Deterministic & Probabilistic Safety Assessment

How much do we know about the risk associated with operation of nuclear power plants?

Mohsen Khatib-Rahbar
Energy Research, Inc.
Ecole Normale Supérieure
Paris, 14-16 November 2011

Energy Research, Inc.
6167 & 6189 Executive Boulevard
Rockville, Maryland 20852
E-Mail: mkr1@eri-world.com
Outline

- Background
- Defense-in-depth
- Deterministic Approach to Licensing & Safety
- Corner-Stone of Reactor Safety
- Probabilistic Approach to Safety Assessment
- Major Sources of Uncertainties
- Typical Risk of Severe Accidents
- Summary
Background

- Nuclear power plants were designed with the ultimate aim of:
  - Preventing release of radioactivity to environment in order to ensure public health and safety.
  - Striving to assure that nuclear power does not contribute significantly to individual and societal health risks
- For light water reactors this philosophy has been historically implemented through deterministic requirements for emergency core cooling systems aimed at preventing fuel overheating during abnormal and accident conditions.
Background – Cont.

● Reactor safety is extensively regulated. It is required to have:
  - Permit/license for siting, plant construction, plant operation, plant modification, etc.
  - Detailed safety analyses/positions that are extensively documented, verified and supported by experimental/test data.
  - Follow and satisfy detailed regulatory requirements, which are often prescriptive (and lean towards large conservatisms)

● Nuclear safety is not a constant of time (i.e., regulatory requirements change/evolve)

● Plant owners are concerned with constructing, operating and maintaining “safe” facilities that are “economically” feasible (e.g., construction costs, licensing costs, operational efficiency, capacity factor, fuel cycle costs, maintenance costs, etc.). Balance between:
  - Safety
  - Economics
Defense in Depth Approach to Safety

- In the early days of nuclear power development, it was recognized that standards that need to be observed for nuclear power plant safety needed to be higher than other industrial facilities.
  - Concept of “defense-in-depth” became the cornerstone of nuclear power development

- Defense-in-depth is a design safety philosophy that uses:
  - Multiple lines of defense,
  - Conservative design,
  - Conservative evaluation methods, and
  - Conservative regulatory limits

That are employed to ensure that public health and safety is protected.

- The philosophy intended to ensure that a plant design is tolerant to uncertainties in knowledge of plant behavior, component reliability, or operator performance that might potentially compromise safety.
Concept of Multiple Barriers

- Nuclear plants are designed with:
  - Multiple,
  - Independent, and
  - concentric barriers

to radionuclide release and transport.

First barrier: fuel encased in cladding
Second barrier: reactor coolant system boundary
Third barrier: leak-tight containment building
Assurance of Defense in-Depth Principles

- Provides for accident prevention through:
  - Sound engineering design that can be built and operated with stringent quality standards.
  - High degree of freedom from failures and errors.
  - High tolerance for malfunctions, should they occur.
  - Tested components and materials.
  - Redundancy of instrumentation and controls.

- Assumes there will be human or equipment failure:
  - Provides protection systems to maintain safe operation or achieve stable plant state when events occur.
    - Redundant sources of in-plant electricity.
    - Sensitive detection systems to warn of incipient failure of fuel cladding or coolant systems.
    - System for automatic shutdown (“SCRAM”) of reactors on signal from monitoring instruments.

- Provides for consequence mitigation through:
  - Requirement for siting and adequate exclusion boundary.
  - Conservative design and construction with stringent quality standards.
  - Requirements for testing (e.g., containment leak tightness).
  - Requirements for protection against radiological releases (e.g., release mitigation).
  - Emergency planning
Deterministic Approach to Licensing & Safety

- Designs primarily based on prescriptive/deterministic requirements & safety evaluation techniques:
  - To reduce the likelihood of accidents that can result in fuel damage & radiological releases through careful/balanced design, construction and operation
  - To prevent damage to fuel, should events/accidents occur (i.e., emergency core cooling systems)
  - To mitigate consequences of fuel/core damage, should they occur (i.e., remote siting, containment system, and emergency planning)

- Even though potential for core/fuel damage are qualitatively considered, nonetheless, they are expected to have a low probability and low consequences, given the defense-in-depth design philosophy and the deterministic requirements.

- Concept of “Design Basis Accidents (DBAs)” used to assess plant performance as part of deterministic licensing basis:
  - DBA is a postulated accident that a plant must be designed and built to withstand without loss to the systems, structures, and components that are necessary to ensure public health and safety
Deterministic Approach – Cont.

- Analysis method shall either follow a “conservative” methodology (e.g., Appendix K) to calculate post loss of coolant accident (LOCA) conditions (e.g., maximum fuel cladding temperature) based on prescribed:
  - Models,
  - Correlations,
  - Input data,
  - Accident condition (e.g., break size, break location, etc.)
  - System configuration (e.g., simultaneous loss of AC-power, assumed failure of an active system involved in mitigating the accident, etc.)

- Conservative Acceptance Criteria – for example:
  - Peak cladding temperature < 2200°F (1204°C)
  - Maximum Cladding Oxidation shall not exceed 0.17 x max clad thickness before oxidation

- Alternatively, analyses can use a “best estimate” approved methodology, but they must account/quantify the uncertainties
Deterministic Approach – Cont.

Acceptance Criterion

2200°F (1204°C)

Margin

Unacceptable

Acceptable

Calculated Parameter (e.g., maximum cladding temperature)

Conservative Estimate

Best Estimate

Time
Cornerstone of Reactor Safety

- Remote siting
- Design Basis Accidents (DBAs)
- Deterministic analysis for DBAs
- Deterministic acceptance criteria for:
  - Reactor fuel,
  - Reactor coolant system,
  - Containment performance,
  - Etc.
Transition to Risk Approach to Reactor Safety

- The deterministic basis for regulation continues to this day; however, in early 1970’s initiatives started for “quantitative” measures of risk.
- Farmer proposed a limit line for accidental releases.
  - When potential accidents found to fall below the line, they were considered acceptable.
  - When potentials found to fall above the line, they were considered unacceptable:
    - Measures would have to be instituted to move them below the limit line.
Farmer’s Limit Line Approach

- Line (A) has a slope of -1, indicating an equal risk acceptance for large as well as small events.
- Line (B) has a slope of -1.5, indicating a societal aversion toward the large accidents.
- To fix the limit line, the point at 1000 curies ($3.7 \times 10^{13}$ Bq*) with a frequency of one release per year of $10^{-3}$ was selected. Small accidental releases would be considered unacceptable above a frequency of $10^{-2}$ per year.

*Typical inventory for a 1100 MW plant is $3.4 \times 10^{18}$ Bq
Probabilistic Approach to Safety Assessment

- Uses reliability & probability theory to consider likelihood of events & their potential consequences:
  - Observations (actuarial data)
  - Logical & mathematical models (fault trees, event trees, decision trees, etc.).
- Methods first proposed by Watson in 1960s
- Later, methods extended/developed for application to reactor safety as part of WASH-1400 (published in 1975).
- Extensive criticism of WASH-1400 deflected attention from strengths/merits of Probabilistic Risk/Safety Assessment (PRA/PSA)-based methods
- Accident at Three Mile Island in 1979 helped refocus attention to merits of PRA/PSA techniques

Fundamental conclusion of WASH-1400:
- Design Basis Accident (DBA) concept, although powerful in developing designs with substantial margin, does not address all of the issues related to severe accidents.
- Other accidents more likely & potentially more challenging to the reactor system and containment.
Probabilistic Safety Assessment

• Risk can be defined as a triplet:
  Risk = (Frequency of Undesirable Events) X
  (Conditional Probability of Damage) X
  (Consequences)

• Frequencies based on actuarial data & statistical methods

• Conditional damage probabilities based on:
  - Logic models (fault trees/event trees) for components and systems.
  - Physical/chemical models to determine outcomes of “uncertain” processes that impact progression of accidents

• Use mathematical models to calculate consequences associated with release of fission products/radionuclides to environment

PSA is an integration of “probabilistic” and “deterministic” concepts to arrive at conclusions on safety of complex engineering system
PRA/PSA Process

- Three distinct levels to PRA/PSA:
  - Level-1: Given an initiating event and using integrated logic (fault & event trees) calculates **Core Damage Frequency (CDF)** in units of per reactor-year of operation for each initiator
  - Level-2: Starting at core damage and using integrated logic models together with models for physical processes calculates **conditional probability** (due to uncertainties in phenomenological processes) associated with **quantity of radioactivity** released from containment to environment
  - Level-3: Starting from release of radioactivity and using models for dispersion, uptake of radionuclides and economic aspects to calculate **consequences** (e.g., health effects, property damage, etc.) in units of number of consequences (e.g., fatalities, injuries, Euros, etc.)

- So-called “initiating events” considered include:
  - Internal to plant systems (e.g., pipe break)
  - Internal & external floods, fires, etc.
  - Earthquakes
  - Tsunamis, aircraft crash, etc.

- Modes of operation include power operation, refueling, shutdown and accident involving spent fuel pools
Level-1 PRA/PSA Process

- Initiating Event Analysis
- Success Criteria/Accident Sequences
- Data Analysis
- Systems Analysis
- Human Reliability Analysis
- Quantification
Level-2 PRA/PSA Process

Level-1 PSA Results:
- Indicators
- Cutssets
- System status
- Relevant AM actions
- Uncertainties
- Etc.

Level-1/Level-2 PSA Interface

Accident Progression Event Time

- RB
- RB
- RB

- RB frequency
- Uncertainties in RB

- Source Term Model
- Experimental data
- Literature information
- Subjective judgment

- Source Term Characteristics
- Release Frequencies
- Risk Results (e.g., risk of activity)

Load Fractility

- Physical Process Model
- Experimental Data
- Literature Information
- Subjective Judgment

FDs
- FDs Frequencies
- Uncertainties in FDs Frequencies

Release Bos attributes

Containment systems & FDs Attributes

Level-3 PRA/PSA Process

Release magnitudes & composition
Xe 100%
I 45%
Cs 30%
Sr 10%

Consequence Analysis Model
- Number of Early Fatalities
- Number of Cancers
- Economic impact ($)

14-16 November 2011
**Major Sources of Uncertainties (Level-1 PSA)**

- **Initiating event frequencies for rare events:**
  - Pipe Breaks (also affects internal floods)
  - High (Magnitude) Acceleration Seismic Hazard
    - Events of high frequency based on actual data
    - Events at low frequency based on models and expert judgment (both source & attenuation)
  - Major External Floods Hazard (same as seismic for low frequency high impact)
  - Absence of multiple simultaneous events (not currently modeled)

- **Human Reliability (worse for seismic and fire):**
  - Feasibility & timing of recovery following natural phenomena events
  - Low confidence in models
  - Difficulty in interpreting human performance data

- **Fire severity (modeling):**
  - Propagation
  - Heat release rates
  - Duration

- **Fire detection (very limited credit for very early warning fire detection systems)**
- **Seismic response estimates (typically large uncertainties)**
- **Seismic-induced fire (considered qualitatively; however, consequential impacts not known)**
Major Sources of Uncertainties (Level-2 PSA)

- In general, uncertainties are due to:
  - Randomness/stochastic ("Aleatory") - arise because of natural, unpredictable variations: Expert knowledge cannot reduce aleatory uncertainties, but it can help to quantify (irreducible uncertainty)
  - State-of-knowledge ("Epistemic") – arise because of incomplete knowledge: Conceptually, Epistemic uncertainties can be narrowed over time.

- Uncertainties associated with core damage progression (severe accidents) and radionuclide releases are, for the most part, Epistemic in nature
Severe Accidents

- These accidents are characterized by a permanent imbalance (i.e., failure and/or partial failure of emergency systems) in heat generation & heat removal. They include two fundamental classes:
  - Under-cooling events (i.e., TMI-2 and Fukushima Dia-ichi), and
  - Overpower events (i.e., Chernobyl)
- Involve very complex chemical & physical processes:
  - Multiple components & phases
  - Numerous time scales
  - Materials interactions
- Limited large scale tests & data
- TMI-2 (PWR) provided considerable insights.
- Fukushima (BWR) expected to provide considerable insights (in time)

Uncertainties in prediction of severe accidents and radiological releases

14-16 November 2011
Nuclear Risk and Public Decision-Making Scientific Conference
Reasons for Understanding Severe Accidents

- Evaluate response of plants for a spectrum of severe accident conditions to determine whether design/procedural modifications are warranted.
  - Accident prevention and/or
  - Accident mitigation

- Understand nature of accidents to determine most effective actions to mitigate/manage severe accidents

  - Confidence in estimating risk associated with severe accidents.
  - To improve designs/operations & eliminate potential vulnerabilities
Key Events & Their Significance

- **Core Uncovery** – Challenges fuel integrity
- **Metal Oxidation** – Release of hydrogen to containment
- **Core Damage** – Releases radionuclides to containment
- **Failure of Steam Generator Tubes (PWRs)** – Containment bypass (Radionuclides released to environment.
- **Failure of Reactor Pressure Vessel** – Molten fuel discharged to containment.
- **Failure of Containment** – Radionuclides released to environment.
# Key Phenomena & State-of-Knowledge

Resolution of uncertainties as they impact risk, design, and accident management actions

<table>
<thead>
<tr>
<th>Phenomena</th>
<th>Resolved</th>
<th>Not fully resolved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core uncovery/metal oxidation</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Melt progression (relocation, crust formation &amp; failure)</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Creep rupture of reactor coolant system pipes</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Creep rupture of steam generator tubes</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>In-vessel steam explosions</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>In-vessel cooling mechanisms</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Reactor vessel failure mode</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Lower head external cooling</td>
<td>Where possible</td>
<td></td>
</tr>
<tr>
<td>Ex-vessel steam explosions</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Direct containment heating</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>BWR (Mark I) shell melt-through</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Ex-vessel debris cooling*</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Hydrogen distribution &amp; combustion</td>
<td>combustion</td>
<td>distribution</td>
</tr>
</tbody>
</table>

* Close to resolution
## Typical Risk of Severe Accidents (PWR)

<table>
<thead>
<tr>
<th>Class of Sequences</th>
<th>CDF (per reactor-year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station Blackout</td>
<td>1E-6 (50%)</td>
</tr>
<tr>
<td>Other Transients</td>
<td>4E-7 (20%)</td>
</tr>
<tr>
<td>LOCAs</td>
<td>5E-7 (25%)</td>
</tr>
<tr>
<td>SGTR</td>
<td>1E-7 (5%)</td>
</tr>
<tr>
<td>LOCA Outside Containment</td>
<td>7E-9 (&lt;&lt;1%)</td>
</tr>
<tr>
<td>Total Core Damage Frequency</td>
<td>2E-6 (100%)</td>
</tr>
</tbody>
</table>
Typical Uncertainties in Risk Estimates (PWR)

Plant Damage State

5th percentile ○ 50th percentile ● Mean ○ 95th percentile
Typical Uncertainties in Risk Estimates (PWR)
Typical Uncertainties in Risk Estimates (BWR)

Core Damage Frequency (per reactor year)
Summary

- Deterministic safety assessment, although powerful for design; however, not sufficient to fully ensure safety
- Probabilistic risk/safety assessment, despite uncertainties, provides the best means for identifying design and operational vulnerabilities
- Despite uncertainties in assessment of severe accidents, improvements to design, accident management actions, and operator training can be realized
- In the aftermath of TMI-2, through research, technical improvements, and collaborations, significant improvement in plant safety was realized
- The Fukushima Dia-ichi events are no exception
  - Improvements in ways of assessing risk; and identifying additional changes to designs, operations, and emergency procedures are inevitable
  - Technology improvements provide higher levels of standards that public is likely to demand
- Increasing knowledge-base, lessons learned from accidents, and continued R&D can only enhance our ability to assess the risk associated with operation of nuclear power plants; therefore:
  
  continue to learn more about risk contributors, and as a result, safety enhancements will continue to emerge