Engineering Risk Benefit Analysis

1.155, 2.943, 3.577, 6.938, 10.816, 13.621, 16.862, 22.82, ESD.72, ESD.721

RPRA 6. Probabilistic Risk Assessment

George E. Apostolakis
Massachusetts Institute of Technology

Spring 2007

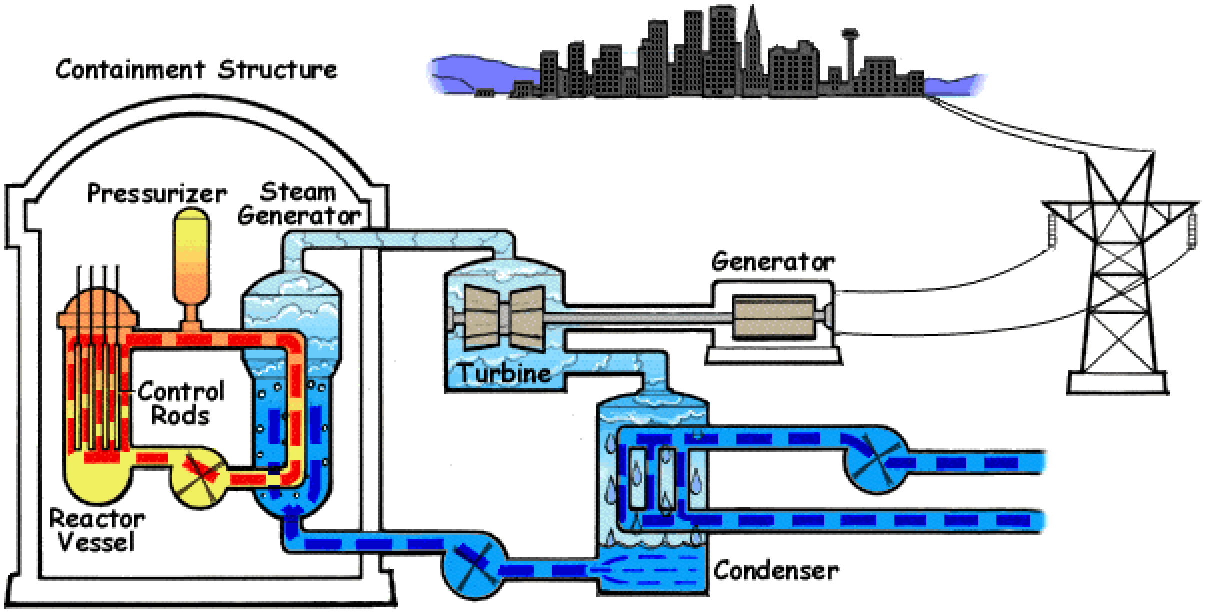
Objectives

- Identify accident scenarios.
- Rank these scenarios according to their probabilities of occurrence.
- Rank systems, structures, and components according to their contribution to various risk metrics.

PRA Steps

- **Define end states**
- **Identify initiating events**
- **Develop event and fault trees**
- **Quantify**

Example: Nuclear Power Plant



PWRs keep water under pressure so that it heats, but does not boil. Water from the reactor and the water in the steam generator that is turned into steam never mix. In this way, most of the radioactivity stays in the reactor area.

Courtesy NRC
http://www.nrc.gov/reading-rm/basic-ref/students/animated-pwr.html

NPP End States

- Various states of degradation of the reactor core.
- Release of radioactivity from the containment.
- Individual risk.
- Numbers of early and latent deaths.
- Number of injuries.
- Land contamination.

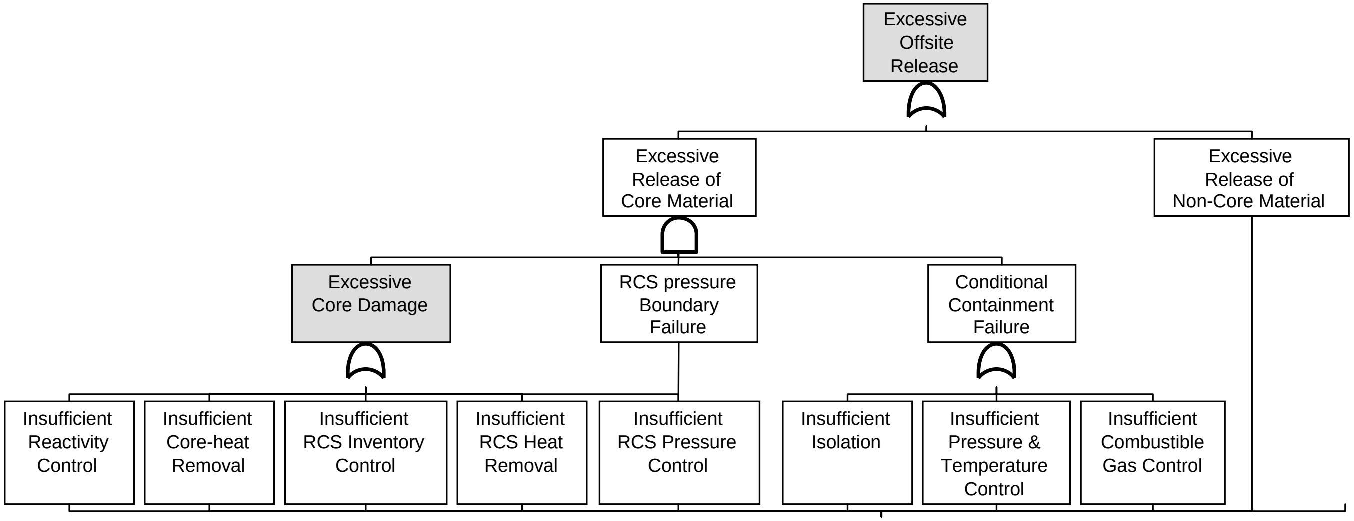
The Master Logic Diagram (MLD)

- Developed to identify Initiating Events in a PRA.
- Hierarchical depiction of ways in which system perturbations can occur.
- Good check for completeness.

MLD Development

- Begin with a top event that is an end state.
- The top levels are typically functional.
- Develop into lower levels of subsystem and component failures.
- Stop when every level below the stopping level has the same consequence as the level above it.

Nuclear Power Plant MLD


Excessive Offsite Release
Excessive Release of Core Material
Excessive Release of Non-Core Material
Excessive Core Damage
RCS pressure Boundary Failure
Conditional Containment Failure
Insufficient Reactivity Control
Insufficient Core-heat Removal
Insufficient RCS Inventory Control
Insufficient RCS Heat Removal
Insufficient RCS Pressure Control
Insufficient Isolation
Insufficient Pressure & Temperature Control
Insufficient Combustible Gas Control

NPP: Initiating Events

- Transients
  - *Loss of offsite power*
  - *Turbine trip*
  - *others*
- Loss-of-coolant accidents (LOCAs)
  - *Small LOCA*
  - *Medium LOCA*
  - *Large LOCA*

Event Sequence Diagrams and Event Trees

- Two different ways of depicting the progression of a scenario.

- Logically, they are equivalent.

NPP: Loss-of-offsite-power event tree

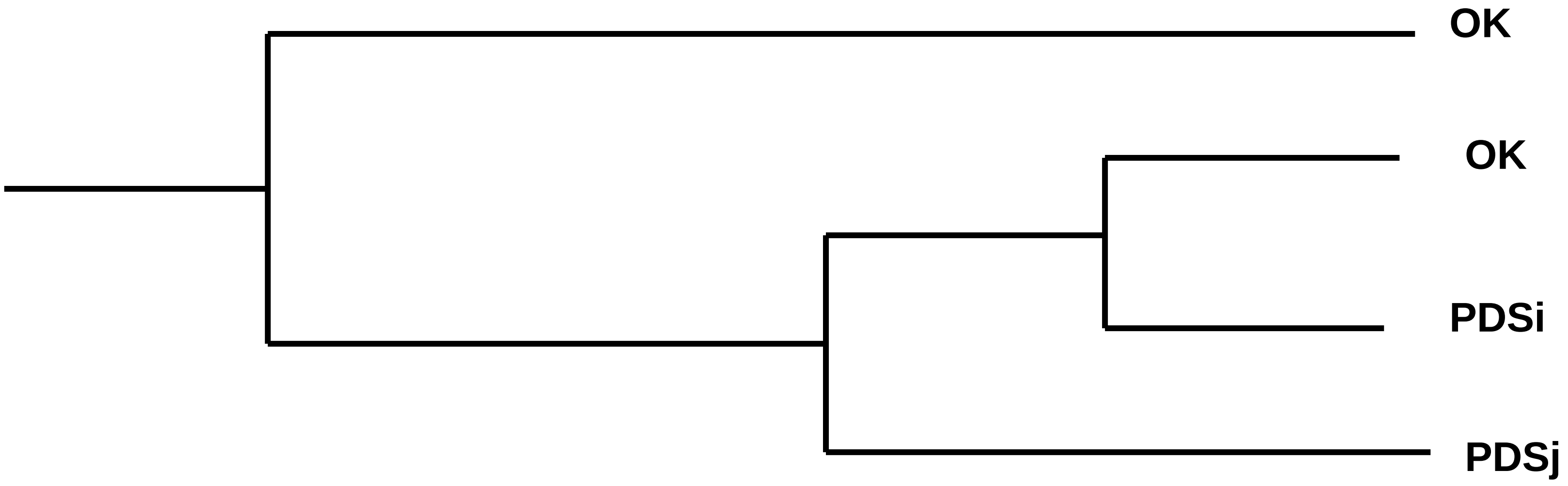
LOOP

Secondary Heat Removal

Bleed & Feed

Recirc.

Core



Human Performance

- The operators must decide to perform feed & bleed.
- Water is “fed” into the reactor vessel by the high-pressure system and is “bled” out through relief valves into the containment. Very costly to clean up.
- Must be initiated within about 30 minutes of losing secondary cooling (a thermal-hydraulic calculation).

J. Rasmussen's Categories of Behavior

- ***Skill-based behavior:*** **Performance during acts that, after a statement of intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior.**
- ***Rule-based behavior:*** **Performance is consciously controlled by a stored rule or procedure.**
- ***Knowledge-based behavior:*** **Performance during unfamiliar situations for which no rules for control are available.**

J. Rasmussen, *Information Processing and Human-Machine Interaction*, North-Holland, 1986.

Reason's Categories

Unsafe acts

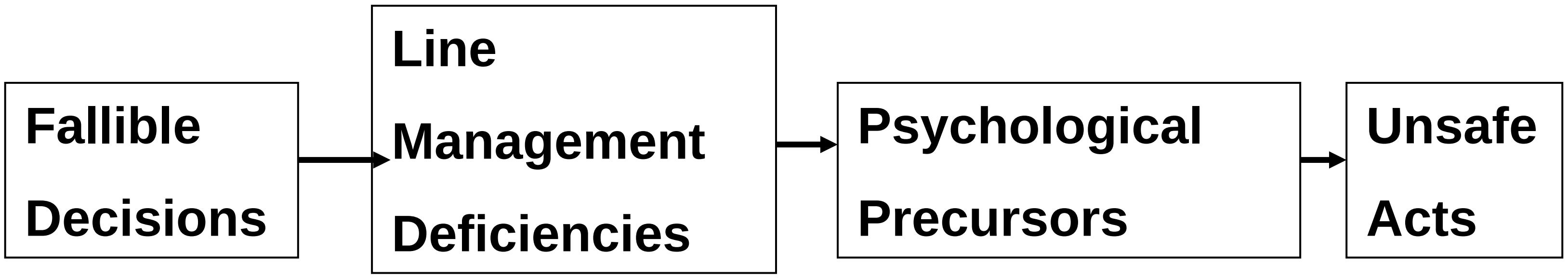
- *Unintended action*
  - Slip
  - Lapse
  - Mistake
- *Intended violation*

J. Reason, *Human Error*, Cambridge University Press, 1990

Latent Conditions

- Weaknesses that exist within a system that create *contexts* for human error beyond the scope of individual psychology.
- They have been found to be significant contributors to incidents.
- Incidents are usually a combination of hardware failures and human errors (latent and active).

Reason's Model



Pre-IE (“Routine”) Actions

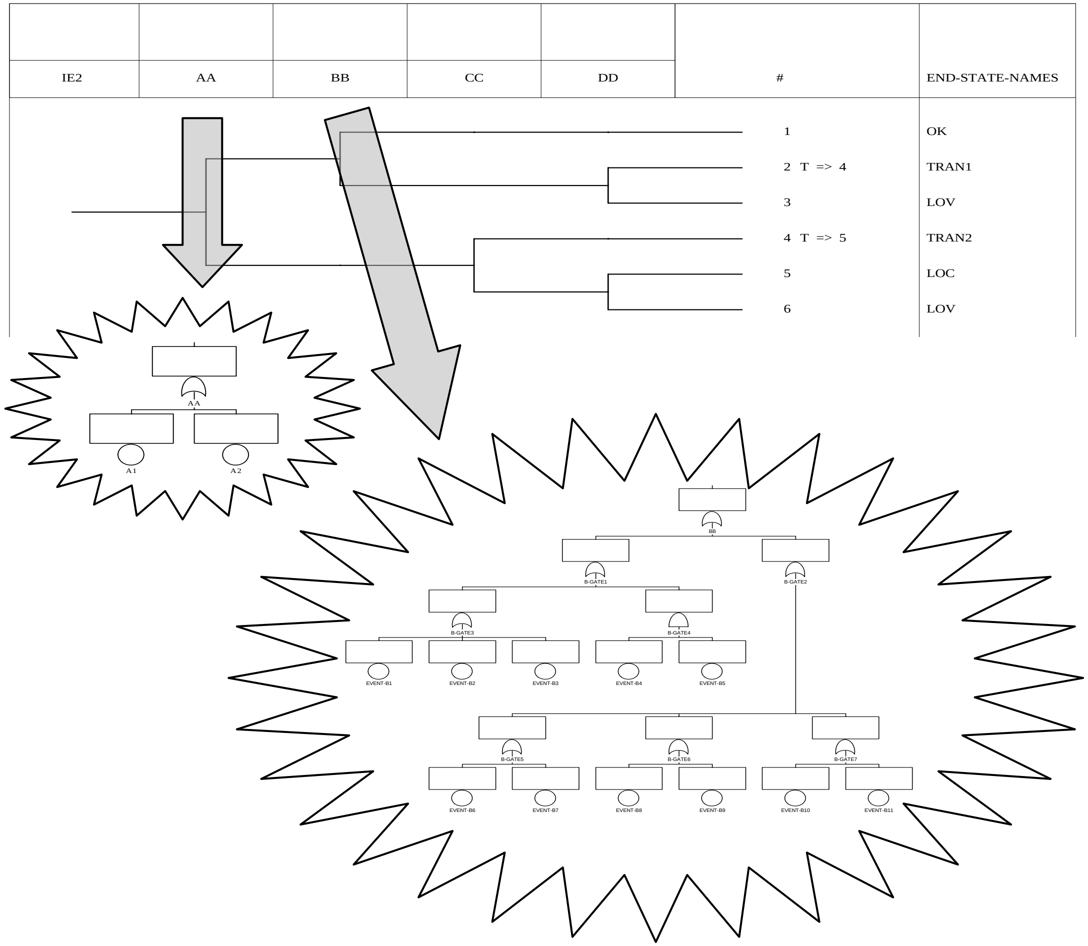
	Median	EF
Errors of commission	$3x10^{-3}$	3
Errors of omission	10^{-3}	5

A.D. Swain and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,* Report NUREG/CR 1278, US Nuclear Regulatory Commission, 1983.

Post-IE Errors

- Models still being developed.
- Typically, they include detailed task analyses, identification of performance shaping factors (PSFs), and the subjective assessment of probabilities.
- PSFs: System design, facility safety culture, organizational factors, stress level, others.

Risk Models

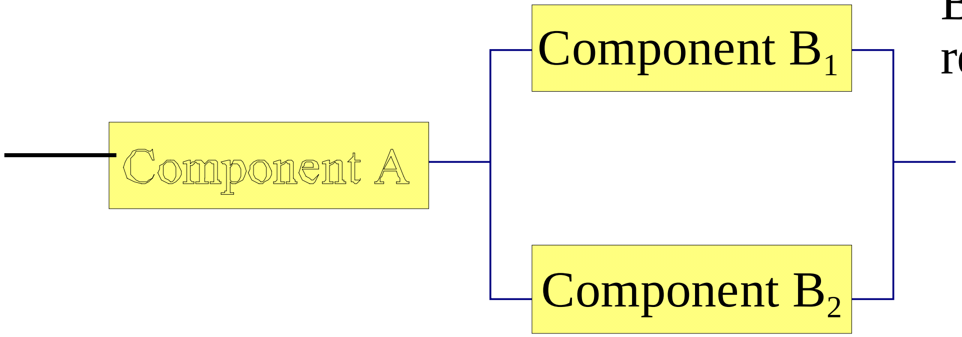


IE2	AA	BB	CC	DD	#	END-STATE-NAMES
					1	OK
					2 T => 4	TRAN1
					3	LOV
					4 T => 5	TRAN2
					5	LOC
					6	LOV

System Analysis

- What components constitute the system?
- How do the components and system operate?
- How does the system interact with other systems?
- What functions does the system perform?
- How does the system fail? (NOTE: The event tree determines the boundary conditions)
  - Hardware
  - Software
  - Human errors
- What external events is the system susceptible to?

Dependent Failures: An Example



B_1 and B_2 are identical redundant components

System Logic	$X_S = X_A + X_{B1} X_{B2} - X_A X_{B1} X_{B2}$
Failure Probability	$P(\text{fail}) = P(X_A) + P(X_{B1} X_{B2}) - P(X_A X_{B1} X_{B2})$

Example (cont'd)

- In general, we cannot assume independent failures of B_1 and B_2. This means that

$$P(X_{B1}\, X_{B2}) \geq P(X_{B1})\, P(X_{B2})$$

- How do we evaluate these dependencies?

Dependencies

- **Some dependencies are modeled explicitly, e.g., fires, missiles, earthquakes.**

- **After the explicit modeling, there is a class of causes of failure that are treated as a group. They are called *common-cause failures*.**

Special Issue on Dependent Failure Analysis, *Reliability Engineering and System Safety*, vol. 34, no. 3, 1991.

Expanding the set of failure causes

- The complete set of basic events involving component A in a three-component system is:

A_I = *Independent failure of component A.*

C_{AB} = *Failure of components A and B (and not C) from common causes.*

C_{AC} = *Failure of components A and C (and not B) from common causes.*

C_{ABC} = *Failure of components A, B, and C from common causes.*

Component Failure

- The equivalent Boolean representation of total failure of component A is

$$A = A_I + C_{AB} + C_{AC} + C_{ABC}$$

or

$$X_A = 1 – (1- X_I)(1- X_{AB})(1- X_{AC})(1- X_{ABC})$$

Minimal Cut Sets

- **The minimal cut sets of the expanded fault tree are:**

$$\{A_I,B_I\};\ \{A_I,C_I\};\ \{B_I,C_I\};\ \{C_{AB}\};\ \{C_{AC}\};$$

$$\{C_{BC}\};\ \{C_{ABC}\}$$

Calculating Probabilities

- Using the rare event approximation, the system failure probability of a two-out-of-three system is given by

$$P(S) = P(A_I)\ P(B_I) + P(A_I)\ P(C_I) + P(B_I)\ P(C_I) +$$

$$P(C_{AB}) + P(C_{AC}) + P(C_{BC}) + P(C_{ABC})$$

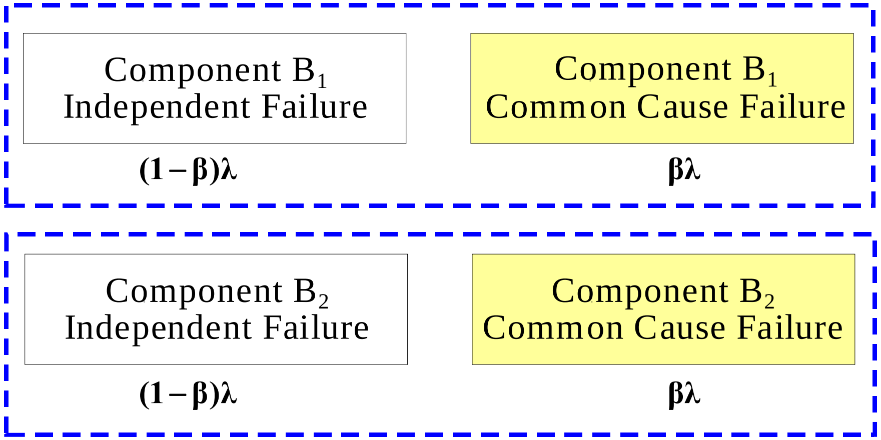
The Beta-Factor Model

- The β -factor model assumes that common-cause events always involve failure of all components of a common cause component group

- It further assumes that

$$\beta = \frac{\lambda_{\mathbf{CCF}}}{\lambda_{\mathbf{total}}}$$

β - Factor Model (cont’d)



Component B_1 Independent Failure

$(1-\beta)\lambda$

Component B_1 Common Cause Failure

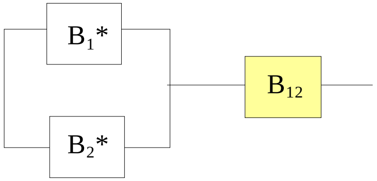
$\beta\lambda$

Component B_2 Independent Failure

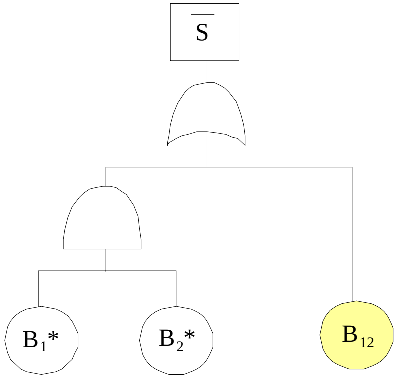
$(1-\beta)\lambda$

Component B_2 Common Cause Failure

$\beta\lambda$



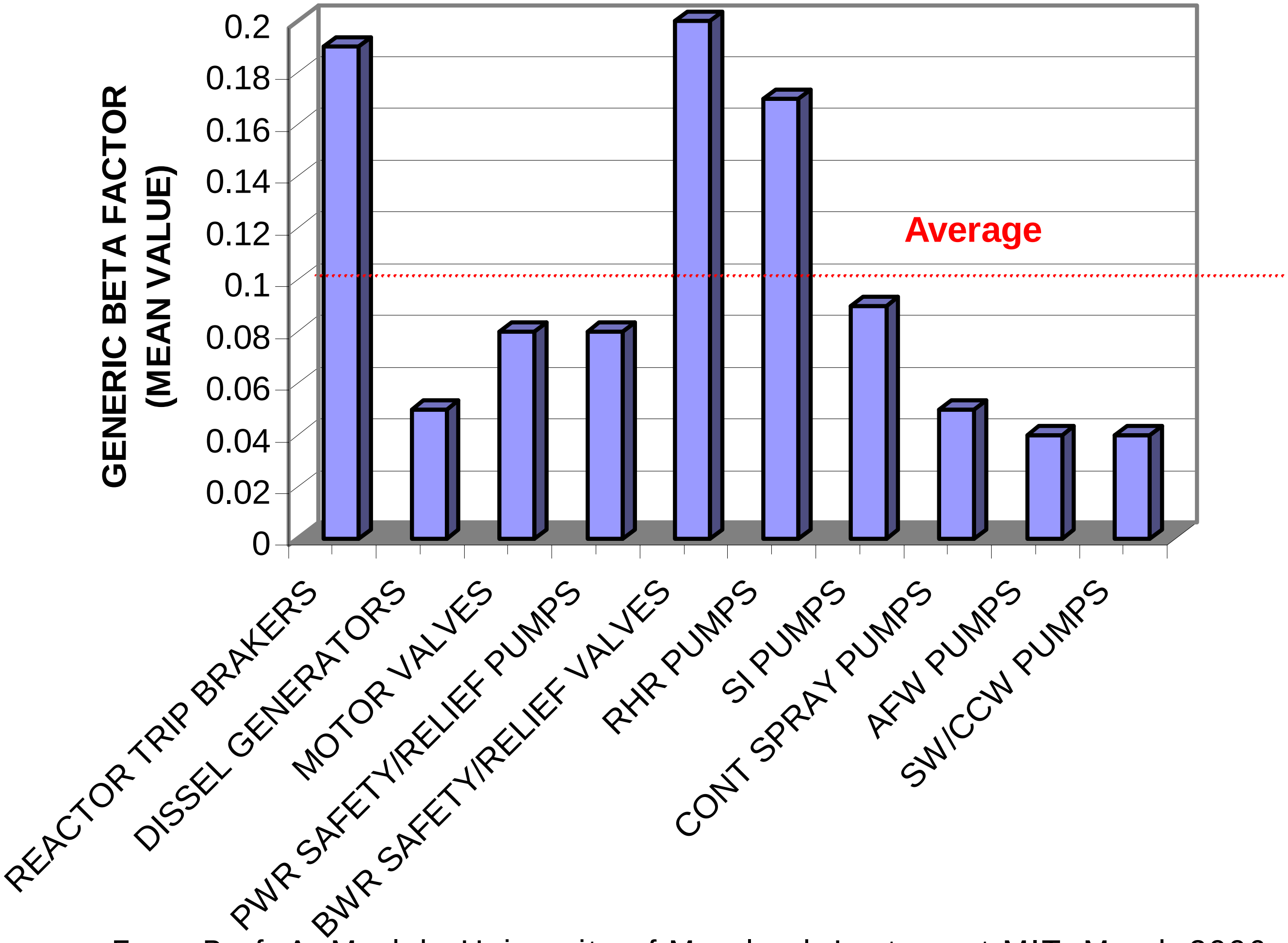
Reliability Block Diagram



Fault Tree

From Prof. A. Mosleh, University of Maryland. Lecture at MIT, March 2006.
Courtesy of A. Mosleh. Used with permission.

Generic Beta Factors

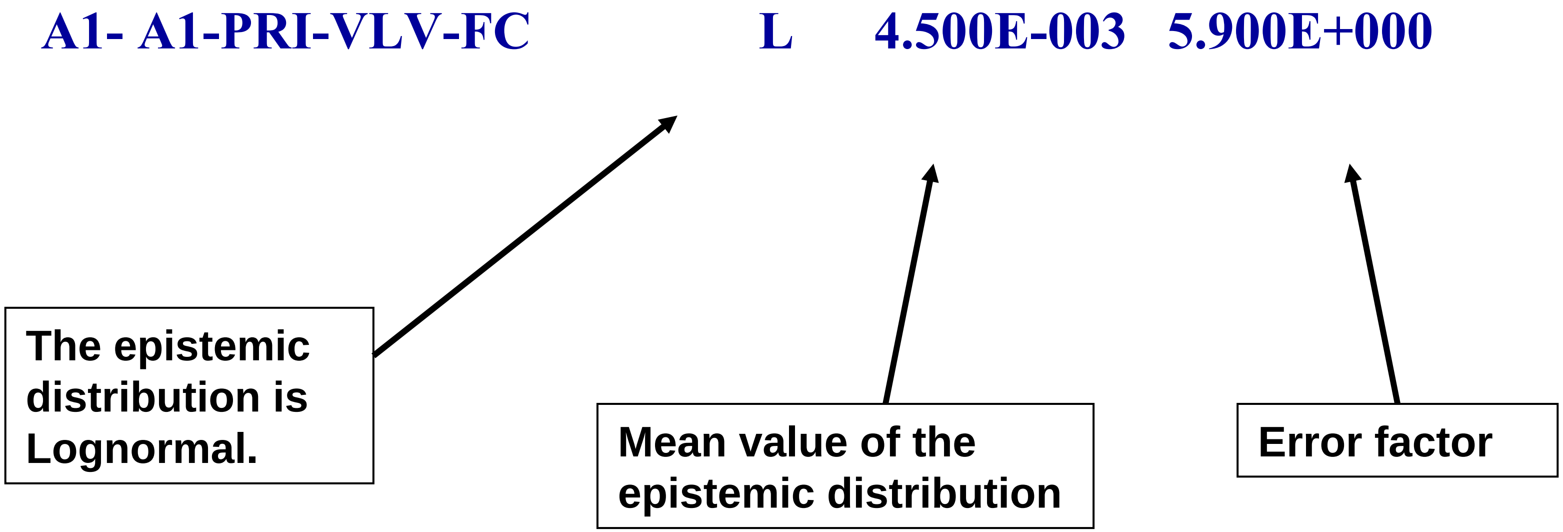


From Prof. A. Mosleh, University of Maryland. Lecture at MIT, March 2006. Courtesy of A. Mosleh. Used with permission.

Space Shuttle Orbiter Dependent Failure Data Collection, Analysis, and Results

- **474 Space Shuttle orbiter in-flight anomaly reports analyzed.**
- **Data used to:**
  - ***Determine frequency and types of dependent failures, causes, and defenses associated with spacecraft***
  - ***Estimate a beta factor of 0.13.***

Data



A1- A1-PRI-VLV-FC L 4.500E-003 5.900E+000

The epistemic distribution is Lognormal.

Mean value of the epistemic distribution

Error factor

Data Analysis

- The process of collecting and analyzing information in order to estimate the parameters of the epistemic PRA models.

- Typical quantities of interest are:
  - Initiating Events Frequencies
  - Component Failure Frequencies
  - Component Test and Maintenance Unavailability
  - Common-Cause Failure Probabilities
  - Human Error Rates

Sources of Information

- Ideally parameters of PRA models of a specific system should be estimated based on test and/or operational data of that system.

- Often, however, the analysis has to rely on a number of other sources and types of information as the quantity or availability of system-specific data are insufficient.

- In such cases surrogate data, generic information, or expert judgment are used directly or in combination with (limited) system-specific data.

Data Sources

- **Generic**
    - **IEEE Standard 500**
    - **Reliability Analysis Center**
    - **MIL-Std 217**
    - **Offshore Reliability Data Project**
    - **T-Book**
- **System-specific**
    - ***Maintenance Logs***
    - ***Test Logs***
    - ***Operation Records***

Data Needs

- The type of data needed varies depending on the type of event and their specific parametric representation

- Probabilities typically require
  - *Event Counts (e.g., Number of Failure)*
  - *Exposure, or “Success Data” (e.g., Total Operating Time)*

- Other parameters may require only one type of data
  - *Maintenance/Repair Duration*
  - *Counts of Multiple Failures (CCFs)*

Bayesian Estimation

- Two main steps:
  - The first step involves using available information fit a subjective, or prior, distribution to a parameter, such as a failure rate. The uncertainties in the parameter values are expressed in the prior distribution.
  - The second step involves using additional or new data to update an existing prior distribution using Bayes' Theorem.

Updating Epistemic Distributions

- Bayes' Theorem allows us to incorporate new evidence into the epistemic distribution.

$$\pi'(\lambda / E) = \frac{L(E / \lambda)\pi(\lambda)}{\int L(E / \lambda)\pi(\lambda)d\lambda}$$

The Quantification of Judgment

- **Where does the epistemic distribution $\pi(\lambda)$ come from?**
- **Both substantive and normative "goodnesses" are required.**
- **Direct assessments of parameters like failure rates should be avoided.**
- **A reasonable measure of central tendency to estimate is the median.**
- **Upper and lower percentiles can also be estimated.**

SEABROOK STATION RISK RESULTS

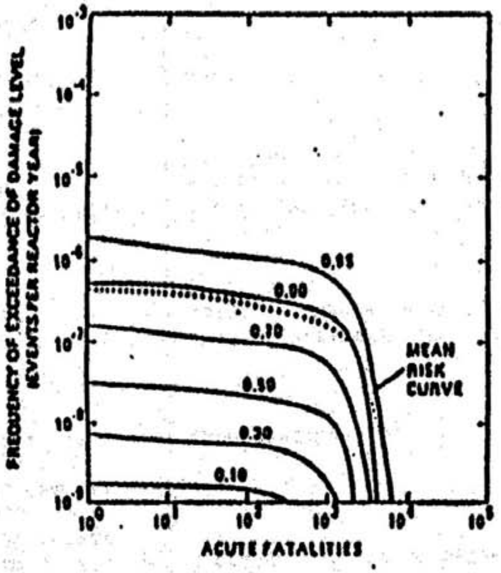


FIGURE 1-1a. RISK OF EARLY FATALITIES

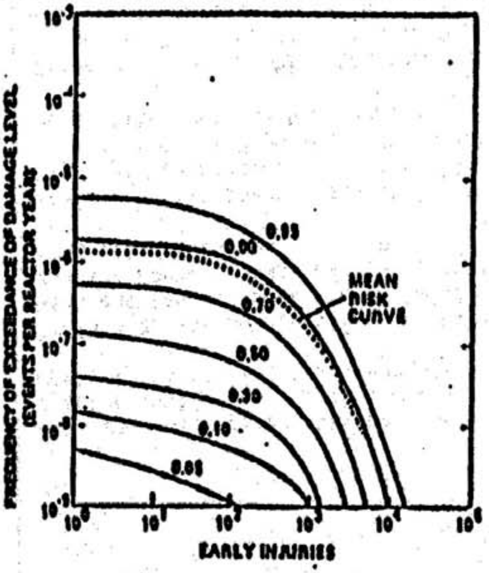


FIGURE 1-1b. RISK OF INJURIES

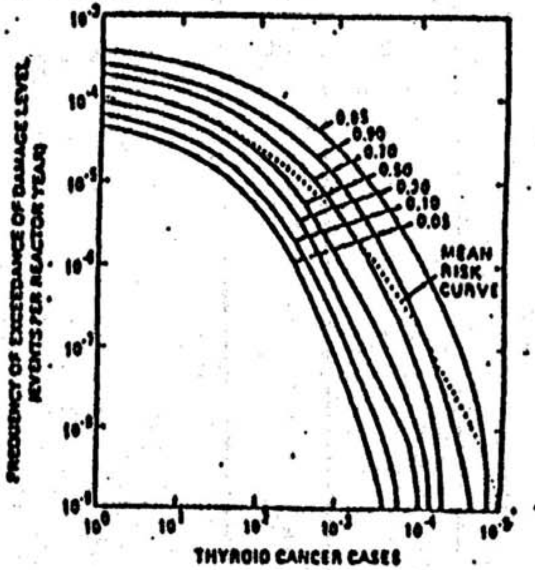


FIGURE 1-1c. RISK OF THYROID CANCER CASES

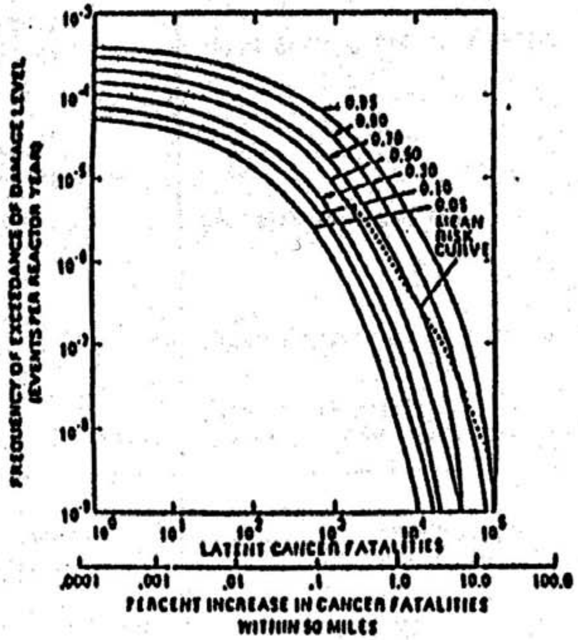


FIGURE 1-1d. RISK OF LATENT CANCER FATALITIES (OTHER THAN FATAL THYROID CANCERS)

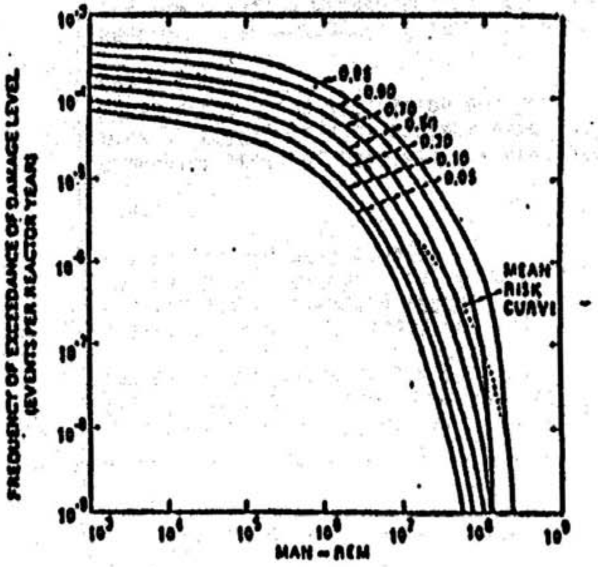


FIGURE 1-1e. RISK OF MAN-REM

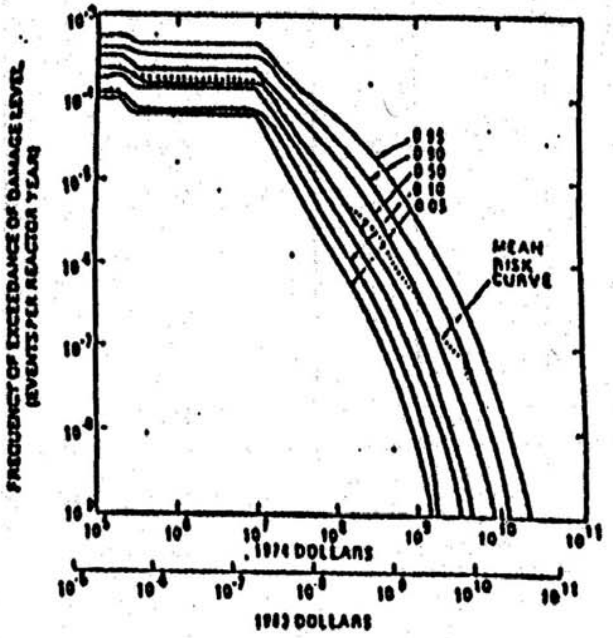


FIGURE 1-1f. RISK OF PROPERTY DAMAGE AND EVACUATION COSTS

Courtesy of K. Kiper. Used with permission.