IMPLICATIONS OF NUCLEAR POWER PLANT REGULATION FOR FUTURE NUCLEAR PLANTS BASED ON RISK AND PERFORMANCE INFORMATION

Mohammad Modarres
Professor, Nuclear Engineering Program and
Reliability Engineering Program
University of Maryland

Why We Need A New Approach?

- Current Regulations Are:
  - Largely LWR Design-Specific
  - Evolved, But Fundamentally 50-Years Old
  - Case-by-Case Reviews, Exemptions, Etc.
  - Highly Deterministic
- New and Future Designs Will Be:
  - Diverse with Unconventional Interfaces
  - Standard and Mostly Modular
  - Run with 50-Years of Nuclear Operating Experience
  - Advanced Fuel-Cycles
- Present Safety Regulating Paradigm Need Serious Review

Some Facts

- Safety Regulation Is Used To Ensure That The Thing or Organization Will Do Only What It Is Meant To Do.
- We must Know the behaviors (functions) of the thing or organization
- Lack of knowledge = Uncertainty
- Therefore, Safety Regulation (Preventing, Protecting, and Mitigating Harm) Must Characterize Uncertainties
- Everything Is Uncertain to Varying Degrees Including Every Engineering Principle, Law, Process, Etc.

Some History

- U.S. Atomic Energy Act of 1946 rests atomic technology and military applications with Government.
- U.S. Act of 1954 ended the government's monopoly and made peaceful uses of atomic energy provided that: " . . . a *reasonable assurance* exists that such uses would not result in undue risks to the health and safety of the public"
- Defense-in-Depth was a consequence of having *imprecise knowledge* about safety system *design margins* in the early days nuclear power

Defense-In-Depth

In the ensuing years, the defense-in-depth evolved into a collection of design and operating requirements to overcome lack of precise knowledge:

- Use of multiple active and/or passive engineered barriers to rule out any single failures.
- Use of large design margins about performance of safety barriers under normal or accident conditions.
- Application of quality assurance in manufacturing and construction.
- Operation within predetermined safe design limits.
- Continuous testing, inspections, and maintenance to preserve original design margins.

Defense-In-Depth (Cont.)

- Acceptance criteria needed to measure the extent of conformance to the defense-in-depth, so a reactor system was "safe"
  - If it could withstand a fixed set of accident scenarios *judged* by experts as most significant adverse events (DBAs).
  - If a plant can handle the DBAs, then it can handle any other accidents
  - Thus reasonable assurance in this context meant conformance to the body of regulations built in the basis of defense-in-depth.

- Acceptances Criteria Measured Deterministically with Conservative Methods or Bounds

Emergence of PSA and Objectives of this Paper

- In the mid-1960s, safety concerns such as containment integrity under LOCA paved the way for use of PSA methods to address the shortcomings of the DBAs by modeling considerably more realistic accident scenarios
- This Paper Propose that PSA Plays an Integral Role on Regulating Future Nuclear Power Plants

Goal-Driven Regulatory Paradigm

- Sets overarching objectives to achieve or maintain without mandating a solution
- Adds systematic structure to the traditional performance-based regulation
- Guides the regulators and licensees to select appropriate goals that conform with the overarching objectives and means to monitor them
- Uses “best-estimate” means and probabilistic-based conformance methods
- Relies on Risk-Informed mostly Probabilistic-Based Acceptance Criteria

Goal-Driven Regulatory Paradigm (Cont.)

- Uses a Top-Down approach to establish clear links between the overarching objectives, critical safety functions, and safety (or hazard) barriers (e.g., SSCs, human interventions)
- At each level, the regulator may require explicit safety and other *goals*, convincing *methods and arguments* to justify the goals are met and adequate *evidence* to support the arguments exist.
- In practice the rigor of the arguments and the amount of evidence will depend on the safety significance

Performance Measures

- In safety regulation, *performance* may be measured by two core constituents : *Capability* and *Availability*
- Capability is the ability of an SSC to realize its intended function(s) under all possible conditions (normal and accidental). For example to assure that an ECCS has the capacity (e.g., adequate flow) to overcome all challenges (e.g., PSA defined transients and LOCAs)
- Examples:
  - Capability Value (e.g., probability of meeting a design margin) = Pr (emergency cooling flow either natural or forced > flow needed to prevent fuel or cladding damage | small SLOCA of cold leg).
  - Capability Value (e.g., probability of reactor vessel failure) = Pr (Vessel plates and welds fracture toughness > thermally induced stress intensity | a PTS transient)
  - Capability Value (e.g., probability of support structure failure) = Pr (yielding point > applied stress | a specific seismic load of x)

Performance Measures (Cont.)

- Performance may be expressed by capability values alone, but for maintainable components and systems *availability* is the prime measure of performance.
- One may use physics-of-failure models to estimate the probability of failure of SSCs using Stress-Strength, Degradation (or Damage)-Endurance and Performance-Requirement models
- But, traditionally historical data on time of failure and time of repair are used to estimate "availability" in PSAs
- Example:
  - *Availability = Pr (component or system is in good operating condition |component or system is needed in a scenario i)*

Best Estimate Approach

- Examples of Overarching Objectives: Present safety goals, surrogate objectives, radiation protection, additional quantifiable security objectives
- Use of PSA approach to estimate whether a safety function, system or technology agrees with the objectives
- Best-estimate approach to assess performance of safety barriers that support or realize safety functions including characterization of epistemic and aleatory uncertainties;
- Use of traditional defense-in-depth concept for cases where there are substantial lack of knowledge (Unknown unknowns!)
- Continuous monitoring of safety and security-critical elements and periodic reassessment of risk and security and its trend to maintain agreement with the goals and overarching objectives

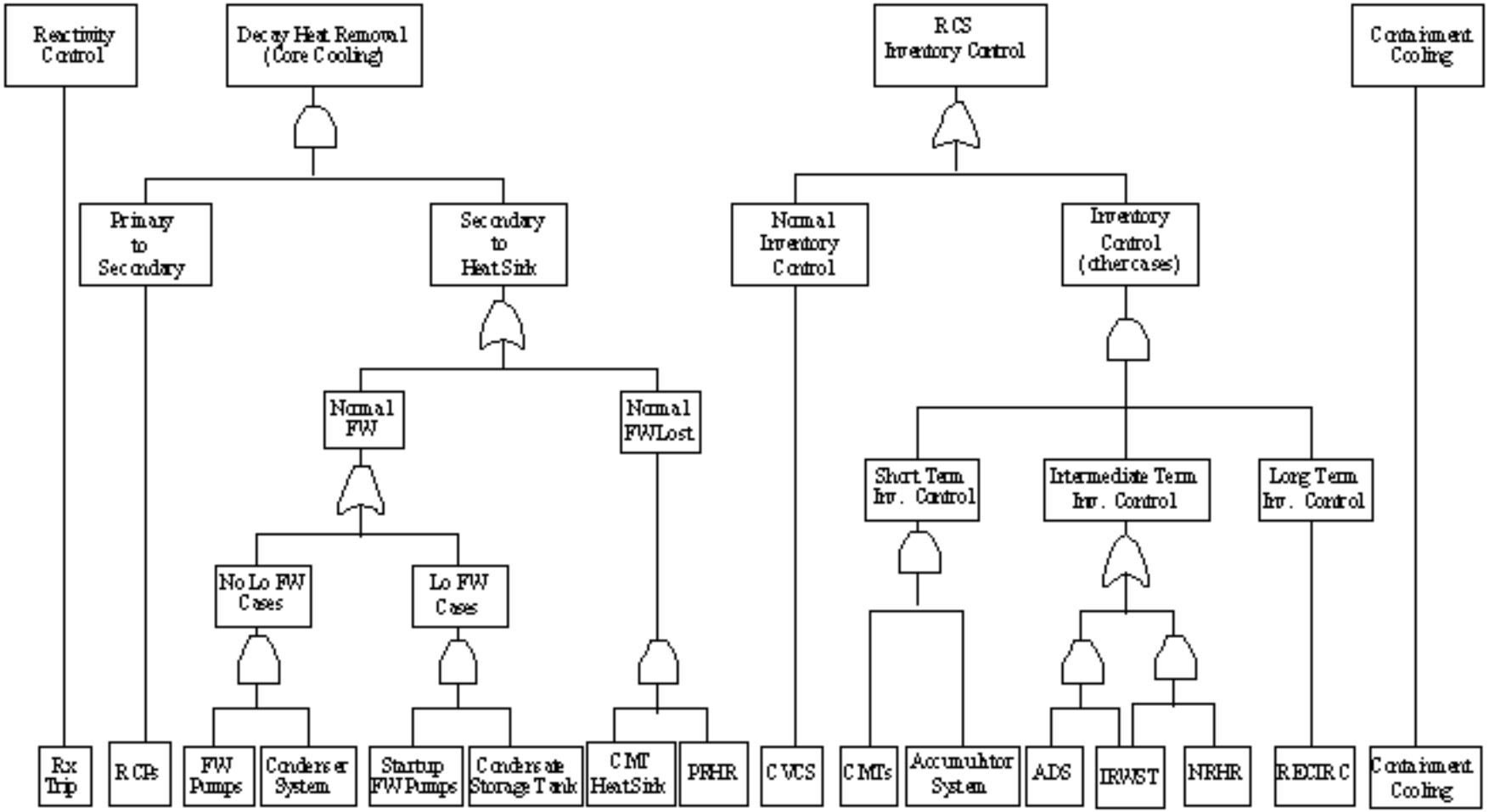
Examples of Overarching Objectives

- Core Integrity (No radiation released from the core; No more than a fixed number of events/year identified as significant precursor of accidents; No statistically significant adverse trends in performance of SSCs)
- Containment Integrity (No radiation or less than a minimal release to the environment)
- Plant Security (No intentional harm inflicted; No breakdown of physical security that weakens protection against radiological sources; prevent sabotage, theft or diversion of special nuclear materials in accordance with abnormal occurrence criteria)

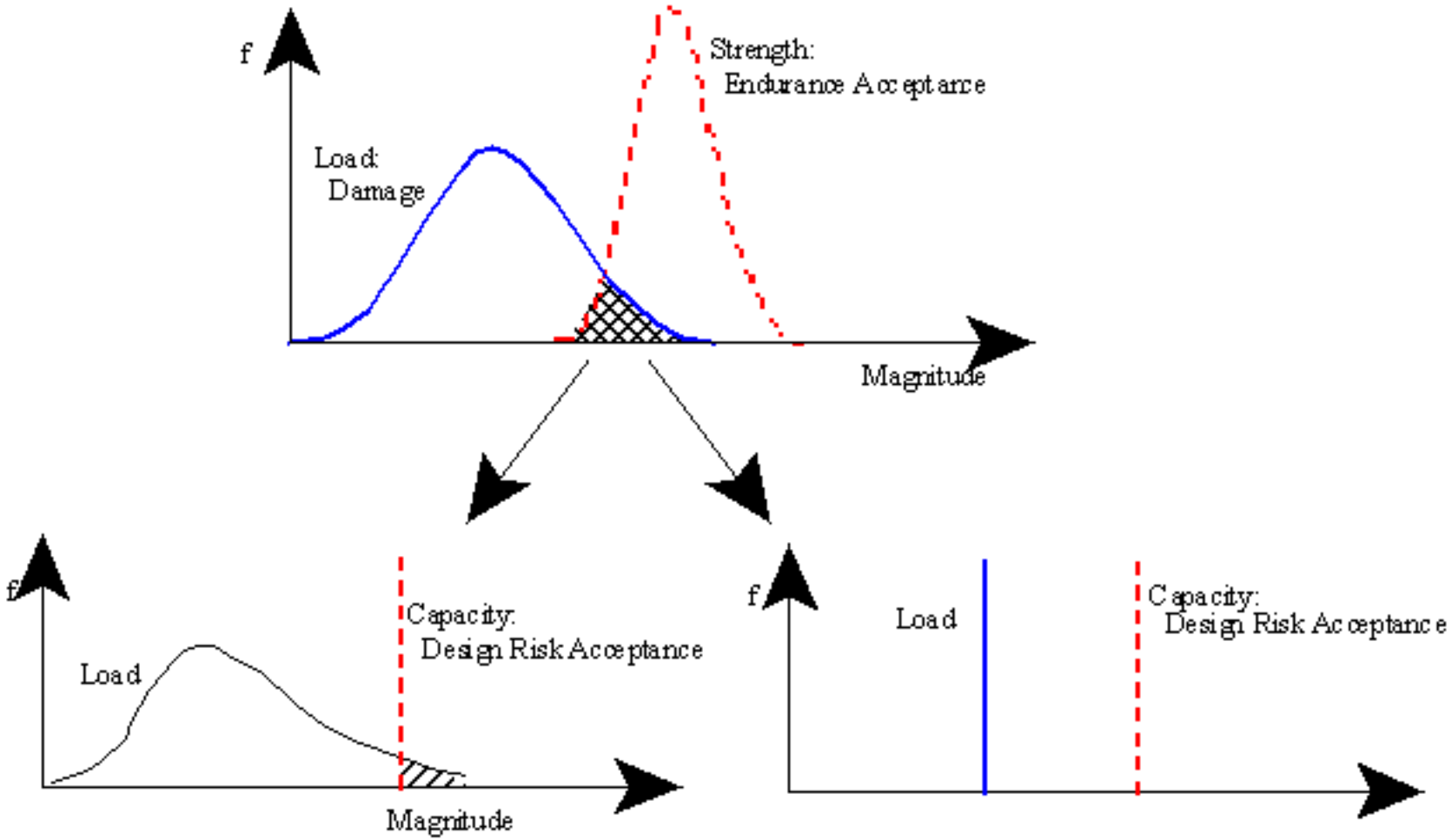
Examples of Overarching Objectives (cont.)

- Radiation Protection (Radiation exposure standards are met, No radiation overexposures from nuclear reactors accidents that exceed applicable regulatory limits; No more than a fixed number of radiation releases per year to the environment that exceed the regulatory limits)
- Organizational Safety (Programs, processes and safety culture that support safety requirements)
- Emergency Preparedness (Plans, drills assure adequate response to emergency situations)

A Top-Down Plant Model



Probabilistic Performance Analysis



Conclusions

- Goals-driven risk-informed performance-based approach to regulation provides the opportunity to characterize all uncertainties including engineering ones into the regulatory process
- Empowers innovation in reactor design and safety methods
- Allows a body of regulations independent of the reactor design

Thank you!

Questions?