PRA Methodology Overview

22.39 Elements of Reactor Design, Operations, and Safety

Lecture 9

Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology
PRA Synopsis

Figure removed due to copyright restrictions.
Futron Corp., International Space Station PRA, Dec. 2000
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 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

Excessive Release of Non-Core Material

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

Excessive Offsite Release
NPP: Initiating Events

• Transients
  – Loss of offsite power
  – Turbine trip
  – Others

• Loss-of-coolant accidents (LOCAs)
  – Small LOCA
  – Medium LOCA
  – Large LOCA
ILLUSTRATION EVENT TREE: Station Blackout Sequences

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
LOSP Distribution

Epistemic Uncertainties

- 5th: 0.005/yr (200 yr)
- Median: 0.040/yr (25 yr)
- Mean: 0.070/yr (14 yr)
- 95th: 0.200/yr (5 yr)

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
Offsite Power Recovery Curves

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
STATION BLACKOUT EVENT TREE

Courtesy of U.S. NRC.

Department of Nuclear Science and Engineering
NPP: Loss-of-offsite-power event tree

<table>
<thead>
<tr>
<th>LOOP</th>
<th>Secondary Heat Removal</th>
<th>Bleed &amp; Feed</th>
<th>Recirc.</th>
<th>Core</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PDSi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PDSj</td>
</tr>
</tbody>
</table>

Department of Nuclear Science and Engineering
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.
Reason’s Categories

Unsafe acts
- Unintended action
  - Slip
  - Lapse
  - Mistake
- Intended violation
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

- Fallible Decisions
- Line Management Deficiencies
- Psychological Precursors
- Unsafe Acts

**Pre-IE ("routine") actions**

<table>
<thead>
<tr>
<th></th>
<th>Median</th>
<th>EF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors of commission</td>
<td>$3 \times 10^{-3}$</td>
<td>3</td>
</tr>
<tr>
<td>Errors of omission</td>
<td>$10^{-3}$</td>
<td>5</td>
</tr>
</tbody>
</table>

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 culture, organizational factors, stress level, others.
The ATHEANA Framework

Plant Design, Operations and Maintenance

Error-Forcing Context

Performance Shaping Factors

Human Error

Error Mechanisms

Unsafe Actions

PRA Logic Models

Human Failure Events

Scenario Definition

Plant Conditions

Risk Management Decisions

The ATHEANA Framework


Department of Nuclear Science and Engineering

20
## Risk Models

<table>
<thead>
<tr>
<th>IE2</th>
<th>AA</th>
<th>BB</th>
<th>CC</th>
<th>DD</th>
<th>#</th>
<th>END-STATE-NAMES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>T == 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>LOV</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>T == 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>TRAN2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
<td>LOC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LOV</td>
</tr>
</tbody>
</table>

![Diagram of risk models with states and transitions]
FEED & BLEED COOLING DURING LOOP 1-OF-3 SI TRAINS AND 2-OF-2 PORVVS FOR SUCCESS

Courtesy of U.S. NRC.
HIGH PRESSURE INJECTION DURING LOOP 1-0F-3 TRAINS FOR SUCCESS

Department of Nuclear Science and Engineering

Courtesy of U.S. NRC.
Cut sets and minimal cut sets

- **CUT SET**: Any set of events (failures of components and human actions) that cause system failure.

- **MINIMAL CUT SET**: A cut set that does not contain another cut set as a subset.
Important Note: \( X^k = X, \quad k: 1, 2, \ldots \)

### Indicator Variables

\[
X_j = \begin{cases} 
1, & \text{If } E_j \text{ is } T \\
0, & \text{If } E_j \text{ is } F 
\end{cases}
\]

**Venn Diagram**
\[ X_T = \phi(X_1, X_2, \ldots X_n) \equiv \phi(X) \]

\( \phi(X) \) is the **structure or switching function**. It maps an \( n \)-dimensional vector of 0s and 1s onto 0 or 1.

**Disjunctive Normal Form:**

\[ X_T = 1 - \prod_{i=1}^{N} (1 - M_i) \equiv \bigcap_{i=1}^{N} M_i \]

**Sum-of-Products Form:**

\[ X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i \]
**Dependent Failures: An Example**

Component B₁ and B₂ are identical redundant components.

MCS: \( M₁ = \{Xₐ\} \quad M₂ = \{X_{B₁}, X_{B₂}\} \)

| System Logic | \( Xₛ = 1 - (1 - Xₐ)(1 - X_{B₁}X_{B₂}) = \)  
|              | \( = Xₐ + X_{B₁}X_{B₂} - XₐX_{B₁}X_{B₂} \) |
| Failure Probability | \( P(\text{fail}) = P(Xₐ) + P(X_{B₁}X_{B₂}) - P(XₐX_{B₁}X_{B₂}) \) |
Example (cont’d)

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

\[ P(X_{B_1} X_{B_2}) \geq P(X_{B_1}) P(X_{B_2}) \]

• 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.

The Beta-Factor Model

- The $\beta$-factor model assumes that common-cause events always involve failure of all components of a common cause component group.

- It further assumes that

$$\beta = \frac{\lambda_{CCF}}{\lambda_{total}}$$
Generic Beta Factors

![Bar Chart: Generic Beta Factors](image)

- Reactor Trip Brakers
- Diesel Generators
- Motor Valves
- PWR Safety/Relief Valves
- BWR Safety/Relief Valves
- RHR Pumps
- SI Pumps
- Cont Spray Pumps
- AFW Pumps
- SW/CCW Pumps

Average
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 Event Frequencies
  - Component Failure Frequencies
  - Component Test and Maintenance Unavailability
  - Common-Cause Failure Probabilities
  - Human Error Rates
General Formulation

\[ X_T = \varphi(X_I, \ldots X_n) \equiv \varphi(X) \]

\[ X_T = 1 - \prod_{1}^{N} (1 - M_i) \equiv \bigcup_{1}^{N} M_i \]

\[ X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i \]

\( X_T \) : the TOP event indicator variable (e.g., core melt, system failure)

\( M_i \) : the \( i^{th} \) minimal cut set (for systems) or accident sequence (for core melt, containment failure, et al)
TOP-event Probability

\[ P(X_T) = \sum_{i=1}^{N} P(M_i) + \ldots + (-1)^{N+1} P \left( \prod_{i=1}^{N} M_i \right) \]

\[ P(X_T) \approx \sum_{i=1}^{N} P(M_i) \] Rare-event approximation

The question is how to calculate the probability of \( M_i \)

\[ P(M_i) = P(X^i_k \ldots X^i_m) \]
## RISK-SIGNIFICANT INITIATING EVENTS

<table>
<thead>
<tr>
<th>Risk-Significant Initiating Event</th>
<th>Period</th>
<th>Number of Events</th>
<th>Mean Frequency</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Transients</td>
<td>1998 – 2004</td>
<td>2120</td>
<td>7.57E-1</td>
<td>↓</td>
</tr>
<tr>
<td>BWR General Transients</td>
<td>1997 – 2004</td>
<td>699</td>
<td>8.56E-1</td>
<td>↓</td>
</tr>
<tr>
<td>PWR General Transients</td>
<td>1998 – 2004</td>
<td>1421</td>
<td>7.10E-1</td>
<td>↓</td>
</tr>
<tr>
<td>Loss of Instrument Air (BWR)</td>
<td>1994 – 2004</td>
<td>19</td>
<td>7.60E-3</td>
<td>↓</td>
</tr>
<tr>
<td>Stuck Open SRV (BWR)</td>
<td>1993 – 2004</td>
<td>14</td>
<td>2.07E-2</td>
<td>←</td>
</tr>
<tr>
<td>Stuck Open SRV (PWR)</td>
<td>1988 – 2004</td>
<td>2</td>
<td>2.30E-3</td>
<td>←</td>
</tr>
<tr>
<td>Steam Generator Tube Rupture</td>
<td>1988 – 2004</td>
<td>3</td>
<td>3.48E-3</td>
<td>←</td>
</tr>
</tbody>
</table>
INITIATING EVENT TRENDS

**PWR General Transients**

**BWR General Transients**

**PWR Loss of Heat Sink**

**BWR Loss of Heat Sink**

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.

Department of Nuclear Science and Engineering
INITIATING EVENTS INSIGHTS

- Most initiating events have decreased in frequency over past 10 years.
- Combined initiating event frequencies are 4 to 5 times lower than values used in NUREG-1150 and IPEs.
- General transients constitute majority of initiating events; more severe challenges to plant safety systems are about one-quarter of events.

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.
LOOP FREQUENCY INSIGHTS

• Overall LOOP frequency during critical operation has decreased over the years (from 0.12/ry to 0.036/ry)
• Average LOOP duration has increased over the years:
  – Statistically significant increasing trend for 1986–1996
  – Essentially constant over 1997–2004
• 24 LOOP events between 1997 and 2004; 19 during the “summer” period
• No grid-related LOOP events between 1997 and 2002; 13 in 2003 and 2004
• Decrease in plant-centered and switchyard-centered LOOP events; grid events are starting to dominate
## System Reliability Study Results

<table>
<thead>
<tr>
<th>STUDY</th>
<th>Mean Unreliability</th>
<th>Unplanned Demand Trend</th>
<th>Failure Rate Trend</th>
<th>Unreliability Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDG (1997–2004)</td>
<td>2.18E-2</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

P. Baranowsky, RIODM Lecture, MIT, 2006

Department of Nuclear Science and Engineering

Courtesy of P. Baranowsky. Used with permission.
PWR SYSTEM RELIABILITY STUDIES

EDG Unavailability (FTS)

AFW Unavailability (FTS)

HPI Unreliability (8 hr mission)

AFW Unreliability (8 hr mission)

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.

Department of Nuclear Science and Engineering
PWR SYSTEM INSIGHTS

• **EDG**
  – EDG start reliability much improved over past 10 years.
  – Failure-to-run rates lower than in most PRAs.

• **AFW**
  – Industry average reliability consistent with or better than Station Blackout and ATWS rulemaking.
  – Wide variation in plant specific AFW reliability primarily due to configuration.
  – Failure of suction source identified as a contributor (not directly modeled in some PRAs).

• **HPI**
  – Wide variation in plant specific HPI reliability due to configuration.
  – Various pump failures are the dominant failure contributor.
BWR SYSTEM RELIABILITY STUDIES

HPCI Unreliability (8 hr mission)

RCIC Unavailability (FTS)

HPCS Unreliability (8 hr mission)

RCIC Unreliability (8 hr mission)

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.

Department of Nuclear Science and Engineering
• **HPCI**
  – Industry-wide unreliability shows a statistically significant decreasing trend.
  – Dominant Failure: failure of the injection valve to reopen during level cycling.

• **HPCS**
  – Industry average unreliability indicates a constant trend.
  – Dominant Failure: failure of the injection valve to open during initial injection.

• **RCIC**
  – Industry average unreliability indicates a constant trend.
  – Dominant Failure: failure of the injection valve to reopen during level cycling.
COMMON-CAUSE FAILURE (CCF) EVENTS

• Criteria for a CCF Event:
  – Two or more components fail or are degraded at the same plant and in the same system.
  – Component failures occur within a selected period of time such that success of the PRA mission would be uncertain.
  – Component failures result from a single shared cause and are linked by a coupling mechanism such that other components in the group are susceptible to the same cause and failure mode.
  – Equipment failures are not caused by the failure of equipment outside the established component boundary.
CCF OCCURRENCE RATE

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.
Coupling Factors - Complete CCF Events

- Environment: 14.2%
- Operations: 13.7%
- Maintenance: 28.8%
- Hardware: 43.4%

P. Baranowsky, RIODM Lecture, MIT, 2006

Courtesy of P. Baranowsky. Used with permission.