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.
Farmer’s Paper (1967)

- 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.
Loss-of-offsite-power event tree

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

OK

OK

PDSi

PDSj
THE FARMER LINE

Source: Oak Ridge National Laboratory
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?
The Kaplan & Garrick Definition of Risk

(Risk Analysis, 1 (1981) 11-28)

\[ R = \{ < s_i, \pi_i(\varphi_i), c_i > \} \]

- \( s_i \): scenario \( i \), \( i = 1, \ldots, N \)
- \( \varphi_i \): frequency of \( s_i \) (aleatory uncertainty)
- \( \pi_i(\varphi_i) \): pdf of \( \varphi_i \) (epistemic uncertainty)
- \( c_i \): consequence \( i \)
PRA Model Overview

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

PLANT MODE
At-power Operation
Shutdown / Transition Evolutions

SCOPE
Internal Events
External Events

Uncertainties
At Power Level I Results

CDF = $4.5 \times 10^{-5}$ / yr (Modes 1, 2, 3)

Initiator Contribution to CDF Total:

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

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
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

Courtesy of K. Kiper. Used with permission.
At Power Level II Results

Release Categories

- Large-Early 0.002
- Small-Early 0.090
- Large-Late 0.249
- Intact 0.659

Large-Early Release Freq (LERF) = 7x10^{-8} / yr

Large-Early Failure Mode

- Containment Bypass 82%
- Containment Isolation Failure 18%
- Gross Containment Failure 0.1%

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
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.
  - \textit{Midloop level monitor, alarm}
  - \textit{Procedures, training}
  - \textit{Administrative controls on outage planning}

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
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.” At-power risk is designed in.
## 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>
</tbody>
</table>

- Total Core Damage Frequency: 6.86E-5 100%

From: K. Kiper, MIT Lecture, 2006

Courtesy of K. Kiper. Used with permission.
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)

Source: WASH-1400, U.S. AEC.
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."
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.”
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.
Example PRA Results

M.I.T. Dept. of Nuclear Engineering
Department of Nuclear Science and Engineering

Courtesy of K. Kiper. Used with permission.
### Summary of Accident Sequences with Significant Risk and Core Melt Frequency Contributions

<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>1 1 *</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>0.9-6</td>
<td>3 *</td>
</tr>
<tr>
<td>Control Room Fire</td>
<td>None</td>
<td>None</td>
<td>0.7-6</td>
<td>4 3 *</td>
</tr>
<tr>
<td>Loss of Main Feedwater</td>
<td>Solid State Protection System</td>
<td>Component cooling, high and low pressure makeup (ECCS), reactor coolant pump seal LOCA, 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>Reactor trip, emergency feedwater, high and low pressure makeup (ECCS), containment filtration and heat removal</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>4.5-6</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.

Courtesy of K. Kiper. Used with permission.
NUREG-1150 and RSS CDF for Peach Bottom
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.
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**
  - 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)
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.
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

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

SCOPE
- Internal Events
- External Events

CDF 10^{-4}$/ry
LERF 10^{-5}$/ry
QHOs

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

- **UNACCEPTABLE REGION**
  - Risk cannot be justified save in extraordinary circumstances

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

- **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

- 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.

- 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
  - Realistic
- Rationalist Defense in Depth
  - Incomplete
  - Quality is an issue