Operational Reactor Safety
22.091/22.903

Professor Andrew C. Kadak
Professor of the Practice

Probabilistic Safety Analysis
Lecture 11
Topics to be Covered

• Probabilistic Basics
• Event Trees
• Fault Trees
• Applications
• Examples
• Safety Goals
• Uses
Deterministic Safety Analysis

• Chapter 15 Analyses and Regulations Require
  – Design Basis Accident Analysis
  – Establishes strict criteria for assumptions at most conservative conditions
  – Assumes single failure criteria (worst)
  – Assumes other systems function normally
  – Most restrictive is Appendix K - LOCA criteria
  – Defines safety grade components that must work
Probabilistic Safety Analysis

- Models entire plant and all systems using best estimate analysis
- Nothing is assumed to work - Probabilities of failure of components assigned
- Includes human error
- Detailed analysis of consequences of failure required to determine the conditional consequences of failure of other components

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
PWR Engineered Safety Systems

FIGURE 14-2

Figures © Hemisphere. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
BWR Early Engineered Safety Systems

FIGURE 14-6

Figures © Hemisphere. All rights reserved. This content is excluded from our Creative Commons license.
For more information, see http://ocw.mit.edu/fairuse.
PSA Applications

- Risk (Based) or Informed regulation
  - an informed combination of deterministic and probabilistic analysis with judgement
- Safety Goals - How safe is safe enough
- Individual licensing decisions to assess marginal impact of plant changes.
- Performance based regulation.
The Pre-PRA Era (prior to 1975)

- Management of (unquantified at the time) uncertainty was always a concern.
- Defense-in-depth and safety margins became embedded in the regulations.
- “Defense-in-Depth is an element of the NRC’s safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility.” [Commission’s White Paper, February, 1999]
- Design Basis Accidents are postulated accidents that a nuclear facility must be designed and built to withstand without loss to the systems, structures, and components necessary to assure public health and safety.
## Potential Offsite Doses

### Potential Offsite Doses Due to Design-Basis Accidents
**(Conservative Case)**

<table>
<thead>
<tr>
<th>Accident</th>
<th>Two Hour Exclusion Boundary (3200 feet or 975 meters)</th>
<th>Duration of Accident Low Population Zone (4 miles or 6.4 km)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Thyroid (Rem)</td>
<td>Whole Body (Rem)</td>
</tr>
<tr>
<td>Loss of Coolant</td>
<td>155</td>
<td>3</td>
</tr>
<tr>
<td>Control Rod Ejection</td>
<td>&lt;1</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Fuel Handling</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Steam Line Break</td>
<td>16</td>
<td>1</td>
</tr>
</tbody>
</table>

**10 CFR 100 Dose Guideline**

300 25 300 25
Iodine-131 is a major threat to health in a nuclear plant accident.

Attempting to differentiate between credible (DBAs) and incredible accidents (Class 9; multiple protective system failures) is not logical.

If one considers a fault, such as a loss-of-coolant accident (LOCA), one can determine various outcomes, from safe shutdown and cooldown, to consideration of delays and partial failures of shutdown or shutdown cooling with potential consequences of radioactivity release.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
THE FARMER LINE

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Historical Risk Studies

1. Farmer's Paper (1967)

2. Reactor Safety Study (1975) Wash-1400

3. German Risk Study (1979)


5. Zion and Indian Point PRAs (1981)


7. Individual Plant Examinations
Technological Risk Assessment

• Study the system as an integrated socio-technical system.

Probabilistic Risk Assessment (PRA) supports Risk Management by answering the questions:

• What can go wrong? (accident sequences or scenarios)
• How likely are these scenarios?
• What are their consequences?
Reactor Safety Study (WASH-1400; 1975)

Prior Beliefs:

1. Protect against large LOCA.
2. CDF is low (about once every 100 million years, $10^{-8}$ per reactor year)
3. Consequences of accidents would be disastrous.

Major Findings

1. Dominant contributors: Small LOCAs and Transients.
2. CDF higher than earlier believed (best estimate: $5 \times 10^{-5}$, once every 20,000 years; upper bound: $3 \times 10^{-4}$ per reactor year, once every 3,333 years).
3. Consequences significantly smaller.
4. Support systems and operator actions very important.
Risk Curves

Frequency of Fatalities Due to Man-Caused Events (RSS)
CRITICAL SAFETY FUNCTIONS

KEEP FISSION PRODUCTS WITHIN THE FUEL

- Control Reactor Power
  - Control reactivity additions
  - Shutdown reliably
- Cool the Reactor and Spent Fuel
  - Maintain coolant inventory
  - Maintain coolant flow
  - Maintain coolant heat sinks

KEEP RADIOACTIVE MATERIAL OUT OF THE BIOSPHERE

- Maintain Containment Integrity
  - Prevent over-pressurization
  - Prevent over-heating
  - Prevent containment bypass
- Capture Material Within Containment
  - Scrubbing
  - Deposition
  - Chemical capture

SHIELD PERSONNEL FROM RADIATION
The Single-Failure Criterion

• “Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.”

• The intent is to achieve high reliability (probability of success) without quantifying it.

• Looking for the worst possible single failure leads to better system understanding.
“Defense-in-Depth is an element of the Nuclear Regulatory Commission’s safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility.”

[Commission’s White Paper, USNRC, 1999]
PRA Model Overview

Level I

PLANT MODEL

Results
Accident sequences leading to plant damage states

Level II

CONTAINMENT MODEL

Results
Containment failure/release sequences

PLANT MODE
At-power Operation
Shutdown / Transition Evolutions

Level III

SITE/CONSEQUENCE MODEL

Results
Public health effects

SCOPE
Internal Events
External Events

Uncertainties
Basic Elements of PSA

- Probability
- Combinatorial Events and Expectations
- Event Trees
- Fault Trees
- Risk
- Data
- Uncertainties
- Nuclear Power Plant PRA Structure
- Typical Results
Transition of a Risk Assessment

INITIATING EVENT STATES → PLANT DAMAGE STATES → PLANT DAMAGE STATES → RELEASE STATES → RELEASE STATES → FINAL DAMAGE STATES

PLANT MODEL | CONTAINMENT MODEL | SITE MODEL

Level 1  Level 2  Level 3
Event and Fault Tree Structure

Example of event tree analysis with fault trees
Loss-of-offsite-power event tree

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

OK
OK
PDSi
PDSj
CDF and LERF Definitions

- **Core damage frequency** is defined as the sum of the frequencies of those accidents that result in uncovery and heatup of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core (i.e., sufficient, if released from containment, to have the potential for causing offsite health effects) is anticipated.

- **Large early release frequency** is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is the potential for early health effects. Such accidents generally include unscrubbed releases associated with early containment failure shortly after vessel breach, containment bypass events, and loss of containment isolation.

At Power Level I Results

CDF = 4.5x10^{-5} / yr (Modes 1, 2, 3)

Initiator Contribution to CDF Total:

- Internal Events ..................... 56%
- External Events ..................... 44%
  - Seismic Events 24%
  - Fires 18%
  - Other 2%

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
# Level I Results

- **Functional Sequences**

<table>
<thead>
<tr>
<th>Contribution</th>
<th>CDF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transients - Station Blackout/Seal LOCA</td>
<td>45%</td>
</tr>
<tr>
<td>Transients - Loss of Support Systems/Seal LOCA</td>
<td>29%</td>
</tr>
<tr>
<td>Transients - Loss of Feedwater/Feed &amp; Bleed</td>
<td>12%</td>
</tr>
<tr>
<td>LOCA - Injection/Recirculation Failure</td>
<td>7%</td>
</tr>
<tr>
<td>ATWS - No Long Term Reactivity Control</td>
<td>6%</td>
</tr>
<tr>
<td>ATWS - Reactor Vessel Overpressurization</td>
<td>2%</td>
</tr>
</tbody>
</table>

From: K. Kiper, MIT Lecture, 2006
## At Power Level II Results

<table>
<thead>
<tr>
<th>Release Categories</th>
<th>Conditional Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large-Early</td>
<td>0.002</td>
</tr>
<tr>
<td>Small-Early</td>
<td>0.090</td>
</tr>
<tr>
<td>Large-Late</td>
<td>0.249</td>
</tr>
<tr>
<td>Intact</td>
<td>0.659</td>
</tr>
</tbody>
</table>

Large-Early Release Freq (LERF) = \(7 \times 10^{-8} \) / yr

### Large-Early Failure Mode

<table>
<thead>
<tr>
<th>Percent Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Containment Bypass</td>
</tr>
<tr>
<td>Containment Isolation Failure</td>
</tr>
<tr>
<td>Gross Containment Failure</td>
</tr>
</tbody>
</table>

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see [http://ocw.mit.edu/fairuse](http://ocw.mit.edu/fairuse).
SHUTDOWN

Shutdown, Full Scope, Level 3 PSA (1988)

Results: \( \text{Mean CDF}_{\text{shutdown}} \sim \text{Mean CDF}_{\text{power}} \)

- Dominant CD sequence:
  \textit{Loss of RHR at reduced inventory.}

- Risk dominated by operator actions - causing and mitigating events.

- Significant risk reductions with low-cost modifications and controls.
  Midloop level monitor, alarm
  Procedures, training
  Administrative controls on outage planning

From: K. Kiper, MIT Lecture, 2006

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Shutdown PRA Issues

- Risk is dominated by operator actions - importance of HRA.
- Generic studies give useful insights, but risk-controlling factors are plant-specific.
- Shutdown risk is dynamic - average risk is generally low (relative to full power risk), but is subject to risk “spikes.”
- Shutdown risk is more amenable to “management.”

From: K. Kiper, MIT Lecture, 2006

Source unknown. All rights reserved. This content is excluded from our Creative Commons license.
For more information, see http://ocw.mit.edu/fairuse.
## Integrated Risk (All Modes) – 2002 Update

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>CDF</th>
<th>Percent of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode 1</td>
<td>Full-power (&gt;70% pwr)</td>
<td>4.28 E-5</td>
<td>63%</td>
</tr>
<tr>
<td>Mode 2</td>
<td>Low-power (&lt;70% pwr)</td>
<td>0.15 E-5</td>
<td>2%</td>
</tr>
<tr>
<td>Mode 3</td>
<td>Hot Standby</td>
<td>0.08 E-5</td>
<td>1%</td>
</tr>
<tr>
<td>Mode 4</td>
<td>Hot Shutdown</td>
<td>0.05 E-5</td>
<td>1%</td>
</tr>
<tr>
<td>Mode 5</td>
<td>Cold Shutdown</td>
<td>0.91 E-5</td>
<td>13%</td>
</tr>
<tr>
<td>Mode 6</td>
<td>Refueling</td>
<td>1.38 E-5</td>
<td>20%</td>
</tr>
<tr>
<td></td>
<td><strong>Total Core Damage Frequency</strong></td>
<td><strong>6.86E-5</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see [http://ocw.mit.edu/fairuse](http://ocw.mit.edu/fairuse).
Risk Assessment Review Group

- “We are unable to define whether the overall probability of a core melt given in WASH-1400 is high or low, but we are certain that the error bands are understated.”

- WASH-1400 is "inscrutable."

- "…the fault-tree/event-tree methodology is sound, and both can and should be more widely used by NRC."

- "PSA methods should be used to deal with generic safety issues, to formulate new regulatory requirements, to assess and revalidate existing regulatory requirements, and to evaluate new designs."

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Commission Actions (Jan. 18, 1979)

- “…the Commission has reexamined its views regarding the Study in light of the Review Group’s critique.”

- “The Commission withdraws any explicit or implicit past endorsement of the Executive Summary.”

- “…the Commission does not regard as reliable the Reactor Safety Study’s numerical estimate of the overall risk of reactor accidents.”

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Zion and Indian Point PRAs (1981)

- First PRAs sponsored by the industry.
- Comprehensive analysis of uncertainties (Bayesian methods).
- Detailed containment analysis (not all accidents lead to containment failure).
- “External” events (earthquakes, fires) may be significant contributors to risk.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Additional System Failures/ Human Actions</th>
<th>Resulting Dependent Failures</th>
<th>Sequence Frequency (per reactor year)</th>
<th>Sequence Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Offsite Power</td>
<td>Onsite AC Power, No Recovery of AC Power Before Core Damage</td>
<td>Component cooling, high pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>- 3.3-5</td>
<td>Core Melt 1, Latent Health Risk 1, Early Health Risk *</td>
</tr>
<tr>
<td>Loss of Offsite Power</td>
<td>Service Water, No Recovery of Offsite Power</td>
<td>Onsite AC power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>9.2-6</td>
<td>2, 2, *</td>
</tr>
<tr>
<td>Small LOCA</td>
<td>Residual Heat Removal</td>
<td>None.</td>
<td>8.9-6</td>
<td>3, *, *</td>
</tr>
<tr>
<td>Control Room Fire</td>
<td>None</td>
<td>Component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>8.7-6</td>
<td>4, 3, *</td>
</tr>
<tr>
<td>Loss of Main Feedwater</td>
<td>Solid State Protection System</td>
<td>Reactor trip, emergency feedwater, high and low pressure makeup (ECCS), containment filtration and heat removal.</td>
<td>8.3-6</td>
<td>5, 4, *</td>
</tr>
<tr>
<td>Steam Line Break Inside Containment Heat Removal</td>
<td>Operator Failure to Establish Long Term</td>
<td></td>
<td>5.6-6</td>
<td>6, *, *</td>
</tr>
<tr>
<td>Reactor trip</td>
<td>Component Cooling</td>
<td>High and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>4.6-6</td>
<td>7, 5, *</td>
</tr>
<tr>
<td>Loss of Offsite Power</td>
<td>Train A Onsite Power, Train B Service Water, No Recovery of AC Power Before Core Damage</td>
<td>Train B onsite power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>4.4-6</td>
<td>8, 6, *</td>
</tr>
<tr>
<td>Loss of Offsite Power</td>
<td>Train B Onsite Power, Train A Service Water, No Recovery of AC Power Before Core Damage</td>
<td>Train A onsite power, component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration and heat removal.</td>
<td>4.4-6</td>
<td>9, 7, *</td>
</tr>
<tr>
<td>PCC Area Fire</td>
<td>None</td>
<td>Component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, containment filtration, and heat removal.</td>
<td>4.1-6</td>
<td>10, 8, *</td>
</tr>
</tbody>
</table>

*Negligible contribution to risk.

NOTE: Exponential notation is indicated in abbreviated form; i.e., 3.3-5 = 3.3 × 10^-5.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
NUREG-1150 and RSS CDF for Peach Bottom

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Comparison of Iodine Releases (Peach Bottom)

Note: Shaded area indicates reduction in median releases between WASH-1400 and NUREG-1150.
Early and latent cancer mortality risks to an individual living near the plant should not exceed 0.1 percent of the background accident or cancer mortality risk, approximately $5 \times 10^{-7}$/year for early death and $2 \times 10^{-6}$/year for death from cancer.

- The prompt fatality goal applies to an average individual living in the region between the site boundary and 1 mile beyond this boundary.
- The latent cancer fatality goal applies to an average individual living in the region between the site boundary and 10 miles beyond this boundary.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see [http://ocw.mit.edu/fairuse](http://ocw.mit.edu/fairuse).
Societal Risks

- **Annual Individual Occupational Risks**
  - All industries: $7 \times 10^{-5}$
  - Coal Mining: $24 \times 10^{-5}$
  - Fire Fighting: $40 \times 10^{-5}$
  - Police: $32 \times 10^{-5}$
  - US President: $1,900 \times 10^{-5}$ (!)

- **Annual Public Risks**
  Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see [http://ocw.mit.edu/fairuse](http://ocw.mit.edu/fairuse).
  - Total: $870 \times 10^{-5}$
  - Heart Disease: $271 \times 10^{-5}$
  - All cancers: $200 \times 10^{-5}$
  - Motor vehicles: $15 \times 10^{-5}$

Subsidiary Goals

- The average core damage frequency (CDF) should be less than $10^{-4}$/ry (once every 10,000 reactor years)

- The large early release frequency (LERF) should be less than $10^{-5}$/ry (once every 100,000 reactor years)

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.
Large Early Release Frequency

- LERF is being used as a surrogate for the early fatality QHO.

- It is defined as the frequency of those accidents leading to significant, unmitigated releases from containment in a time frame prior to effective evacuation of the close-in population such that there is a potential for early health effects.

- Such accidents generally include unscrubbed releases associated with early containment failure at or shortly after vessel breach, containment bypass events, and loss of containment isolation.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license.
For more information, see http://ocw.mit.edu/fairuse.
PRA Model Overview and Subsidiary Objectives

Level I

**PLANT MODEL**

- Results
  - Accident sequences leading to plant damage states

Level II

**CONTAINMENT MODEL**

- Results
  - Containment failure/release sequences

Level III

**SITE/CONSEQUENCE MODEL**

- Results
  - Public health effects

---

**SCOPE**

- PLANT MODE
  - At-power Operation
  - Shutdown / Transition
  - Evolutions

- QHOs
  - Internal Events
  - External Events

---

Massachusetts Institute of Technology
Department of Nuclear Science & Engineering

Prof. Andrew C. Kadak, 2008
Page 42
Risk cannot be justified save in extraordinary circumstances

Control measures must be introduced for risk in this region to drive residual risk towards the broadly acceptable region

Level of residual risk regarded as insignificant -- further effort to reduce risk not likely to be required

Increasing individual risks and societal concerns

UNACCEPTABLE REGION

TOLERABLE REGION

BROADLY ACCEPTABLE REGION

"Acceptable" vs. "Tolerable" Risks (UKHSE)

- The use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy.

- PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements.

Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/fairuse.

Comply with Regulations

Maintain Defense-in-Depth Philosophy

Maintain Safety Margins

Integrated Decision Making

Risk Decrease, Neutral, or Small Increase

Monitor Performance
Acceptance Guidelines for Core Damage Frequency

Region I
- No changes
Region II
- Small Changes
- Track Cumulative Impacts
Region III
- Very Small Changes
- More flexibility with respect to Baseline
- Track Cumulative Impacts
Risk-Informed Framework

Traditional “Deterministic” Approaches

- Unquantified Probabilities
- Design-Basis Accidents
- Structuralist Defense in Depth
- Can impose heavy regulatory burden
- Incomplete

Risk-Informed Approach

- Combination of traditional and risk-based approaches

Risk-Based Approach

- Quantified Probabilities
- Scenario Based
- Rationalist Defense in Depth
- Incomplete
- Quality is an issue
Homework

- Knief
  - Problems: 14.16, 19, 24, 28