \times C_1 = 0.01\ \text{yr}^{-1} \times \$1{,}000{,}000 = \$10{,}000/\text{yr}$$
$$R_2 = f_2 \times C_2 = 1\ \text{yr}^{-1} \times \$10{,}000 = \$10{,}000/\text{yr}$$

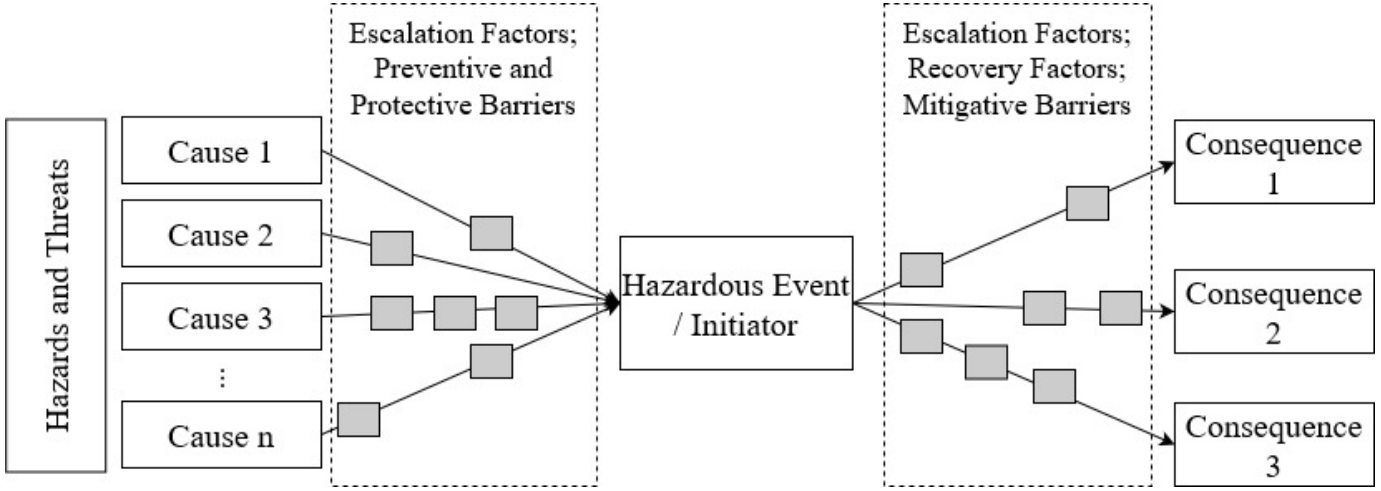
- QRA results can also be interpreted via a **risk profile** that plots probability against consequences, which can differentiate the low-P, high-C events from high-P, low-C events and thus provide a basis for decision.

Farmer's Curve



QRA Process

- The process of QRA is a function of the scenarios, probabilities/frequencies, and consequences in a system.
- QRA attempts to identify all possible scenarios that lead to losses, and for each scenario:
  - Probabilities or frequencies of each event
  - Description and amount of consequences
- The **bowtie model** visualizes the key elements of QRA



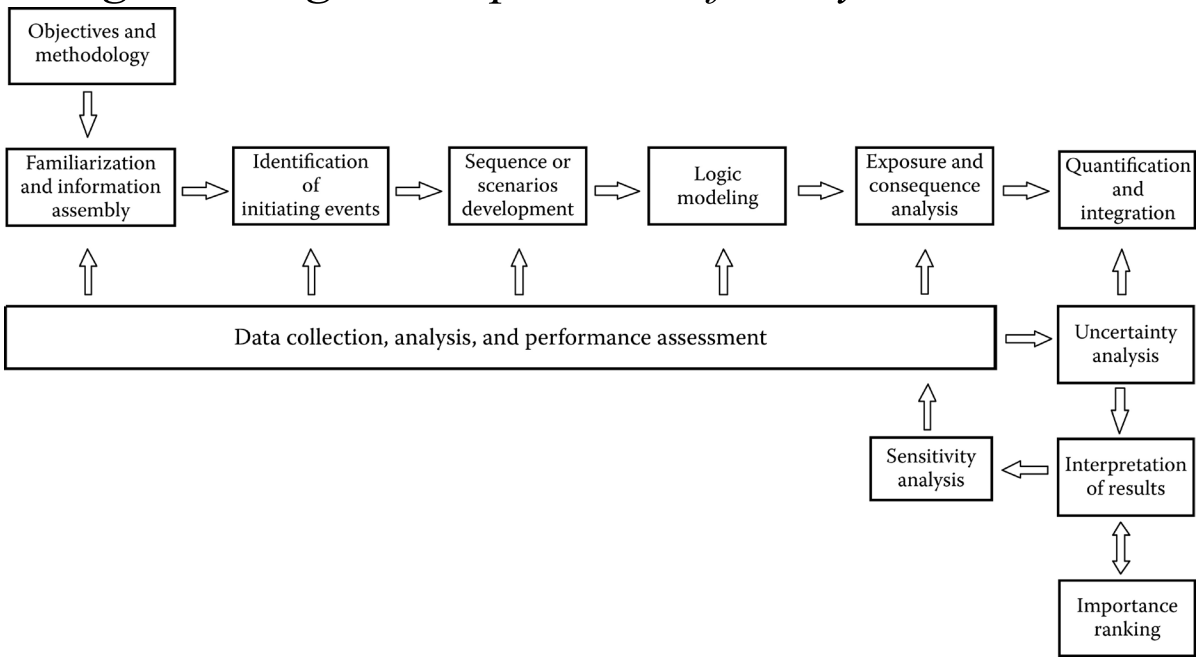
Steps in QRA

QRA requires characterizing several key aspects of a system and scenario:

1. **Initiating event**: identify root causes, preventive & protective barriers, escalating factors
2. **Hazard exposure**: form the chain of events for each scenario S_i that lead to exposure of the hazard and, if not mitigated, consequence C_i.
3. **Hazard identification**: survey the process/system to identify hazards.
4. **Barrier identification**: identify the barriers that contain, prevent, or minimize exposure to the hazard.
5. **Barrier challenges**: identify the mechanisms by which barriers may be challenged and/or degrade.
   - **Barrier strength degradation:** reduced thickness, material property changes
   - **Barrier stress:** internal forces or pressure, penetration/distortion from external forces
   - **Degradation conditions:** process malfunction, poor design, natural phenomena

PRA process

- **Probabilistic risk assessment (PRA)** is the most well-known QRA method.
  - *The primary value of a PRA is to highlight the system design and operational deficiencies and support subsequent risk management efforts to identify and optimize resources that can be invested on improving the design and operation of the system.*



PRA process (1)

1. **Objectives & Methodology**
   - Define/review the method, scope, rules and objectives of the analysis
2. **Familiarization & Information Assembly**
   - Identify major barriers, structures, systems, human interventions, subsystem interactions
   - Study past failures, dependent events, near-misses, abnormalities
3. **Initiating Events**
   - Identify the events that, if not responded to, could result in hazard exposure
4. **Scenario Development**
   - Create scenario event trees that encompass all potential exposure paths
5. **Causal Logic Modeling**
   - Create event and fault trees
6. **Data Collection, Analysis, and Assessment**
   - Gather data from generic sources, past events, expert judgment, etc.
7. **Consequence Analysis**
   - Characterize the range of possible effects from hazard exposure
8. **Quantification & Integration**
   - Form a single, coherent model from the logic trees; find minimal cut sets and frequencies

PRA process (2)

9. Uncertainty Analysis

- Incorporate the uncertainties from all facets of the PRA and inform risk managers

10. Sensitivity Analysis

- Determine the significance of model/parameter choice
- Identify PRA elements that might be sensitive to the final risk results
- Vary the value of sensitive items to propagate the changes through to the final result
- Rank the elements that are most sensitive

11. Risk Ranking and Importance Analysis

- Rank the scenarios and system elements corresponding to their risk/safety significance
- Importance Measures indicate the absolute or relative (to other system elements) importance of specific system elements

12. Interpretation of Results

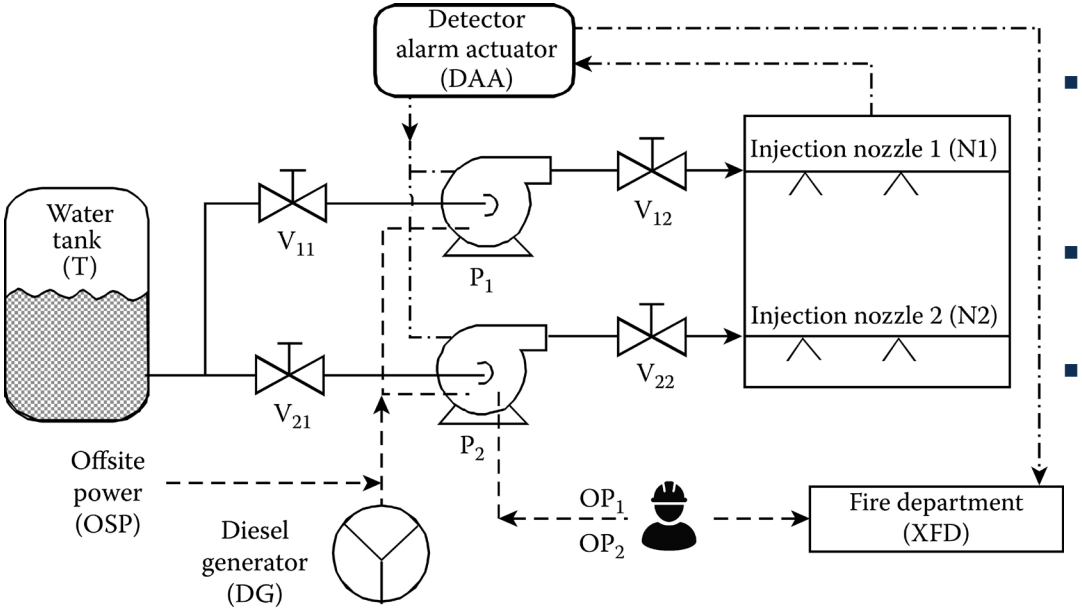
- Determine the accuracy of logic models and scenario structures, assumptions, and scope of PRA
- Identify system elements for which better information is necessary to reduce uncertainties
- Revise the PRA and reinterpret results until stable and accurate results are obtained

Strengths of PRA

- PRA is the most rigorous formal QRA approach with many strengths:
  1. Integrated, systematic explanation of design and operational features
  2. Insight into the root causes of failure and effectiveness of barriers
  3. Incorporation of causal factors, system interactions, and interfaces
  4. Incorporation of operating experience and relevant data
  5. Explicit consideration of uncertainty
  6. Analysis and comparison of competing risks
  7. Formal sensitivity evaluation of assumptions and data
  8. Absolute and relative importances of systems & components
  9. Consistent and transparent framework for data & information fusion
  10. Documented process for exploring priorities & encouraging discourse

Example PRA: Fire protection system (1/6)

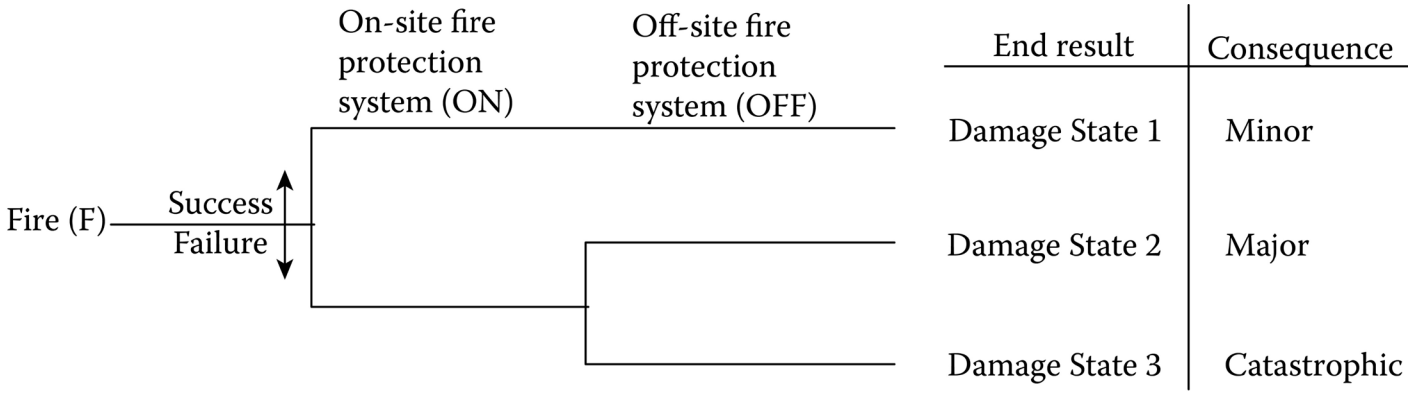
- Assess the potential risk and financial loss from possible failure scenarios of a fire protection system at a power plant
  - Independent nozzle trains – each can control any fire; nozzle N1 is primary.
  - Signal from DAA automatically starts pump P_1 and alerts fire department
  - Operator OP_1 can start the second injection path manually.
    - If this does not occur, operator OP_2 calls for fire department
    - Damage is greater if fire department required (i.e., nozzles unable to extinguish)



- If normal off-site power (OSP) not available, on-site diesel generator (DG) provides power to pumps.
- Battery power for pumps always available.
- Valves are normally open, but manually shut when pumps are being repaired.

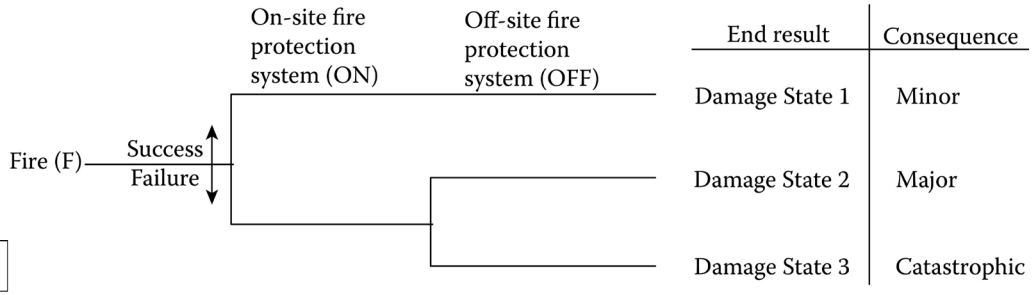
Example PRA: Fire protection system (2/6)

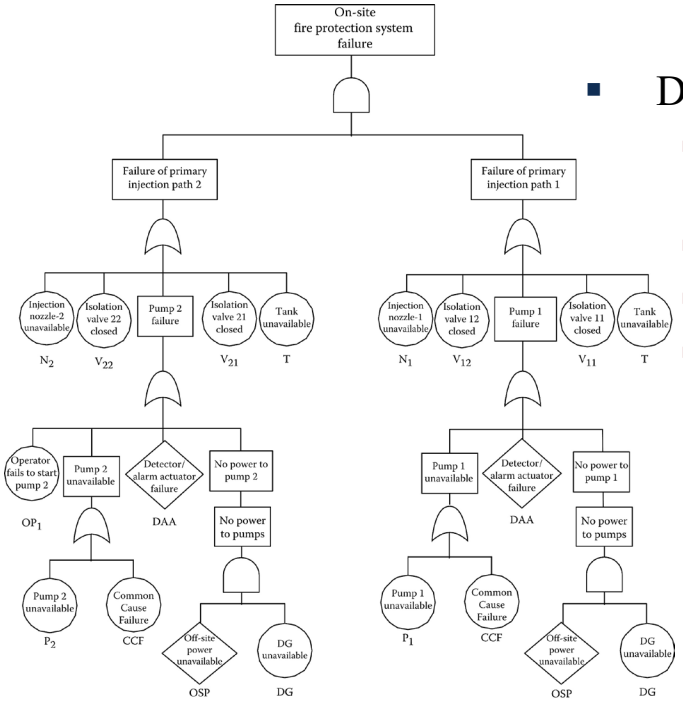
- **Identify initiating events:**
  - Find all events that could cause a sustained fire in the main building
    - Equipment malfunction, human error, facility conditions
  - Estimate the frequency of each event
  - If multiple events lead to the same magnitude of fire (e.g., same consequence), sum the individual frequencies
  - Assume fire frequency: $f_F = 7.1 \times 10^{-4}\ \mathrm{yr}^{-1}$ (only initiating event)
- **Scenario development:**
  - Model the cause-effect relationships between the fire and following events
  - **Recall:** two types of protective measures (onsite pumps/tanks, offsite fire dept.)



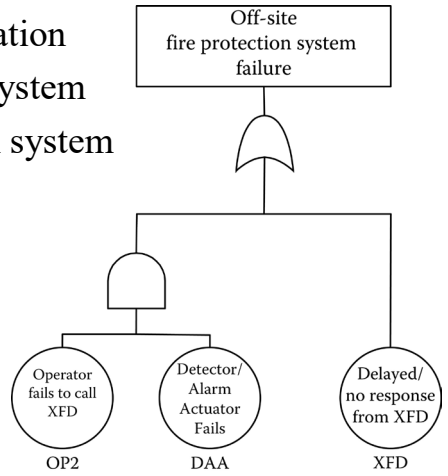
Example PRA: Fire protection system (3/6)

- **Causal logic model development:**
  - Identify the failures (equipment or human) that lead to failure of pivotal events





- Describe all basic events that lead to failure in **fault trees**
  - Note that there are physical dependencies between components that are not accounted for in the fault tree
  - Dependencies will be considered in quantification
  - Left: fault tree for the on-site fire protection system
  - Right: fault tree for the off-site fire protection system

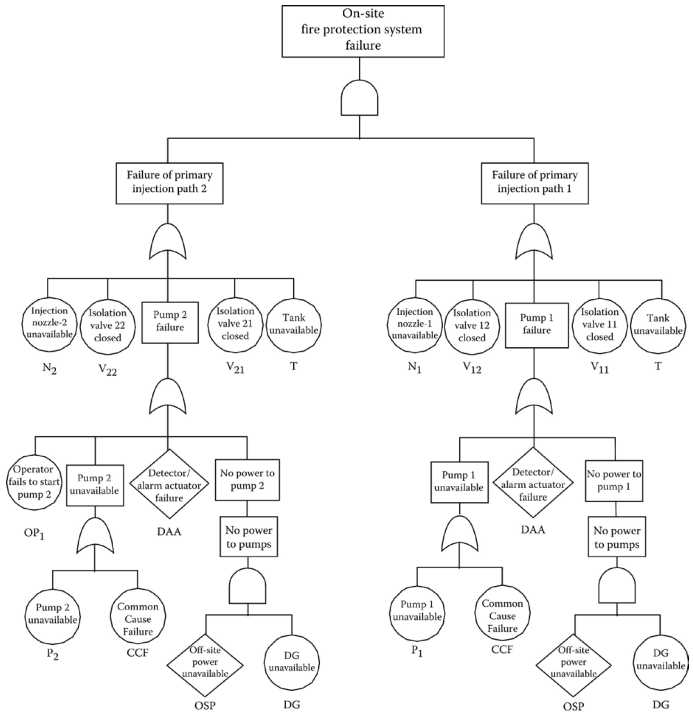


Example PRA: Fire protection system (4/6)

- **Failure data analysis:**
  - Find the basic event probabilities
  - Assume CCF b/w valves and nozzles, ≥10 hrs operation
- **Quantification and Interpretation:**
  - Find the cut sets and probabilities of the fault trees

Cut Set No.	Cut Set	Probability
1	XFD	1×10^{-4}
2	$OP_2 \cdot DAA$	1×10^{-7}

$$\text{Total Pr(OFF)} = \sum_i C_i \approx 1 \times 10^{-4}$$

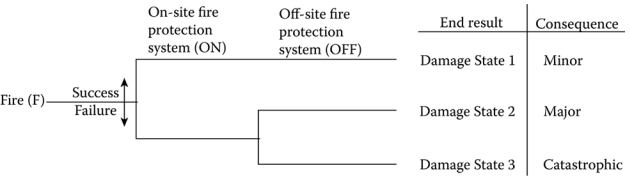


Cut Set #	Cut Set	Probability/(% of Total)	Cut Set #	Cut Set	Probability/(% of Total)
1	T	1.0×10^{-5} (0.36%)	13	$V_{21} \cdot V_{12}$	1.8×10^{-5} (0.65%)
2	DAA	1.0×10^{-4} (3.62%)	14	$V_{21} \cdot P_1$	6.7×10^{-5} (2.43%)
3	OSP·DG	6.1×10^{-6} (0.22%)	15	$V_{21} \cdot V_{11}$	1.8×10^{-5} (0.65%)
4	$N_2 \cdot N_1$	1.0×10^{-10} (~0%)	16	$OP_1 \cdot N_1$	1.0×10^{-7} (~0%)
5	$N_2 \cdot V_{12}$	4.2×10^{-8} (~0%)	17	$OP_1 \cdot V_{12}$	4.2×10^{-5} (1.52%)
6	$N_2 \cdot P_1$	1.6×10^{-7} (0.01%)	18	$OP_1 \cdot P_1$	1.6×10^{-4} (5.80%)
7	$N_2 \cdot V_{11}$	4.2×10^{-8} (~0%)	19	$OP_1 \cdot V_{11}$	4.2×10^{-5} (1.52%)
8	$V_{22} \cdot N_1$	4.2×10^{-8} (~0%)	20	$P_2 \cdot N_1$	1.6×10^{-7} (0.01%)
9	$V_{22} \cdot V_{12}$	1.8×10^{-5} (0.65%)	21	$P_2 \cdot V_{12}$	6.7×10^{-5} (2.43%)
10	$V_{22} \cdot P_1$	6.7×10^{-5} (2.43%)	22	$P_2 \cdot P_1$	2.6×10^{-4} (9.42%)
11	$V_{22} \cdot V_{11}$	1.8×10^{-5} (0.65%)	23	$P_2 \cdot V_{11}$	6.7×10^{-5} (2.43%)
12	$V_{21} \cdot N_1$	4.2×10^{-8} (~ 0%)	24	CCF	1.8×10^{-3} (65.2%)

$$\textbf{Total } \boldsymbol{Pr(ON)} = \sum_i \boldsymbol{C_i} \approx \mathbf{2.8 \times 10^{-3}}$$

Example PRA: Fire protection system (5/6)

- With the cut sets from the fault trees, we find the cut sets of each scenario:



Scenario 1 = $F \cdot \overline{ON}$

Scenario 2 = $F \cdot ON \cdot \overline{OFF}$

Scenario 3 = $F \cdot ON \cdot OFF$

- **Consequences of each scenario:**

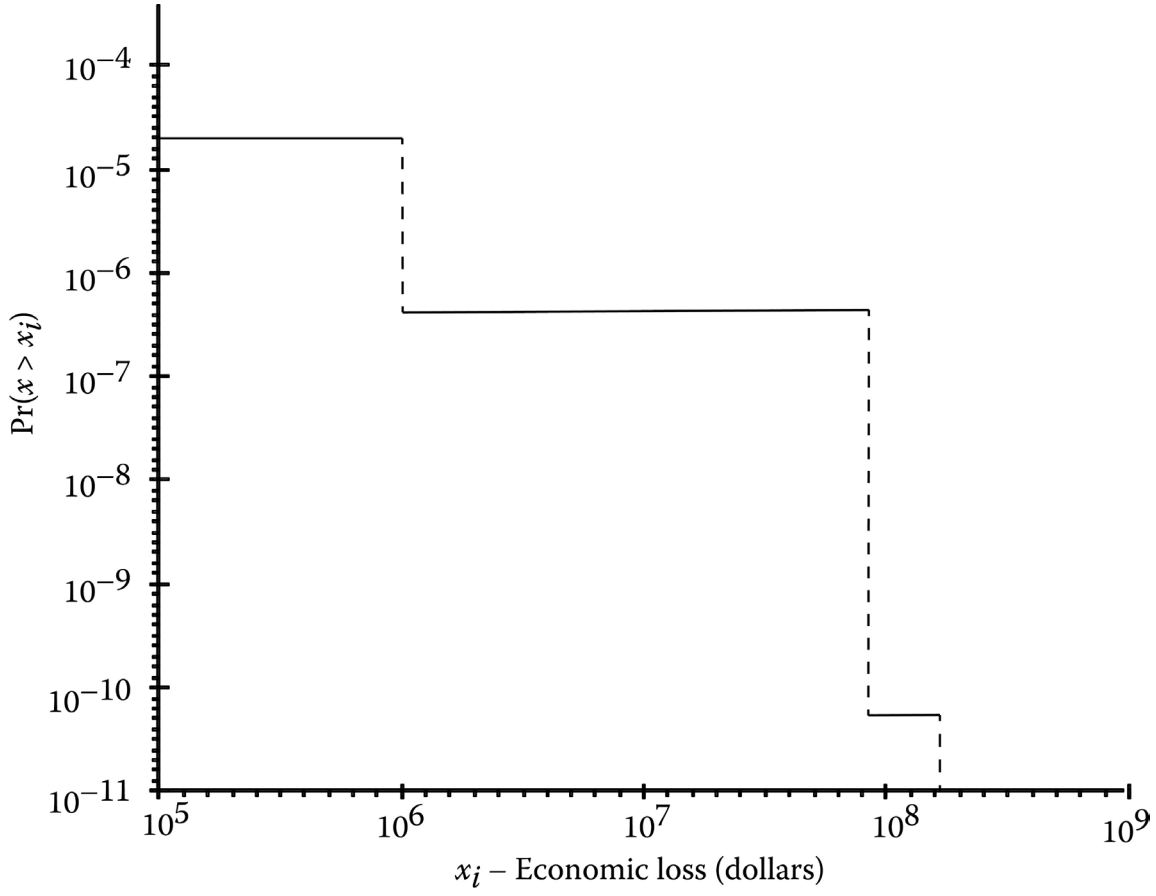
Scenario #	Economic Consequence
1	$1,000,000
2	$92,000,000
3	$210,000,000

- **Risk associated with each scenario:**

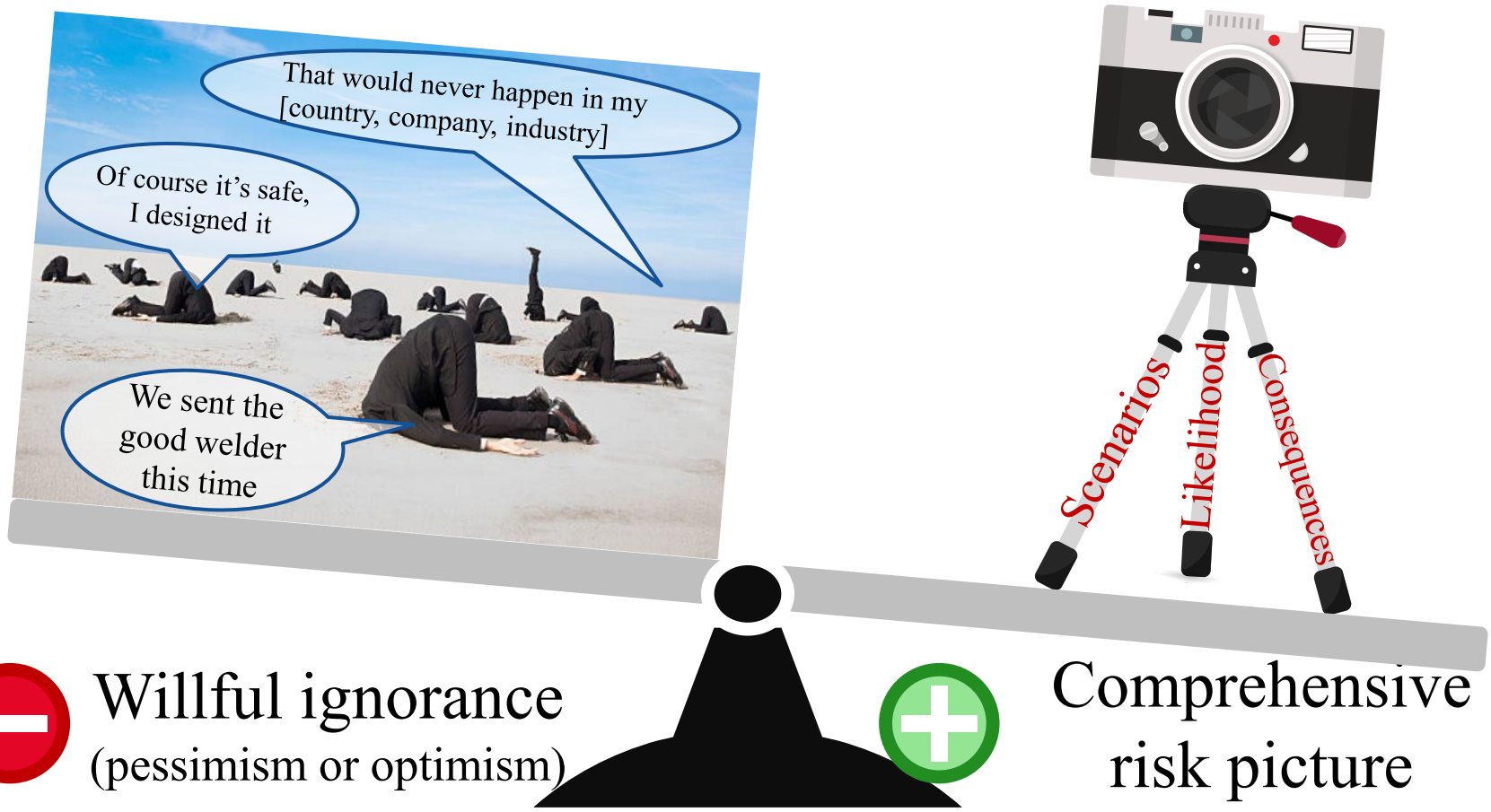
Scenario #	Economic Consequence
1	$(7.1 \times 10^{-4})(\$1{,}000{,}000) = \$710.00\ \mathrm{yr}^{-1}$
2	$(3.7 \times 10^{-6})(\$92{,}000{,}000) = \$340.00\ \mathrm{yr}^{-1}$
3	$(2.6 \times 10^{-10})(\$210{,}000{,}000) = \$0.05\ \mathrm{yr}^{-1}$

Scenario No.	Cut Sets	Frequency	Comment
1	$F \cdot \overline{ON}$	$7.1\times10^{-4}(1-2.8\times10^{-3})$ $\approx 7.1\times10^{-4}$	Since the probability can be directly evaluated for $\overline{ON}$ without the need to generate cut sets, only the probability is calculated
2	$F \cdot DAA \cdot \overline{XFD} \cdot \overline{OP_2}$	7.1×10^{-8}	1. Only cut sets that have a contribution greater than 1% of total are shown. 2. Cut set $F \cdot DAA \cdot \overline{XFD} \cdot \overline{DAA}$ is eliminated since $DAA \cdot \overline{DAA} = \phi$
	$F \cdot V_{22} \cdot P_1 \cdot \overline{XFD} \cdot \overline{OP_2}$	4.8×10^{-8}	
	$F \cdot V_{21} \cdot P_1 \cdot \overline{XFD} \cdot \overline{OP_2}$	4.8×10^{-8}	
	$F \cdot V_{22} \cdot P_1 \cdot \overline{XFD} \cdot \overline{DAA}$	4.8×10^{-8}	
	$F \cdot V_{21} \cdot P_1 \cdot \overline{XFD} \cdot \overline{DAA}$	4.8×10^{-8}	
	$F \cdot OP_1 \cdot V_{12} \cdot \overline{XFD} \cdot \overline{OP_2}$	3.0×10^{-9}	
	$F \cdot OP_1 \cdot V_{12} \cdot \overline{XFD} \cdot \overline{DAA}$	3.0×10^{-9}	
	$F \cdot OP_1 \cdot P_1 \cdot \overline{XFD} \cdot \overline{OP_2}$	1.1×10^{-7}	
	$F \cdot OP_1 \cdot P_1 \cdot \overline{XFD} \cdot \overline{DAA}$	1.1×10^{-7}	
	$F \cdot OP_1 \cdot V_{11} \cdot \overline{XFD} \cdot \overline{OP_2}$	3.0×10^{-9}	
	$F \cdot OP_1 \cdot V_{11} \cdot \overline{XFD} \cdot \overline{DAA}$	3.0×10^{-9}	
	$F \cdot P_2 \cdot V_{12} \cdot \overline{XFD} \cdot \overline{OP_2}$	4.8×10^{-8}	
	$F \cdot P_2 \cdot V_{12} \cdot \overline{XFD} \cdot \overline{DAA}$	4.8×10^{-8}	
	$F \cdot P_2 \cdot P_1 \cdot \overline{XFD} \cdot \overline{OP_2}$	1.8×10^{-7}	
	$F \cdot P_2 \cdot P_1 \cdot \overline{XFD} \cdot \overline{DAA}$	1.8×10^{-7}	
	$F \cdot P_2 \cdot V_{11} \cdot \overline{XFD} \cdot \overline{OP_2}$	4.8×10^{-8}	
	$F \cdot P_2 \cdot V_{11} \cdot \overline{XFD} \cdot \overline{DAA}$	4.8×10^{-8}	
	$F \cdot CCF \cdot \overline{XFD} \cdot \overline{OP_2}$	1.3×10^{-6}	
	$F \cdot CCF \cdot \overline{XFD} \cdot \overline{DAA}$	1.3×10^{-6}	
	2 Total	$\sum C_i = 3.7 \times 10^{-6}$	
3	$F \cdot DAA \cdot OP_2$	7.1×10^{-11}	1. Only cut sets that have a contribution greater than 1% of total are shown.
	$F \cdot DAA \cdot XFD$	7.1×10^{-12}	
	$F \cdot V_{22} \cdot P_1 \cdot XFD$	4.8×10^{-12}	
	$F \cdot V_{21} \cdot P_1 \cdot XFD$	4.8×10^{-12}	
	$F \cdot OP_1 \cdot V_{12} \cdot XFD$	3.0×10^{-12}	
	$F \cdot OP_1 \cdot P_1 \cdot XFD$	1.1×10^{-11}	
	$F \cdot OP_1 \cdot V_{11} \cdot XFD$	3.0×10^{-12}	
	$F \cdot P_2 \cdot V_{12} \cdot XFD$	4.8×10^{-12}	
	$F \cdot P_2 \cdot P_1 \cdot XFD$	1.8×10^{-11}	
	$F \cdot P_2 \cdot V_{11} \cdot XFD$	4.8×10^{-12}	
	$F \cdot CCF \cdot XFD$	1.3×10^{-10}	
	3 Total	$\sum C_i = 2.6 \times 10^{-10}$	

Example PRA: Fire protection system (6/6)



Principles



Revisit Quiz 1: Re-Write your failure scenario for the event you discussed on day 1 now that you have more knowledge from this class.

- Your scenario **must include**:
  - Event/accident name, date, description (1-2 sentences), and photo
  - System failure mode, operating environment, consequence(s)
  - At least one of: hardware failure mode, failure mechanism, environment, and human failure
- Example: Air France 447 Airbus A330 (July 1, 2009)

Component & failure mode — Component failure mechanism

Flow blockage of **pitot tubes,** caused by **freezing,** led to

Subsystem failure mode

erroneous airspeed indication resulting in **loss of control,**

System failure mode

loss of aircraft, fatality of all 228 passengers and crew,

Consequences

with pilot failure to diagnose the erroneous output due to

inadequate information, and time load. Occurred at **high**

Human failure mode & PIFs

Environment

altitude, low temperature, in stormy weather.

Image: Brazilian Navy/ Getty Images

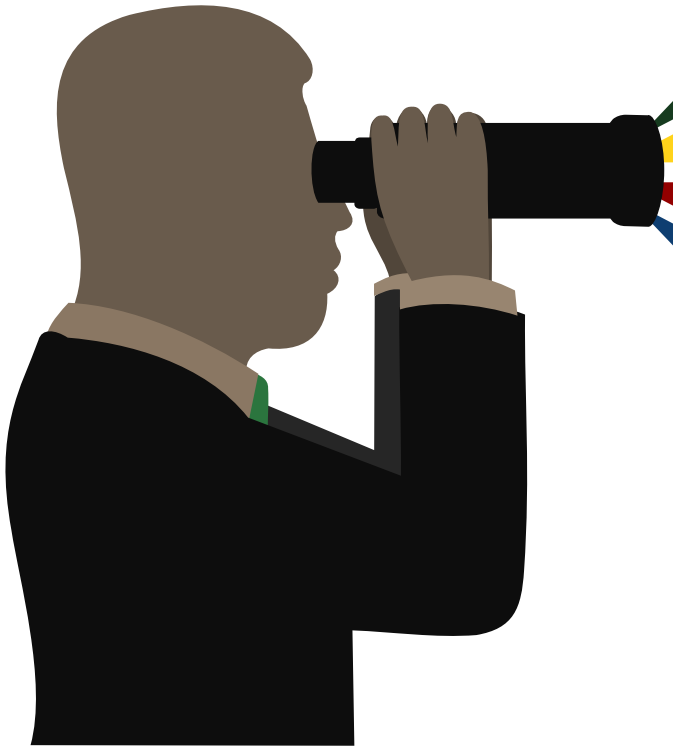
Revisiting Quiz 1

- Could you develop an event tree for the scenario? What about a fault tree? Which events would be placed where?
- Where could you get data for the events that happened in your failure scenario?

Closing thoughts for this course

The future of PRA

Engineering a safer world together



Principles

Remember the risk triplet, it is the tripod that holds us steady.

Progress

Invest in new ideas – some of which rethink PRA completely.

People

Invest in the people – our community is our future

Purpose

Strongly reinforce the purpose and the value of PRA