9. Sequence Quantification
Sequence Quantification

- **Purpose:** This topic will provide students with an understanding of the quantitative basis of PRA. Elements of accident sequence quantification and importance analysis will be presented.

- **Objectives:** At the conclusion, students will be able to:
  - Describe the major processes for accident sequence quantification
  - Explain the concepts of importance analysis

- **References:** NUREG/CR-2300, NUREG-1489 (App. C)
Quantification Inputs

- Initiating events and frequencies
- Event trees to define accident sequences
- Fault trees and Boolean expressions for all systems (front line and support)
- Data (component failures and human errors)
Parameter Inputs for Sequence Quantification

- Initiating event frequencies
  \[ \lambda_{IE} \]
- Demand failures
  \[ Q_d = p \]
- Mission time failures (failure to run)
  \[ Q_r \approx \lambda_h t_m \]
- Standby failures
  \[ Q_s \approx \lambda_s t_f/2 \]
- Test and maintenance unavailability
  \[ Q_m = \lambda_m d_m \]
- Common-cause parameters
  \[ \beta \]
Fault-Tree Linking Approach to Accident Sequence Quantification

- Link fault tree models on sequence level using event trees
- Evaluate each sequence for minimal cut sets (Boolean reduction)
- Quantify sequence minimal cut sets with data
- Add operator recovery actions and common cause failures
- Determine dominant accident sequences
- Place in plant damage state bins
- Perform sensitivity, importance, and uncertainty analysis
Example of Quantification Process

Let's look at Sequence TBC
Example of Quantification Process (cont.)

\[ T = \frac{10 \text{ transients (demands)}}{\text{year}} \]
Example of Quantification Process (cont.)

Systems B AND C Fail = System B Fails * System C Fails

= (Pump 1 + Valve X) * (Pump 1 * Pump 2)

= (Pump 1 * Pump 1 * Pump 2) + (Valve X * Pump 1 * Pump 2)

= (Pump 1 * Pump 2) + (Valve X * Pump 1 * Pump 2)

= Pump 1 * Pump 2

= (1E-3) (1E-3)

= 1E-6 (Probability)

Sequence TBC = T * System B Fails * System C Fails

= 10/Year * 1E-6

= 1E-5/Year (Frequency)
Recovery Analysis

• Analysis on accident sequence level
  ✷ Examination of contributors to failure
  ✷ Identification of potential for recovery

• Recovery factors
  ✷ Critical time for recovery
  ✷ Action required
  ✷ Time for action
  ✷ Time versus probability of recovery

• Final accident sequence frequency includes recovery
Summary of Sequence $T_2L_1P_1$

- This sequence is initiated by a loss of main feedwater ($T_2$), followed by failure of the auxiliary feedwater (AFW) system, and failure of feed and bleed cooling due to the inability to open both power operated relief valves (PORVs).

- The loss of main feedwater initiator places a demand on auxiliary feedwater to remove core decay heat. Failure of the AFW system causes a demand for feed and bleed cooling. Failure to initiate feed and bleed and various failures which prevent one of the two PORVs from opening contribute to this sequence. Success criteria require that two PORVs open for successful feed and bleed.

- The dominant contributors to AFW failure are common cause failure of the air-operated steam generator level control valves and the common cause failure of all three AFW pumps due to steam binding. The dominant contributor to failure of feed and bleed is operator failure to open PORVs, followed by mechanical failures of the PORV block valves and PORVs.
Event Tree for $T_2$ - Loss of Main Feedwater

<table>
<thead>
<tr>
<th>Initiator</th>
<th>RPS</th>
<th>RVC</th>
<th>AFW</th>
<th>SIF</th>
<th>CCW</th>
<th>HPI</th>
<th>PRV</th>
<th>LPI/ LPR</th>
<th>HPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_2$</td>
<td>K</td>
<td>$Q_1$</td>
<td>$L_1$</td>
<td>$D_3$</td>
<td>$W$</td>
<td>$D_1$</td>
<td>$P_1$</td>
<td>$H_3$</td>
<td>$H_2$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STATUS</th>
<th>SEQUENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>$T_2D_3W$</td>
</tr>
<tr>
<td>OK</td>
<td>$T_2L_1H_2$</td>
</tr>
<tr>
<td>CD</td>
<td>$T_2L_1H_3$</td>
</tr>
<tr>
<td>CD</td>
<td>$T_2L_1P_1$</td>
</tr>
<tr>
<td>CD</td>
<td>$T_2L_1D_1$</td>
</tr>
<tr>
<td>CD</td>
<td>$T_2Q$</td>
</tr>
<tr>
<td>CD</td>
<td>$T_2K$</td>
</tr>
</tbody>
</table>

- Seal LOCA vulnerable - Go to Seal LOCA Tree
- Stuck-Open PORV - Go to $S_2$
- ATWS - Go to ATWS Tree
## Identifiers for $T_2$ Event Tree

<table>
<thead>
<tr>
<th>Event Identifier</th>
<th>Description</th>
<th>System Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>D_1</td>
<td>Failure of charging pump system with 1 of 4 success requirements</td>
<td>HPI</td>
</tr>
<tr>
<td>D_3</td>
<td>Failure of charging pump system in seal injection flow mode</td>
<td>SIF</td>
</tr>
<tr>
<td>H_2</td>
<td>Failure of charging pump system in the high pressure recirculation mode</td>
<td>HPR</td>
</tr>
<tr>
<td>H_3</td>
<td>Failure of low pressure injection/recirculation</td>
<td>LPI/LPR</td>
</tr>
<tr>
<td>K</td>
<td>Failure of reactor protection system</td>
<td>RPS</td>
</tr>
<tr>
<td>L_1</td>
<td>Failure of auxiliary feedwater required for transients with reactor trip</td>
<td>AFW</td>
</tr>
<tr>
<td>P_1</td>
<td>Failure of both pressurizer PORVs to open for feed &amp; bleed</td>
<td>PRV</td>
</tr>
<tr>
<td>Q_1</td>
<td>Failure of any relief valve to reclose</td>
<td>RVC</td>
</tr>
<tr>
<td>W</td>
<td>Failure of component cooling water to the thermal barrier of all reactor coolant pumps</td>
<td>CCW</td>
</tr>
</tbody>
</table>
Dominant Contributors to Sequence $T_2L_1P_1$

### Minimal Cut Set

<table>
<thead>
<tr>
<th>Cut Set</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_2 \cdot AFW-AOV-CC \cdot BETA-8AOV \cdot HPI-XHE-FO-FDBLD</td>
<td>5.4E-7</td>
</tr>
<tr>
<td>$T_2 \cdot STEAM-BINDING \cdot HPI-XHE-FO-FDBLD</td>
<td>1.6E-7</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-AOV-CC \cdot BETA-8AOV \cdot PPS-SOV-FT-334</td>
<td>1.6E-7</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-AOV-CC \cdot BETA-8AOV \cdot PPS-SOV-FT-340A</td>
<td>1.6E-7</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-TDP-FS-1AS6 * AFW-MDP-FS * BETA-AFW \cdot HPI-XHE-FO-FDBLD</td>
<td>8.0E-8</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-TDP-FR-1AS6H * AFW-MDP-FS * BETA-AFW \cdot HPI-XHE-FO-FDBLD</td>
<td>8.0E-8</td>
</tr>
<tr>
<td>$T_2 \cdot STEAM-BINDING \cdot PPS-SOV-FT-334</td>
<td>4.6E-8</td>
</tr>
<tr>
<td>$T_2 \cdot STEAM-BINDING \cdot PPS-SOV-FT-340A</td>
<td>4.6E-8</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-ACT-FA-TRNA \cdot AFW-ACT-FA-TRNB \cdot HPI-XHE-FO-FDBLD</td>
<td>4.1E-8</td>
</tr>
<tr>
<td>$T_2 \cdot AFW-TDP-TM-1AS6 * AFW-MDP-FS * BETA-AFW \cdot HPI-XHE-FO-FDBLD</td>
<td>2.7E-8</td>
</tr>
</tbody>
</table>

Total $T_2L_1P_1$: 1.3E-6
Term Descriptions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>T₂</td>
<td>Loss of main feedwater</td>
<td>7.2E-1/reactor year</td>
</tr>
<tr>
<td>STEAM-BINDING</td>
<td>Steam-binding of all AFWS pumps</td>
<td>1.0E-5</td>
</tr>
<tr>
<td>PPS-SOV-FT-334</td>
<td>PORV 334 fails to open</td>
<td>6.3E-3</td>
</tr>
<tr>
<td>PPS-SOV-FT-340A</td>
<td>PORV 340A fails to open</td>
<td>6.3E-3</td>
</tr>
<tr>
<td>AFW-TDP-FS-1AS</td>
<td>AFWS turbine pump fails to start</td>
<td>3.0E-2</td>
</tr>
<tr>
<td>AFW-TDP-FR-1AS6H</td>
<td>AFWS turbine pump fails to run 6 hours</td>
<td>3.0E-2</td>
</tr>
<tr>
<td>AFW-TDP-TM-1AS</td>
<td>AFWS turbine pump unavailable test and maintenance</td>
<td>1.0E-2</td>
</tr>
<tr>
<td>AFW-AOV-CC</td>
<td>AFWS AOV fails to open</td>
<td>1.0E-3</td>
</tr>
<tr>
<td>BETA-AFW</td>
<td>Common cause failure factor of 2 motor pumps</td>
<td>5.6E-2</td>
</tr>
<tr>
<td>BETA-8AOV</td>
<td>Common cause failure factor of 8 AOVs</td>
<td>3.4E-2</td>
</tr>
<tr>
<td>AFW-MDP-FS</td>
<td>AFWS motor pump fails to start</td>
<td>3.0E-3</td>
</tr>
<tr>
<td>HPI-XHE-FO-FDBLD</td>
<td>Operator fails to initiate feed and bleed</td>
<td>2.2E-2</td>
</tr>
<tr>
<td>AFW-ACT-FA-TRNA</td>
<td>AFWS Train A actuation fails</td>
<td>1.6E-3</td>
</tr>
<tr>
<td>AFW-ACT-FA-TRNB</td>
<td>AFWS Train B actuation fails</td>
<td>1.6E-3</td>
</tr>
</tbody>
</table>
Importance Measures

• Provide quantitative perspective on dominant contributors to risk and sensitivity of risk to changes in input values

• Usually calculated at core damage frequency level

• Three are encountered most commonly:
  ✧ Fussell-Vesely
  ✧ Risk Reduction
  ✧ Risk Increase or Risk Achievement
Fussell-Vesely Importance

- Measures overall contribution of an event to risk (CDF)
- Calculated by adding up frequencies of cutsets containing event of interest and dividing by total CDF
  \[ FV_x = \frac{\sum \text{Cutsets with event } x}{F(x)} \]
  or
  \[ FV_x = \frac{[F(x) - F(0)]}{F(x)} \]
  where,
  \( F(x) \) is risk with event \( x \) at nominal failure probability, and
  \( F(0) \) is risk when event \( x \) is never failed (failure probability = 0)
- Range is from 0 to 1
Consider these minimal cut sets:

\[ A = 6 \times 10^{-4} \]
\[ B = 1 \times 10^{-2} \times 3 \times 10^{-3} = 3 \times 10^{-5} \]
\[ C \times D = 3 \times 10^{-3} \times 1 \times 10^{-3} = 3 \times 10^{-6} \]

\[ F(X) = 6.33 \times 10^{-4} \]

where,

\[ A = 6 \times 10^{-4} \]
\[ B = 1 \times 10^{-2} \]
\[ C = 3 \times 10^{-3} \]
\[ D = 1 \times 10^{-3} \]

- Fussell-Vesely Importance

\[ F_{V_A} = \frac{6.0 \times 10^{-4}}{6.33 \times 10^{-4}} = 0.948 \]
\[ F_{V_B} = \frac{3.0 \times 10^{-5}}{6.33 \times 10^{-4}} = 0.047 \]
\[ F_{V_C} = \frac{3.3 \times 10^{-5}}{6.33 \times 10^{-4}} = 0.052 \]
\[ F_{V_D} = \frac{3.0 \times 10^{-6}}{6.33 \times 10^{-4}} = 0.005 \]
Risk Reduction Importance

• Measures amount by which CDF would decrease if event’s failure probability were set to 0 (never fails)
• Calculated as either ratio or difference between baseline CDF and CDF with event failure probability at 0
  Ratio: \( RRR(x) = \frac{F(x)}{F(0)} \)
  Difference (or Interval): \( RRI(x) = F(x) - F(0) \)
  where,
  \( F(x) \) is risk with event \( x \) at nominal failure probability, and
  \( F(0) \) is risk when event \( x \) is never failed (failure probability = 0)
• Ratio - Range is from 1 to \( \infty \)
• Gives same ranking as Fussell-Vesely
• For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RRR significance criterion of 1.005
  ◯ Equivalent to Fussell-Vesely importance of 0.005
Risk Reduction Importance (cont.)

- Consider these minimal cut sets:
  \[ A = 6 \times 10^{-4} \]
  \[ B \times C = 1 \times 10^{-2} \times 3 \times 10^{-3} = 3 \times 10^{-5} \]
  \[ C \times D = 3 \times 10^{-3} \times 1 \times 10^{-3} = 3 \times 10^{-6} \]
  \[ F(x) = 6.33 \times 10^{-4} \]

where,
  \[ A = 6 \times 10^{-4} \]
  \[ B = 1 \times 10^{-2} \]
  \[ C = 3 \times 10^{-3} \]
  \[ D = 1 \times 10^{-3} \]

- Risk Reduction Ratio Importance
  \[ \text{RRR}_A = \frac{6.33 \times 10^{-4}}{3.3 \times 10^{-5}} = 19.18 \]
  \[ \text{RRR}_B = \frac{6.33 \times 10^{-4}}{6.03 \times 10^{-4}} = 1.05 \]
  \[ \text{RRR}_C = \frac{6.33 \times 10^{-4}}{6.00 \times 10^{-4}} = 1.06 \]
  \[ \text{RRR}_D = \frac{6.33 \times 10^{-4}}{6.30 \times 10^{-4}} = 1.00 \]
Risk Increase Importance

- Measures amount by which CDF would increase if event's failure probability were set to 1 (e.g., component taken out of service)
- Calculated as either ratio or difference between CDF with event failure probability at 1 and baseline CDF
  - Ratio: $\text{RAW}(x) \text{ or } \text{RIR}(x) = \frac{F(1)}{F(x)}$
  - Difference (or Interval): $\text{RII}(x) = F(1) - F(x)$
  where,
  - $F(x)$ is risk with event $x$ at nominal failure probability, and
  - $F(1)$ is risk when event $x$ is always failed (failure probability = 1)
- Ratio measure referred to as risk achievement worth (RAW)
- RAW - Range is $\geq 1$
- For Maintenance Rule (10 CFR 50.65), NUMARC Guide 93-01 (endorsed by NRC) uses a RAW significance criterion of 2
Risk Increase Importance (cont.)

- Consider these minimal cut sets:
  \[
  A = 6 \times 10^{-4} = 6 \times 10^{-4} \\
  B \times C = 1 \times 10^{-2} \times 3 \times 10^{-3} = 3 \times 10^{-5} \\
  C \times D = 3 \times 10^{-3} \times 1 \times 10^{-3} = 3 \times 10^{-6} \\
  F(x) = 6.33 \times 10^{-4}
  \]

where,
\[
A = 6 \times 10^{-4} \\
B = 1 \times 10^{-2} \\
C = 3 \times 10^{-3} \\
D = 1 \times 10^{-3}
\]

- Risk Achievement Worth Importance
\[
RAW_A = 1.0 / 6.33 \times 10^{-4} = 1579.78 \\
RAW_B = 3.603 \times 10^{-3} / 6.33 \times 10^{-4} = 5.69 \\
RAW_C = 1.16 \times 10^{-2} / 6.33 \times 10^{-4} = 18.33 \\
RAW_D = 3.63 \times 10^{-3} / 6.33 \times 10^{-4} = 5.73
\]
Limitations of Risk Importance Measures

- Numerical values can be affected by:
  - Exclusion of equipment from PRA model
  - Model truncation during quantification
  - Parameter values used for other events in model
  - Present configuration of plant (equipment that is already out for test/maintenance)
Core Damage Frequency and Number of Cutsets Sensitive to Truncation Limits

Number of cut sets (Y1)  Core damage frequency (Y2)

Truncation level

Core damage frequency
Truncation Limits Affect Importance Rankings

Number of Important Basic Events

Truncation Level

0 50 100 150 200 250 300 350

1E-07 1E-08 1E-09 1E-10

RRW > 1.005  RAW > 2
Limitations of Risk Importance Measures (cont.)

- Risk rankings are not always well-understood in terms of their issues and engineering interpretations.
- RAW provides indication of risk impact of taking equipment out of service but full impact may not be captured.
  - That is, taking component out of service for test and maintenance may increase likelihood of initiating event due to human error.
Other Considerations When Using Importance Measures

- F-V and RAW rankings can differ significantly when using different risk metrics
  - Such as, core damage frequency due to internal events versus external events, shutdown risk, etc.
- Individual F-V or RAW measures cannot be combined to obtain risk importance for combinations of events
  - Critical combinations can be extremely important due to failure of redundant components whereas individual components in one train may have low rankings
10. Accident Progression & Consequence Analysis
Accident Progression Analysis, Containment Response, Fission Product Transport, and Consequence Analysis

- **Purpose:** Students receive a brief introduction to accident progression (Level 2 PRA) and consequence analysis (Level 3 PRA).

- **Objectives:** At the conclusion of this topic, students will be able to:
  - List primary elements which comprise accident phenomenology
  - Explain how accident progression analysis is related to full PRA
  - Explain general factors involved in containment response
  - Explain general factors involved in fission product transport & consequences
  - Name the major computer codes used in accident process and consequence analysis

- **Reference:** NUREG/CR-2300, NUREG-1489 (App. C)
Principal Steps in PRA Process

Level 1
- Accident Frequencies
  - Plant Damage States

Level 2
- Accident Progression, Containment Loading, and Structure Response
  - Accident Progression Bins
    - Transport of Radioactive Material
      - Source Term Groups
        - Offsite Consequences
          - Consequence Measures

Level 3
- Risk Integration
Accident Progression Analysis

- There are 4 major steps in Accident Progression Analysis
  - 1. Develop the Accident Progression Event Trees (APETs)
  - 2. Perform structural analysis of containment
  - 3. Quantify APET issues
  - 4. Group APET sequences into accident progression bins
Schematic of Accident Progression Event Tree

Boundary Conditions:
Plant Damage States

Pressure in vessel
- System Setpoint
  - High
  - Intermediate
  - Low

Recovery of Core Prior to Vessel Breach

Recovery of injection
- Yes
- No

In-vessel Processes & Containment Impact

Hydrogen released?
- Yes
- No

Ex-vessel Processes & Containment Impact

Debris coolability
- Yes
- No

Final Outcome
- Late containment overpressure
  - Yes
  - No

Source: NUREG-1150
06/2002

PRA Basics for Regulatory Applications (P-105) 157
Containment Response

How does the containment system deal with physical conditions resulting from the accident?

- Pressure
- Heat sources
- Fission products
- Steam and water
- Hydrogen
- Other noncondensables
Elements in the Analysis of Radionuclide Behavior in the Reactor

- Input
  - Event times Thermal Hydraulic conditions
  - Radionuclide and structural material source term from the core
- Primary system transport, deposition, and release
- Containment transport, deposition, and release
- Output
  - Radionuclide releases to the environment
Computer codes used to model Accident Progression & Fission Product Behavior

- RELAP5/SCDAP - in-vessel behavior
- CONTAIN - containment behavior
- VICTORIA - fission product behavior
- Integrated, comprehensive codes
  - MAAP - industry code
  - MELCOR - NRC code
Fission Product Source Term Outcomes of Interest

- Fractions Released Outside Containment
  - Noble Gases
  - Iodine
  - Cesium - Rubidium
  - Tellurium - Antimony
  - Barium - Strontium
  - Ruthenium - Molybdenum - Rhenium - Technetium - Cobalt
  - Lanthanum and other rare earth metals

- Parameters for Consequence Model
  - Time of release
  - Duration of release
  - Warning time for evacuation
  - Elevation of release
  - Energy of release
Source Term Calculation Models

Integrated Deterministic Code (MELCOR)

- Point estimate radionuclide release calculations for scenarios important to risk
- Selected sensitivity calculations to explore uncertainties that can be modeled by the code

Parametric Source Term Code

- Point estimate radionuclide release calculations for scenarios less important to risk (simulation of source code package)
- Extensive sensitivity calculations to explore uncertainties that cannot be modeled by code package
Schematic of Parametric Source Term Algorithm

Containment release: late revolatilization
Containment release of CCl species
Late containment decontamination processes
Late release of iodine from water pools

Late revolatilization from vessel
Release from the vessel
In-vessel core release
High-pressure ejection release
Decontamination: suppression pool, sprays & other features
Release during core-concrete interaction

Other decon: pools, sprays, etc.

Early containment decontamination: deposition, etc.

Containment release of in-vessel species

PRA Basics for Regulatory Applications (P-105)
06/2002
Components of a Consequence Model

- Atmospheric transport and diffusion model
- Pathways models
- Dosimetry models
- Health effects model
- Other models:
  - Evacuation
  - Interdiction
  - Decontamination
  - Economic effects
Pathways to People

- Radiation from radionuclides in air
- Inhalation of radionuclides
- Radionuclides in food and water
- Radiation from radionuclides on ground
Consequences

- Population dose
- Acute effects
  - Number of fatalities, injuries, and illnesses occurring within one year due to initial exposure to radioactivity; nonlinear with dose equivalent
- Latent effects
  - Number of delayed effects and time of appearance as functions of dose for various organs; linear, no-threshold model typically used
Consequence Evaluation Models

- MACCS (MELCOR Accident Consequence Code System)
- Improved environmental transport, dosimetry, health effects, and economic cost models
- Improved wet deposition model for rainout
- Dependence of dry deposition velocity on particle size
- Multi-plume dispersion model including multi-step crosswind concentration profile
- Improved code architecture
Dominant Risk Contributors Sometimes Not Dominant With Respect to CDF

- For PWRs, SGTR and bypass sequences (e.g., ISLOCA) dominate LERF and therefore early fatalities

- SGTR and bypass not dominant contributors to core damage frequency
  - If SGTR or bypass occur, consequences are large
  - Remember: risk = frequency \times consequence
11. External Events
External Events

- Purpose: This topic will acquaint students with the definition of external events and the IPEEEs.

- Objectives:
  - Define external events and understand how they differ from internal events
  - List several of the more significant external events, including those analyzed in the IPEEEs
  - Know the objectives of the IPEEE and the acceptable approaches for seismic events and fires
  - Explain the ways in which external events may be evaluated and how this evaluation is related to the overall PRA task flow.

Overview of External Events Analysis

- External Events (EE) refers to those events that are external to system being analyzed
  ✦ e.g., fires, floods, earthquakes
    ✦ Includes on-site events such as flooding of various rooms within plant
- Concern is with dependent nature of EE
  ✦ i.e., EE both initiates potential core damage accident AND results in failure of safety systems
- General approach
  ✦ Identify hazard and its intensity
  ✦ Conditional probability of plant SSCs failure
  ✦ Assess overall plant response to event
NPP External Events Risk First Analyzed 1979

- 1979 - Oyster Creek (first seismic PRA)
- 1979 - HTGR (first fire PRA)
- 1981 - Big Rock Point
- 1982 - Zion/Indian Point
- 1983 - NUREG/CR-2300 (PRA Procedures Guide includes external events)
- 1988 - GL 88-20 (IPEs to include internal floods)
- 1989 - NUREG-1150 (fire and seismic)
- 1991 - GL-88-20, Supplement 4 (IPEEE, revised in 1995 with supplement 5, which revised seismic requirements)
Initial List of Potential External Event Hazards Very Extensive (1 of 2)

- Aircraft
- Avalanche
- *Earthquake
- *Fire in plant
- Fire outside plant but on site
- Fire off site
- Flammable fluid release
- Fog
- *Flooding, external (including seiche, storm surge, dam failure, and tsunami)
- Flooding, internal
- *High winds (including tornadoes)
- Hurricane
- Ice
- Industrial or military accident offsite
- Landslide
- Lightning
- Meteorite impact
Initial List of Potential External Event Hazards Very Extensive (2 of 2)

- Pipeline accident
- Sabotage
- Ship impact
- Toxic gas release
- Transportation accident
- Turbine missile
- Volcanic activity
- War

- Blizzard/Snow
- Drought
- Erosion
- Hail
- Heavy rain
- High temperature
- Low Temperature
- River diversion or change in lake level
Most Hazards Excluded for Various Reasons

- IPEEE required analysis of hazards believed to dominate external event risk
  - Seismic
  - Internal fires
  - High winds and tornadoes
  - External floods (internal flood analysis required in IPE)
  - Transportation and nearby facility accidents
  - Any known plant-unique hazards
External Events Analyses Performed at Various Levels of Detail

- Seismic
  - Seismic PRA or Seismic Margins Assessment (includes HCLPF - high confidence of low probability of failure assessment)

- Fire
  - Fire PRA or Fire Vulnerability Evaluation (FIVE)

- Other
  - EE PRA or screening analysis
Seismic Hazard PRA - 3 Basic Steps

- Hazards analysis (frequency-magnitude relationship for earthquakes)
  - Location-specific hazard curves produced by NRC (LLNL) and EPRI
- Fragility analysis ("strength" of component)
  - Conditional probability of failure given a specific earthquake severity
- Accident sequence analysis

Analysis process briefly looked at in following slides
Four Steps in Seismic Hazard Curve Development

1. Identify seismic sources

2. Develop frequency-magnitude model for each source

3. Develop ground motion model for each source

4. Integrate over sources
Frequencies Estimated for Various Ground Acceleration Levels

- Frequency of 0.1g, 0.2g, 0.3g, etc. earthquake estimated
- Each g-level earthquake analyzed separately (i.e., as a separate and unique event)
- Failure probabilities of plant SSCs calculated based on g-level and fragility of SSC
- Internal events PRA re-evaluated using “new” seismic failure probabilities
Seismic Fragility Expressed in Terms of Peak Ground Acceleration

- Fragility \( (A) = A_m \beta_R \beta_U \) (lognormal model assumed)
  - \( A_m = \) median ground acceleration capacity of SSC
  - \( \beta_R \beta_U = \) Measure of the uncertainty in median fragility due to randomness and confidence, respectively (can also be labeled aleatory and epistemic, respectively).
  - \( A_m \) derived from various safety and response factors \( (F_c F_{RE} F_{RS} A_{SSE}) \), in turn are products of other factors
   - \( F_C \) - Capacity Factor
   - \( F_{RE} \) - Response factor for equipment
   - \( F_{RS} \) - Response factor for structure
   - \( A_{SSE} \) - Safe Shutdown Earthquake acceleration
## Range of Seismic Fragilities for Selected Components

<table>
<thead>
<tr>
<th>Component/Structure</th>
<th>Dominant Failure Mode</th>
<th>Median Fragility Range (g)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concrete containment building</td>
<td>Shear failure</td>
<td>2.50-9.20</td>
</tr>
<tr>
<td>Reactor Pressure Vessel</td>
<td>Anchor bolt</td>
<td>1.04-5.70</td>
</tr>
<tr>
<td>Flat-bottom tank</td>
<td>Shell wall buckling</td>
<td>0.20-1.00</td>
</tr>
<tr>
<td>Batteries and racks</td>
<td>Cases and plates</td>
<td>0.90-5.95</td>
</tr>
<tr>
<td>Motor control centers</td>
<td>Chattering</td>
<td>0.06-4.20</td>
</tr>
<tr>
<td>Diesel generator</td>
<td>Anchor bolt</td>
<td>0.70-3.89</td>
</tr>
<tr>
<td>Offsite power</td>
<td>Ceramic insulators</td>
<td>0.20-0.62</td>
</tr>
</tbody>
</table>

Probability of "Initiating Events" Estimated Given Occurrence of EE (Provides Link to Sequence Analysis)

<table>
<thead>
<tr>
<th>Seismic Event Occurs</th>
<th>Reactor Vessel Rupture</th>
<th>Large LOCA</th>
<th>Medium LOCA</th>
<th>Small LOCA</th>
<th>Loss of Off-Site Power</th>
<th>Rx-Tnp with FW nominally available</th>
</tr>
</thead>
<tbody>
<tr>
<td>EO</td>
<td>RVR</td>
<td>LLOCA</td>
<td>MLOCA</td>
<td>SLOCA</td>
<td>LOSP</td>
<td>T</td>
</tr>
</tbody>
</table>

![Diagram showing the sequence analysis]

SEISMIC - Seismic IE

06/2002

PRA Basics for Regulatory Applications (P-105) 184
Fire Analysis Follows Phased Approach

• Qualitative Screening
  ✧ Fire in area does not cause a demand for reactor trip
  ✧ Fire area does not contain safety-related equipment
  ✧ Fire area does not have credible fire source or combustibles

• Quantitative Screening
  ✧ Utilized existing internal events PRA
  ✧ Estimate fire frequency for area and assume all equipment in fire area failed by fire, calculate CDF

• Detailed Analysis
Detailed Fire Analysis Includes

- Fire occurrence frequency assessment
  - Either location based or component based
  - Generic data updated with plant-specific experience
- Fire growth and propagation analysis
  - Considers: Combustible loading, fire barriers, and fire suppression
  - Modeled with specialized computer codes (COMPBRN IIle)
- Component fragilities and failure mode evaluation
- Fire detection and suppression modeling
- Detailed fire scenarios analyzed using transient ET
Fire-Induced Vulnerability Evaluation (FIVE)

- Developed by EPRI as an alternative to a fire PRA for satisfying IPEEE requirements
- Equivalent to a fire-area screening analysis
  - worksheet-based systematic evaluation using information from Appendix R implementation
  - does not produce detailed quantification of fire CDF
- Most FIVE users (IPEEE) also quantified fire CDF of unscreened areas
Other External Events Analyzed Using Structured Screening Process

- IPEEE Guidance - Progressive Screening approach (see Figure 5.1 of NUREG-1407)
  - Review Plant Specific Hazard Data and Licensing Basis (FSAR)
  - Identify Significant Changes, if any, since OP Issuance
  - Does Plant/Facility Design Meet 1975 SRP Criteria (via quick screening & confirmatory walkdown)
    - If yes, no further analysis is needed
    - If no, continue analysis (next slide)
Examples of SRP Non-Conformance

- Flood
  - Probable Maximum Precipitation (PMP) at site based on old National Weather Service data

- High-Wind/Tornado
  - Design basis tornado missile spectrum different from that specified in SRP
If 1975 SRP Criteria Not Met

- Is Hazard Frequency Acceptably Low (<1E-5/yr)?
  If Not:
- Does bounding analysis estimate CDF <1E-6/yr?
  If Not:
- Perform detailed PRA
  ✷ Details of analysis are tailored to particular hazard
12. SHUTDOWN RISK
Low-Power and Shutdown Risk

- **Purpose:** Discusses why low-power and shutdown modes of operation are thought to be of concern from a risk perspective, and introduces approaches to analyzing shutdown risk.

- **References:**
  - NUREG-1449 - Review of shutdown events
  - NUREG/CR-6143 and -6144 - Analysis of low-power shutdown risks at Grand Gulf and Surry
  - NUREG/CR-6616 - Risk comparison of scheduling preventive maintenance at shutdown vs at power operation for PWRs
Risk From LP/SD Operations Was Not Considered in Early PRAs

- Low-power and shutdown (LP/SD) encompasses operation when the reactor is subcritical or in transition between subcriticality and power operations up to ~15% of rated power.

- In early risk studies, risk from full power operation was assumed to be dominant because during shutdown:
  - Reactor is subcritical
  - Decay heat is decreasing with time
    - Longer time is available to respond to accidents.
LP/SD Operational Events Established the Credibility of LP/SD Risk

- Precursor events implied that potential generic vulnerabilities existed:
  - April 87 Diablo Canyon event resulting in loss of RHR while in mid-loop operation (and numerous similar events at other plants)
  - March 90 Vogtle plant loss of all AC power while shutdown
  - Two generic letters were subsequently issued relating to low-power and shutdown operations:
    - GL 87-12 -- Loss of RHR while the RCS is partially filled
    - GL 88-17 -- Loss of Decay Heat Removal
Operating Experience Insights Reinforced by Early LP/SD Risk Studies

- Limited risk studies of low-power and shutdown operations have suggested that shutdown risk may be significant because
  - Systems may not be available as Tech. Specs. allow more equipment to be inoperable than at power
  - Initiating events can impact operable trains of systems providing critical plant safety functions
  - Human errors are more prevalent because operators may find themselves in unfamiliar conditions not covered by training and procedures
  - Plant instruments and indications may not be available or accurate
Subsequent LP/SD Risk Studies Examined a Range of Issues

- Studies included:
  - Further review of operating experience for domestic and foreign reactors (discussed on next slide)
  - Analysis of selected significant events to estimate conditional probability of core damage using ASP models
  - Review of PRAs that included LP/SD operations
  - NRC sponsored Level 1 PRAs for LP/SD operations for Surry and Grand Gulf
Operating Experience Analysis

- AEOD* investigation of approximately 90 significant shutdown events out of 348 that occurred between January 1988, and July 1990 yielded the following major categories:
  - Loss of S/D cooling due to loss of system flow or loss of heat sink (27 events: 16 PWR and 11 BWR), e.g., errors during emergency power switching logic circuit testing caused a loss of AC power, resulting in loss of RHR for 15 minutes
  - Loss of reactor coolant inventory (22 events: 10 PWR and 12 BWR), e.g., opening RHR pump suction relief valve or PORV, or valve lineup errors
  - Loss of electrical power (19 events: 13 PWR and 6 BWR), e.g., loss of an AC, DC or instrument bus due to maintenance errors
  - Flooding and spills (3 PWR events)
  - Inadvertent reactivity addition (10 events: 4 PWR and 6 BWR), e.g., boron dilution without operator's knowledge
  - Breach of containment integrity (8 events, all human error)

* AEOD Special Report - Review of Operating Events Occurring During Hot and Cold Shutdown and Refueling, December 4, 1990
NRC Continued Monitoring Operating LP/SD Experience

- AEOD performed follow-up investigation of shutdown events that occurred between January 1993 and May 1995, after licensees had time to implement NUMARC 91-06, "Guidelines for Industry Actions to Assess Shutdown Management" (December 1991), and found:
  - Significant number of events during shutdown still occurring (486 during the 29-month investigation period), with 64 events having some measure of risk significance
  - Events similar to those of earlier investigation and still dominated by human errors during test and maintenance
NRC Staff's Evaluation of LP/SD Risk

- Vogtle (1990) SBO Investigation Motivated Broader Look at LP/SD Risk (NUREG-1449)
  - Study published in Sept 1993 documented significant technical findings including:
    - Outage planning is crucial to safety during S/D
    - Significant maintenance activities increase potential for fires during shutdown
    - PWRs are more likely to experience events than BWRs; dominant contributor to PWRs is loss of RHR during operations with reduced inventory (midloop operation)
    - Extended loss of RHR in PWRs can lead to LOCAAs caused by failure of temporary pressure boundaries in RCS or rupture of RHR system piping
Subsequent LP/SD PRA Studies

- Although risks associated with shutdown and refueling conditions have not been studied as extensively as those for power operation, several limited PRAs have been completed for both PWRs and BWRs (e.g., Zion, Seabrook, Surry, Grand Gulf), as well as shutdown decay heat removal studies (Sequoyah, Brunswick); significant findings include:

  - Quantitative core damage frequency estimates for certain shutdown modes of operation are comparable to estimates for full power operation.
Subsequent PRA Studies (Cont.)

- Most significant issues identified from a LP/SD risk perspective are:
  - Mid-loop operation (PWRs) of particular concern
  - Operator errors, especially
    - failure to determine proper actions to restore shutdown cooling
    - procedural deficiencies
  - Loss of RHR shutdown cooling, especially
    - operator induced
    - suction valve trips
    - cavitation due to overdraining of the RCS
  - Loss of offsite power
Few LP/SD PRA Have Been Developed

- Perception continues that LP/SD operations pose less risk than full-power
- LP/SD PRA developed reputation of being very expensive and complicated process
  - NUREG/CR-6143, -6144
- Most utilities have opted to manage LP/SD risk using simple configuration management approach
  - Vital safety functions defined - systems/trains needed to perform vital safety function maintained in-service
How Utilities are Addressing LP/SD Risk

• Some utilities have performed limited PRA studies of selected modes of operation

• Most utilities have adopted non-PRA approach
  ✧ Approach based on guidance in NUMARC 91-06
  ✧ Approach based on maintaining barriers during shutdown
  ✧ EPRI sponsored development of software to implement this approach (ORAM*)

* Outage Risk Assessment and Management
SPAR Program Developing Limited
Number of LP/SD Models

- Scheduled to produce 8 LP/SD models (Mar-02 to Mar-04)
- Models organized using 15 Plant Operating States (POSs) based on plant configuration evolutions and 4 Time Windows (time after reactor shutdown, i.e., different decay heat levels)
- Initiating Events include:
  - Loss of RHR
  - Loss of RHR given primary reactor coolant is at reduced inventory level
  - Loss of Offsite Power
  - Loss of primary reactor coolant Inventory
13. Uncertainties in PRA
Uncertainties in PRA

- **Purpose:** To acquaint students with how PRA treats uncertainty, including the identification of two types of uncertainty, aleatory and epistemic, and the characterization of one type of epistemic uncertainty with probability distributions.

- **Objectives:** Students will be able to identify the two types of uncertainty, along with their sources, and interpret probability distributions as an expression of epistemic uncertainty.

- **References:**
  - NUREG-1489
Uncertainty Arises From Many Sources

- Inability to specify initial and boundary conditions precisely
  - Cannot specify result with deterministic model
  - Instead, use probabilistic models (e.g., tossing a coin)
- Sparse data on initiating events, component failures, and human errors
- Lack of understanding of phenomena
- Modeling assumptions (e.g., success criteria)
- Modeling limitations (e.g., inability to model errors of commission)
- Incompleteness (e.g., failure to identify system failure mode)
Key Terminology:
Frequentist Interpretation of Probability

\[ \Pr(N_1) = \lim_{N \to \infty} \frac{N_1}{N} \]

\[ \hat{p} = \frac{1}{50} = 0.02 = 2E-2 \]
Key Terminology: Subjectivist (Bayesian) Interpretation of Probability

$
\Rightarrow \Pr(N_1) \text{ is the degree of belief the analyst holds about the likelihood of event } N_1 \text{ occurring.}
$
PRAs Identify Two Types of Uncertainty

- Distinction between aleatory and epistemic uncertainty:
  - "Aleatory" from the Latin Alea (dice), of or relating to random or stochastic phenomena. Also called "random uncertainty or variability."
  - "Epistemic" of, relating to, or involving knowledge; cognitive. [From Greek episteme, knowledge]. Also called "state-of-knowledge uncertainty."
Aleatory Uncertainty

- Variability in or lack of precise knowledge about underlying conditions makes events unpredictable. Such events are modeled as being probabilistic in nature. In PRAs, these include initiating events, component failures, and human errors.
- For example, PRAs model initiating events as a Poisson process, similar to the decay of radioactive atoms.
- Poisson process characterized by frequency of initiating event, usually denoted by parameter λ.
Epistemic Uncertainty

- Value of $\lambda$ is not known precisely
- Could model uncertainty in estimate of $\lambda$ using statistical confidence interval
  - Can't propagate confidence intervals through PRA models
  - Can't interpret confidence intervals as probability statements about value of $\lambda$
- PRAs model lack of knowledge about value of $\lambda$ by assigning (usually subjectively) a probability distribution to $\lambda$
  - Probability distribution for $\lambda$ can be generated using Bayesian methods.
Epistemic Uncertainty (cont'.)

- Advantages to Bayesian Approach
  - Allows uncertainties to be propagated easily through PRA models
  - Allows probability statements to be made concerning inputs and outputs that depend upon inputs
  - Provides unified, consistent framework for parameter estimation
Uncertainty in $\lambda$ Expressed as Probability Distribution
Uncertainty Propagation

- Uncertainties propagated via Monte Carlo sampling
- In this approach, output probability distribution is generated empirically by repeated sampling from input parameter distributions
Other Epistemic Uncertainties in PRA

- Modeling uncertainty
  - System success criteria
  - Accident progression phenomenology
  - Health effects models (linear versus nonlinear, threshold versus nonthreshold dose-response model)
Other Epistemic Uncertainties in PRA (cont.)

- Completeness
  - Complex errors of commission
  - Design and construction errors
  - Unexpected failure modes and system interactions
  - All modes of operation not modeled

- Errors in analysis
  - Failure to model all trains of a system
  - Data input errors
  - Analysis errors
Addressing Other Epistemic Uncertainties

- Modeling uncertainty usually addressed through sensitivity studies
  - Research ongoing to examine more formal approaches
- Completeness addressed through comparison with other studies and peer review
  - Some issues (e.g., design errors) are simply acknowledged as limitations
  - Other issues (e.g., errors of commission) are topics of ongoing research
- Analysis errors may be difficult to catch; addressed through peer review and validation process
Uncertainty in PRA

For additional information:

*Probability & Statistics for PRA (P-102)* course covers modeling and propagation of uncertainty in great detail. It covers both the frequentist and Bayesian approaches and compares and contrasts the two.
14. Configuration Risk Management
Configuration Risk Management

- **Purpose:** To acquaint students with the basic concepts of using PRA models to control configuration risk by planning maintenance.

- **Objectives:** Students will be able to explain;
  - Why base case PRA results cannot be used for maintenance planning
  - What is meant by “configuration risk management”
  - How configuration risk management is related to risk-informed regulation

- **Reference:** NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications
Configuration Risk Management

Why an Issue?

- Economics - Plants are moving towards increased maintenance while at power, to reduce outage durations

- Safety
  - Increased maintenance while at power not covered in IPEs/PRAs
  - Increased on-line maintenance can produce high-risk plant configurations
Configuration Risk Management

Why an Issue?

“In general, the industry appears to be adopting the practice of on-line maintenance faster than it is developing and implementing effective controls to manage the safety (risk) implications of this practice.”

Observed Preventive Maintenance Practices of Concern

- Multiple components simultaneously out of service, as allowed (implicitly) by technical specifications
- Repeated entries into Action Statements to perform PM + long equipment downtimes
- Significant portions of power operations may be spent in Action Statements to carry out PMs
Configuration Risk Management
Traditional Approaches

- Technical Specifications and Limiting Conditions for Operation
  - Identify systems/components important to safety based on traditional engineering approach
  - Limit component out-of-service times for individual and combinations of component outages (not based on formal risk analysis)
- Maintenance planning guidelines such as 12-week rolling schedule, etc.
  - Provide guidance to work week planners on allowable maintenance/testing
  - Based on train protection concept and Technical Specifications
- Operator judgment
Configuration Risk Management

Traditional Approaches

- Weaknesses of Traditional Approaches
  - Generally based on and limited to Technical Specification equipment
  - No limit on frequencies of equipment outages - only on duration of each outage
- Is the traditional approach good enough, given the increased emphasis on on-line maintenance?
- How can PRA help?
Configuration Risk Management

• Configuration risk management: one element of risk-informed regulation

• Can be forward-looking or retrospective
  ▶ Forward-looking to plan maintenance activities & outage schedules
  ▶ Retrospective to evaluate risk significance of past plant configurations
Configuration Risk Management

- Plant configuration: state of the plant as defined by status of plant components
- Involves taking measures to avoid risk-significant configurations, limit duration and frequency of such configurations that cannot be avoided
Configuration Risk Management

- Configuration risk has various measures
  - Core damage frequency (instantaneous)
    - Baseline CDF (the zero maintenance CDF)
    - Configuration-specific CDF
  - Incremental CDF
    - = Configuration-specific CDF - Baseline CDF
  - Core damage probability (CDP)
    - = CDF * duration
  - Incremental core damage probability (ICDP)
    - = ICDF * duration
    - = CCDP - CDP
  - Incremental large early release probability (ICLERP)
    - = ILERF * duration
    - = CLERP - LERP
CDF Profile

(P-105)

10^{-3}

10^{-4}

10^{-5}

Time

Baseline CDF (without Test & Maintenance)

PRA CDF (with Test & Maintenance)

Configuration-specific CDF

06/2002
Cumulative CDP Profile

- PRA CDP (with Test & Maintenance)
- Baseline CDP (without Test & Maintenance)

Time:
- $t_1$
- $t_2$
- $t_3$
- $t_4$
Configuration Risk Management

• Requires management of:
  ✷ OOS components
    ✷ instantaneous CDF (configuration-specific CDF)
  ✷ Outage time of components & systems
    ✷ configuration duration
    ✷ CCDP
    ✷ ICDP
  ✷ Backup components
    ✷ instantaneous CDF
  ✷ Configuration frequency
    ✷ cumulative CDP over time
Managing OOS Components

- Involves scheduling maintenance and tests to avoid having critical combinations of components or systems out of service concurrently.

- For Maintenance Rule, 10 CFR 50.65
  - A value of $1 \times 10^{-3}$/year is suggested in NUMARC 93-01 for a ceiling for configuration-specific CDF.
  - Subject of such a ceiling value being studied by the NRC.
  - NRC neither endorses nor disapproves $1 \times 10^{-3}$/year value.
Managing Outage Time

- Must determine how long configuration can exist before risk incurred becomes significant
  - Many utilities using EPRI PSA Application Guide numerical criteria, although not endorsed by NRC
  - NRC has no numerical criteria at present for temporary changes to plant
  - For Maintenance Rule,
    - Configuration Should not normally be entered voluntarily
      - >1E-5 ICDP
      - >1E-6 ILERP
    - Assess non quantifiable factors and establish risk management actions
      - 1E-6 to 1E-5 ICDP
      - 1E-7 to 1E-6 ILERP
    - Normal work controls
      - <1E-6 ICDP
      - <1E-7 ILERP
  - For risk-informed Tech. Specs., for single AOT:
    - ICCDP < 5E-7
    - ICLERP < 5E-8
- Must know compensatory measures to take to extend outage time without increasing risk
Managing Backup Components

- Must determine which components can carry out functions of those out of service
Controlling Frequency

- Must track frequency of configurations and modify procedures & testing to control occurrences, as necessary and feasible
Why Configuration Risk Management is Needed...

- PRA/IPE assumes random failures of equipment (including equipment outages for testing & maintenance)
- PRA/IPE baseline model does not correctly model simultaneous outages of critical components
- Simultaneous outages (i.e., plant configurations) can increase risk significantly above the PRA/IPE baseline
- Lack of configuration management can affect initiating events and equipment designed to mitigate initiating events, leading to increased risk
Preventive Maintenance Risk Calculations

- Risk impact of PM on single component
- Risk impact of maintenance schedule
- Risk impact of scheduling maintenance (power operations versus shutdown)
Risk Monitors

- On-line risk monitors can be used to evaluate plant configurations for a variety of purposes:
  - To provide current plant risk profile to plant operators
  - As a forward-looking scheduling tool to allow decisions about test and maintenance actions weeks or months in advance of planned outages
  - As a backward-looking tool to evaluate the risk of past plant configurations
Current Risk Monitor Software Packages

- Erin Engineering Sentinel
- Scientech/NUS Safety Monitor
  - The NRC acquired this package from Scientech, and has an agency-wide license covering its use
- EPRI R&R Workstation
- Commonwealth Edison OSPRE
Requisite Features

- Risk monitor software requires (at a minimum) the following features:
  - PRA solution engine for analysis of the plant logic model
  - Database to manage the various potential plant configurations
  - Plotting program to display results
Risk Monitor Capabilities

- As a tool for plant operators to evaluate risk based on real-time plant configuration:
  - Calculates measure of risk for current or planned configurations
  - Displays maximum time that can be spent in that particular configuration without exceeding pre-defined risk threshold
  - Provides status of plant systems affected by various test and maintenance activities
  - Operators can do quick sensitivity studies to evaluate the risk impacts of proposed plant modifications
Risk Monitor Capabilities (cont.)

- As a tool for plant scheduling for maintenance and outage planning:
  ✷ Generates time-line that shows graphically the status of plant systems and safety functions
  ✷ Generates risk profile as plant configuration varies over time
  ✷ Identifies which components have strongest influence on risk
Risk Monitor Strengths and Weaknesses

- Risk Monitor Strengths
  - Provides risk determinations of current and proposed plant configurations
  - Compact model
  - Many current PRA models can be converted into risk monitor format
  - Can obtain importance and uncertainty information on results
  - Provides risk management guidance by indicating what components should be restored first
Risk Monitor Strengths and Weaknesses (cont.)

- Risk Monitor Limitations
  - For some PRA codes, difficulty of converting PRA models into master logic diagram (e.g., Large Event Tree approach models)
  - Effort required to set up databases to link master logic diagram events to plant components and electronic P&IDs, and interface with scheduling software
  - Analysis Approximations
    - CCF adjustments
    - Human recovery modeling
    - Consideration of plant features not normally modeled in PRA studies
    - Cut set updating versus logic model solution
    - Truncation limits
Additional Sources of Information

- Further details on configuration risk management can be found in NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications.

- Risk Assessment for Event Evaluation (P-302) course in the PRA Technology Transfer Program curriculum explores the use of PRA techniques for evaluating the risk significance of operational events, as well as plant configuration risk management, discusses the other risk measures mentioned in this module (e.g., CCDP and event importance), and illustrates use of the GEM code to perform the necessary PRA calculations.
15. Introduction to Risk-Informed Decision-Making
Introduction to Risk-Informed Decision-Making

• Purpose: Discuss the principal steps in making risk-informed regulatory decisions, including the acceptance guidance contained in the draft SRPs addressing this subject.
Risk-Informed Regulatory Guides and SRPs

- R. G. 1.174 - General guidance to licensees
- R.G.-1.175 - Application-specific guidance on in-service testing
- R.G. – 1.176 - Application-specific guidance on graded quality assurance
- R.G. – 1.177 - Application-specific guidance on technical specifications
- R.G. – 1.178 - Application-specific guidance on in-service inspection
- SRP Chapter 19 - General guidance to staff
- SRP Section 3.9.7 - Application-specific guidance on IST
- Inspection guidance - under development
- SRP Section 16.1 - Application-specific guidance on technical specifications
- SRP Section 3.9.8 - Application-specific guidance on ISI
Decision Logic for Submittal Reviews

Staff Proposes Increased Requirements - Use 50.109 Backfit Rule (Reg. Analysis Guidelines)

Licensee Makes Change Consistent with 50.59 Process

"Licensing Basis"

Licensee Requests Change in Requirements via Approved Staff Position - (10 CFR 50.90-92)

Licensee Requests Change in Requirements Beyond Approved Staff Positions - 10CFR50.90-92

Licensee Requests Change Consistent with Approved Staff Position (Rule, RG, SRP, BTP...) "Normal Staff Review"

Licensee Requests Change Consistent with 50.59 Process

Does not Present Risk Information "Normal Staff Review"

Does Present Risk Information "Use Risk-Informed RG/SRP"
Principal Steps in Risk-Informed Plant-Specific Decision-Making

1. Define Change
2. Perform Engineering Analysis
3. Define Monitoring Program
4. Submit Proposed Change
Principles of Risk-Informed Regulation

- The proposed change meets current regulations unless it is explicitly related to a requested exemption or rule change
- The proposed change is consistent with the defense-in-depth philosophy
- The proposed change maintains sufficient safety margins
- Proposed increases in core damage frequency and risk are small and are consistent with the intent of the Commission's Safety Goal Policy Statement
- The impact of the proposed change should be monitored using performance measurement strategies
Expectations from Risk-Informed Regulation

- All safety impacts of the proposed change are evaluated in an integrated manner as part of an overall risk management approach in which the licensee is using risk analysis to improve operational and engineering decisions broadly by identifying and taking advantage of opportunities for reducing risk, and not just to eliminate requirements the licensee sees as undesirable. For those cases where risk increases are proposed, the benefits should be described and should clearly outweigh the proposed risk increases. The approach used to identify changes in requirements should be used to identify areas where requirements should be increased, as well as where they could be reduced.
Expectations from Risk-Informed Regulation (cont.)

- Acceptability of proposed changes should be evaluated by the licensee in an integrated fashion that ensures that all principles are met.
- The use of core damage frequency (CDF) and large early release frequency (LERF) as bases for probabilistic risk assessment acceptance guidelines is an acceptable approach. Use of the Commission's Safety Goal Quantitative Health Objectives (QHOs) for this purpose is acceptable in principle and licensees may propose their use; however, in practice, implementing such an approach would require careful attention to the methods and assumptions used in the analysis, and treatment of uncertainties.
Expectations from Risk-Informed Regulation (cont.)

- Increases in estimated CDF and LERF resulting from proposed changes will be limited to small increments and the cumulative effect of such changes should be tracked.
- The scope and quality of the engineering analyses (including traditional and probabilistic analyses) conducted to justify the proposed change should be appropriate for the nature and scope of the change and should be based on the as-built and as-operated and maintained plant, including reflection of operating experience at the plant.
- Appropriate consideration of uncertainty is given in analyses and interpretation of findings.
- A program of monitoring, feedback, and corrective action should be used to address significant uncertainties.
Expectations from Risk-Informed Regulation (cont.)

- The plant-specific PRA supporting licensee proposals has been subjected to quality controls such as an independent peer review or certification.
- Data, methods, and assessment criteria used to support regulatory decision-making must be scrutable and available for public review.
Acceptance Guidelines

- Defense-in-depth is maintained
  - A reasonable balance among prevention of core damage, prevention of containment failure, and consequence mitigation is preserved
  - Over-reliance on programmatic activities to compensate for weaknesses in plant design is avoided
  - System redundancy, independence, and diversity are preserved commensurate with the expected frequency and consequences of challenges to the system (e.g., no risk outliers)
  - Defenses against potential common-cause failures are preserved and the potential for introduction of new common-cause failure mechanisms is assessed
Acceptance Guidelines (cont.)

- Defense-in-depth is maintained (cont.)
  - Independence of barriers is not degraded
  - Defenses against human errors are preserved
  - The intent of the General Design Criteria in 10 CFR 50, App. A, are maintained

- Sufficient safety margins are maintained
  - Codes and standards or alternatives approved for use by the NRC are met
  - Safety analysis acceptance criteria in the licensing basis (e.g., FSAR, supporting analyses) are met, or proposed revisions provide sufficient margin to account for analysis and data uncertainty
Acceptance Guidelines (cont.)

- Risk guidelines on following slides are met
  - Risk guidelines are intended for comparison with full-scope PRA results
    - Internal events (full power, low power, shutdown)
    - External events (seismic, fire, etc.)
    - Use of less than full scope PRA may be acceptable
Mean Core Damage Frequency
Acceptance Guidelines

- **Region I**
  - Not allowed
  - Management attention
  - Full uncertainty analysis
  - Track cumulative impacts

- **Region II**
  - Very small changes
  - Not tied to baseline CDF
  - Uncertainty analysis only on ΔCDF
  - Track cumulative impacts

- **Region III**

**Mean Core Damage Frequency (CDF)**

06/2002

PRA Basics for Regulatory Applications (P-105)
Mean Large Early Release Frequency Acceptance Guidelines

- **Region I**
  - Not allowed
  - Management attention
  - Full uncertainty analysis
  - Track cumulative impacts

- **Region II**
  - Very small changes
  - Not tied to baseline LERF
  - Uncertainty analysis only on ΔLERF
  - Track cumulative impacts

- **Region III**

**Mean Large Early Release Frequency (LERF)**
Increased Management Attention

- Application is given increased NRC management attention when the calculated values of the changes in the risk metrics, and their baseline values when appropriate, approach the guidelines. The issues addressed by management will include:
  - Cumulative impact of previous changes and trend in CDF and LERF (licensee’s risk management approach)
  - Impact of proposed change on operations complexity, burden on operating staff, and overall safety practices
  - Benefit of the change with respect to its risk increase
  - Level 3 PRA information, if available
Consideration of Uncertainties

- Use mean values for comparison with guidelines
- Identify important sources of uncertainty
  - Parameter
  - Modeling
  - Completeness
- Perform sensitivity calculations on parameter and modeling uncertainties
- Perform quantitative or qualitative analysis on completeness uncertainties
- Results of sensitivity studies should generally meet guidelines
- Region III - no need to calculate uncertainty on baseline CDF/LERF
Combined Change Requests

- Several changes can be combined in one submittal
- Will be reviewed against acceptance guidelines
  - Individually with respect to defense in depth
  - Cumulatively
- Combined changes should be related. For example
  - Be associated with same system, function, or activity
  - Changes reviewed individually against risk criteria if not closely related
- Combined changes should not trade many small risk decreases for a large risk increase (i.e., create a new significant contributor to risk)
Key Issues in PRA Quality

- Ensure that, within scope, PRA analysis is complete and has appropriate level of detail
  - Consideration of relevant initiating events, plant systems, and operator actions
  - Analysis reflects plant-specific operating experience, design features, and accident response
  - All calculations are documented
- PRA methodology and associated input
  - Influence of models, input data, and assumptions on results and conclusions
- Licensee review and QA process
  - Peer review
  - Certification
  - Standards
NRC Staff and Management Responsibilities

- Ensure that licensing submittals are identified and processed in accordance with risk-informed guidance
- Identify current requirements that could be significantly enhanced with a risk-informed and/or performance-based approach
- Ensure objectives of risk-informed regulation are met
  - Enhanced safety decisions
  - Efficient use of NRC resources
  - Reduced unnecessary industry burden
- Ensure adequate staff training on use of risk-informed guidance and underlying PRA technical disciplines
- Maintain current levels of safety
16. Acronyms and Abbreviations
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Alternating current</td>
</tr>
<tr>
<td>ACRS</td>
<td>Advisory Committee on Reactor Safeguards</td>
</tr>
<tr>
<td>ADS</td>
<td>Automatic depressurization system</td>
</tr>
<tr>
<td>ADV</td>
<td>Atmospheric dump valve</td>
</tr>
<tr>
<td>AEOD</td>
<td>Office for Analysis and Evaluation of Operational Data</td>
</tr>
<tr>
<td>AFW</td>
<td>Auxiliary feedwater</td>
</tr>
<tr>
<td>AOP</td>
<td>Abnormal Operating Procedure</td>
</tr>
<tr>
<td>AOT</td>
<td>Allowed outage time</td>
</tr>
<tr>
<td>AOV</td>
<td>Air-operated valve</td>
</tr>
<tr>
<td>APB</td>
<td>Accident progression bin</td>
</tr>
<tr>
<td>APET</td>
<td>Accident progression event tree</td>
</tr>
<tr>
<td>ASEP</td>
<td>Accident Sequence Evaluation Program</td>
</tr>
<tr>
<td>ASP</td>
<td>Accident Sequence Precursor</td>
</tr>
<tr>
<td>ATHEANA</td>
<td>A Technique for Human Event Analysis</td>
</tr>
<tr>
<td>ATWS</td>
<td>Anticipated transient without scram</td>
</tr>
<tr>
<td>BC</td>
<td>Boundary condition</td>
</tr>
<tr>
<td>BNL</td>
<td>Brookhaven National Laboratory</td>
</tr>
<tr>
<td>BTP</td>
<td>Branch Technical Position</td>
</tr>
<tr>
<td>BWR</td>
<td>Boiling water reactor</td>
</tr>
<tr>
<td>BWROG</td>
<td>BWR Owners' Group</td>
</tr>
<tr>
<td>BWST</td>
<td>Borated water storage tank</td>
</tr>
<tr>
<td>CCDF</td>
<td>Complementary cumulative distribution flinction</td>
</tr>
<tr>
<td>CCDP</td>
<td>Conditional core damage probability</td>
</tr>
<tr>
<td>CCF</td>
<td>Common-cause failure</td>
</tr>
<tr>
<td>CCI</td>
<td>Core-concrete interaction</td>
</tr>
<tr>
<td>CCW</td>
<td>Component Cooling Water</td>
</tr>
<tr>
<td>CDF</td>
<td>Core damage frequency</td>
</tr>
<tr>
<td>CDFM</td>
<td>Conservative Deterministic Failure Margin</td>
</tr>
<tr>
<td>CDP</td>
<td>Core damage probability</td>
</tr>
<tr>
<td>CE</td>
<td>Combustion Engineering</td>
</tr>
<tr>
<td>CEOG</td>
<td>Combustion Engineering Owners' Group</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CLB</td>
<td>Current licensing basis</td>
</tr>
<tr>
<td>CRD</td>
<td>Control rod drive</td>
</tr>
<tr>
<td>CSIP</td>
<td>Charging/safety injection pump</td>
</tr>
<tr>
<td>CST</td>
<td>Condensate storage tank</td>
</tr>
<tr>
<td>CW</td>
<td>Circulating water</td>
</tr>
<tr>
<td>DBA</td>
<td>Design basis accident</td>
</tr>
<tr>
<td>DC</td>
<td>Direct current</td>
</tr>
<tr>
<td>DCH</td>
<td>Direct containment heating</td>
</tr>
<tr>
<td>DF</td>
<td>Decontamination factor</td>
</tr>
<tr>
<td>DFSD</td>
<td>Dominant functional sequence diagram</td>
</tr>
<tr>
<td>DHR</td>
<td>Decay heat removal</td>
</tr>
<tr>
<td>ECCS</td>
<td>Emergency core-cooling system</td>
</tr>
<tr>
<td>EDG</td>
<td>Emergency diesel generator</td>
</tr>
<tr>
<td>EOOS</td>
<td>Equipment Out of Service System</td>
</tr>
<tr>
<td>EOP</td>
<td>Emergency Operating Procedure</td>
</tr>
<tr>
<td>EPA</td>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>EPIX</td>
<td>Equipment performance and information exchange system</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
</tbody>
</table>
### Acronyms and Abbreviations (2 of 4)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESF</td>
<td>Engineered safeguards feature</td>
</tr>
<tr>
<td>ESW</td>
<td>Emergency service water</td>
</tr>
<tr>
<td>ESWGR</td>
<td>Emergency switchgear</td>
</tr>
<tr>
<td>ET</td>
<td>Event tree</td>
</tr>
<tr>
<td>FCI</td>
<td>Fuel-coolant interaction</td>
</tr>
<tr>
<td>FIVE</td>
<td>Fire-Induced Vulnerability Evaluation</td>
</tr>
<tr>
<td>FMEA</td>
<td>Failure modes and effects analysis</td>
</tr>
<tr>
<td>FSAR</td>
<td>Final Safety Analysis Report</td>
</tr>
<tr>
<td>FT</td>
<td>Fault tree</td>
</tr>
<tr>
<td>F-V</td>
<td>Fussell-Veseley (importance)</td>
</tr>
<tr>
<td>FW</td>
<td>Feedwater</td>
</tr>
<tr>
<td>GE</td>
<td>General Electric</td>
</tr>
<tr>
<td>GL</td>
<td>Generic Letter</td>
</tr>
<tr>
<td>HCLPF</td>
<td>High confidence, low probability of failure</td>
</tr>
<tr>
<td>HCR</td>
<td>Human Cognitive Reliability</td>
</tr>
<tr>
<td>HEP</td>
<td>Human error probability</td>
</tr>
<tr>
<td>HHISI</td>
<td>High-head safety injection</td>
</tr>
<tr>
<td>HLW</td>
<td>High-level waste</td>
</tr>
<tr>
<td>HPCI</td>
<td>High-pressure coolant injection</td>
</tr>
<tr>
<td>HPCS</td>
<td>High-pressure core spray</td>
</tr>
<tr>
<td>HPI</td>
<td>High-pressure injection</td>
</tr>
<tr>
<td>HPR</td>
<td>High-Pressure re-circulation</td>
</tr>
<tr>
<td>HPSI</td>
<td>High-pressure safety injection</td>
</tr>
<tr>
<td>HRA</td>
<td>Human reliability analysis</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, ventilation, and air conditioning</td>
</tr>
<tr>
<td>HTGR</td>
<td>High-Temperature Gas Reactor</td>
</tr>
<tr>
<td>HX</td>
<td>Heat exchanger</td>
</tr>
<tr>
<td>ICCDP</td>
<td>Incremental conditional core damage probability</td>
</tr>
<tr>
<td>ICLERP</td>
<td>Incremental conditional large early release probability</td>
</tr>
<tr>
<td>IE</td>
<td>Initiating event</td>
</tr>
<tr>
<td>INEEL</td>
<td>Idaho National Engineering and Environmental Laboratory</td>
</tr>
<tr>
<td>INPO</td>
<td>Institute for Nuclear Plant Operations</td>
</tr>
<tr>
<td>IPE</td>
<td>Individual Plant Examination</td>
</tr>
<tr>
<td>IPEEE</td>
<td>Individual Plant Examination for External Events</td>
</tr>
<tr>
<td>IREP</td>
<td>Interim Reliability Evaluation Program</td>
</tr>
<tr>
<td>ISA</td>
<td>Integrated Safety Analysis</td>
</tr>
<tr>
<td>ISI</td>
<td>In-service inspection</td>
</tr>
<tr>
<td>ISLOCA</td>
<td>Interfacing system loss-of-coolant accident</td>
</tr>
<tr>
<td>IST</td>
<td>In-service testing</td>
</tr>
<tr>
<td>JCO</td>
<td>Justification for Continued Operation</td>
</tr>
<tr>
<td>LB</td>
<td>Licensing basis</td>
</tr>
<tr>
<td>LCO</td>
<td>Limiting Condition for Operation</td>
</tr>
<tr>
<td>LER</td>
<td>Licensee Event Report</td>
</tr>
<tr>
<td>LERF</td>
<td>Large early release frequency</td>
</tr>
<tr>
<td>LERP</td>
<td>Large early release probability</td>
</tr>
<tr>
<td>LLNL</td>
<td>Lawrence Livermore National Laboratory</td>
</tr>
<tr>
<td>LLW</td>
<td>Low-level waste</td>
</tr>
<tr>
<td>LOCA</td>
<td>Loss-of-coolant accident</td>
</tr>
<tr>
<td>LOOP</td>
<td>Loss of offsite power</td>
</tr>
<tr>
<td>LOSP</td>
<td>Loss of offsite power</td>
</tr>
</tbody>
</table>
Acronyms and Abbreviations (3 of 4)

LP&S  Low power and shutdown
LPCI  Low-pressure coolant injection
LPCS  Low-pressure core spray
LPI   Low-pressure injection
LPR   Low-pressure re-circulation
LPSI  Low-pressure safety injection
LPZ   Low population zone
LWR   Light water reactor
MAAP  Modular Accident Analysis Program
MACCS MELCOR Accident Consequence Code System
MCS   Minimal cut set
MDP   Motor-driven pump
MGL   Multiple Greek letter
MOV   Motor-operated valve
MSIV  Main steam isolation valve
MSP   Maintenance and Surveillance Program
MSP   Maintenance and Surveillance Program
NCV   Non-cited violation
NEI   Nuclear Energy Institute
NMSS  Office of Nuclear Materials Safety and Safeguards
NOED  Notice of Enforcement Discretion
NPRDS Nuclear Plant Reliability Data System
NRC   Nuclear Regulatory Commission
NRR   Office Nuclear Reactor Regulation
NUMARC Nuclear Management and Resources Council
OOS   Out of service
ORAM  Outage Risk Assessment and Management
ORNL  Oak Ridge National Laboratory
OSHA  Occupational Safety and Health Administration
P&ID  Piping and instrumentation diagram
PA    Performance assessment
PCC   PRA Coordinating Committee
PCS   Power conversion system
PDS   Plant damage state
PM    Preventive maintenance
PORV  Power-operated relief valve
POSS  Plant operating state
PRA   Probabilistic risk assessment
PRT   Plant response tree
PRV   Pressurizer power-operated relief valves
PSA   Probabilistic safety assessment
PSF   Performance shaping factor
PTFG  PRA Training Focus Group
PTS   Pressurized thermal shock
PWR   Pressurized water reactor
QA    Quality Assurance
QHO   Quantitative health objective
QRA   Quantitative risk analysis
RAW   Risk achievement worth
RBCCW Reactor building closed cooling water
RCIC  Reactor core isolation cooling
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCP</td>
<td>Reactor coolant pump</td>
</tr>
<tr>
<td>RCS</td>
<td>Reactor coolant system</td>
</tr>
<tr>
<td>RES</td>
<td>Office of Nuclear Regulatory Research</td>
</tr>
<tr>
<td>RG</td>
<td>Regulatory Guide</td>
</tr>
<tr>
<td>RHR</td>
<td>Residual heat removal</td>
</tr>
<tr>
<td>RI</td>
<td>Resident Inspector</td>
</tr>
<tr>
<td>RPS</td>
<td>Reactor protection system</td>
</tr>
<tr>
<td>RRW</td>
<td>Risk reduction worth</td>
</tr>
<tr>
<td>RSS</td>
<td>Reactor Safety Study</td>
</tr>
<tr>
<td>RVC</td>
<td>Relief valve re-close</td>
</tr>
<tr>
<td>RWST</td>
<td>Refueling water storage tank</td>
</tr>
<tr>
<td>S/D</td>
<td>Shutdown</td>
</tr>
<tr>
<td>SAR</td>
<td>Safety Analysis Report</td>
</tr>
<tr>
<td>SBO</td>
<td>Station blackout</td>
</tr>
<tr>
<td>SDC</td>
<td>Shutdown cooling</td>
</tr>
<tr>
<td>SER</td>
<td>Safety Evaluation Report (Staff Evaluation Report for IPE/IPEEE)</td>
</tr>
<tr>
<td>SG</td>
<td>Steam generator</td>
</tr>
<tr>
<td>SGTR</td>
<td>Steam generator tube rupture</td>
</tr>
<tr>
<td>SHARP</td>
<td>Systematic Human Action Reliability Procedure</td>
</tr>
<tr>
<td>SI</td>
<td>Safety injection</td>
</tr>
<tr>
<td>SIF</td>
<td>Seal injection flow</td>
</tr>
<tr>
<td>SIT</td>
<td>Safety injection tank</td>
</tr>
<tr>
<td>SLOCA</td>
<td>Small loss-of-coolant accident</td>
</tr>
<tr>
<td>SNL</td>
<td>Sandia National Laboratory</td>
</tr>
<tr>
<td>SRA</td>
<td>Senior Reactor Analyst</td>
</tr>
<tr>
<td>SRI</td>
<td>Senior Resident Inspector</td>
</tr>
<tr>
<td>SRP</td>
<td>Standard Review Plan</td>
</tr>
<tr>
<td>SRV</td>
<td>Safety/relief valve</td>
</tr>
<tr>
<td>SSC</td>
<td>Systems, structures, and components</td>
</tr>
<tr>
<td>SSET</td>
<td>Support state event tree</td>
</tr>
<tr>
<td>STG</td>
<td>Source term group</td>
</tr>
<tr>
<td>SW</td>
<td>Service water</td>
</tr>
<tr>
<td>SWGR</td>
<td>Switch gear</td>
</tr>
<tr>
<td>TBCCW</td>
<td>Turbine building closed cooling water</td>
</tr>
<tr>
<td>TDP</td>
<td>Turbine-driven pump</td>
</tr>
<tr>
<td>TER</td>
<td>Technical Evaluation Report</td>
</tr>
<tr>
<td>THERP</td>
<td>Technique for Human Error Rate Prediction</td>
</tr>
<tr>
<td>TRC</td>
<td>Time reliability correlation</td>
</tr>
<tr>
<td>VCT</td>
<td>Volume control tank</td>
</tr>
<tr>
<td>WOG</td>
<td>Westinghouse Owners' Group</td>
</tr>
</tbody>
</table>