PSA for Design Certification and Combined License Applications

Mr. John Stetkar
Advisory Committee on Reactor Safeguards (ACRS)

Quadripartite Working Group Meeting
October 9-10, 2008
Paris, France

Guidance on PSA for Design Certification

- Requirements in 10CFR52.47, 10CFR50.71
- Regulatory Guide 1.206, Sections C.I.19 and C.III.1.19 – "Combined License Applications for Nuclear Power Plants", June 2007
- Standard Review Plan NUREG-0800, Section 19.0 – "Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors", Revision 2, June 2007
- Interim Staff Guidance COL/DC-ISG-003 – "Probabilistic Risk Assessment Information to Support Design Certification and Combined License Applications", June 2008

PSA Purpose

- Licensing Stage
  - Design Certification (DC)
  - Combined License (COL)
- PSA Applications
  - Regulatory compliance
  - Classification of structures, systems, components (SSCs)
  - Risk-informed Technical Specifications, testing, maintenance, etc.

PSA Required Scope

- Level 1 and Level 2 PSA
  - Core damage frequency (CDF)
  - Large release frequency (LRF)
- Full-power, low-power, shutdown modes
  - Complete quantification of full-power
  - Quantitative / qualitative analyses for low-power, shutdown
- Internal events, internal hazards, external events
  - Complete quantification of internal events (including floods)
  - Quantitative / screening analyses for internal hazards, external events

Design Certification PSA Objectives

- Identify potential design features where "small number of failures" could lead to core damage or large release (including common cause failures)
- Select among alternative design options
- Demonstrate design robustness and defense-in-depth
- Reduce or eliminate known significant risk contributors of existing plants

Design Certification PSA Objectives (cont'd)

- Balance preventive and mitigative design features
- Determine risk significance of human errors
- Demonstrate risk reduction from existing plants
- Compare risk with Commission goals
  - Core damage frequency < 1×10^{-4} event / year
  - Large release frequency < 1×10^{-6} event / year
  - Containment integrity for 24 hours after core damage
  - Conditional Containment failure probability < 0.1 (composite for all core damage sequences)

Design Certification PSA Applications

- Support Regulatory Treatment of Non-Safety Systems (RTNSS)
  - Determine adequacy of proposed RTNSS scope
  - Identify specific SSCs for RTNSS
- Input to COL
  - Objectives for inspections, tests, analyses, and acceptance criteria (ITAAC)
  - Reliability assurance program (RAP)
  - Technical Specifications (TS)
  - COL action items and DC interface requirements

Combined License PSA

- "Plant-Specific" PSA
  - Changes to certified design
  - Details not specified in certified design (e.g., resolution of ITAAC and DAC)
  - SSCs outside scope of certified design (e.g., balance-of-plant systems)
  - Construction details (e.g., pipe and cable routing)
  - Operating, testing, maintenance procedures
  - Site-specific features (e.g., seismic, flooding, winds, etc.)
  - Revised / updated PSA methods, models, data

Combined License PSA (continued)

- Required prior to initial fuel loading
- Quantify all initiating events and operating modes, consistent with "NRC-endorsed consensus standards" in effect 1 year before fuel load date
- Formal submittal to NRC not required
- Full PSA must be available for NRC audit
- Report results if CDF or LRF differ by > 10% from DC PSA (positive or negative change)
- Update PSA every 4 years

PSA Quality and Level of Detail

- Determined by applications and use
- Guidance in Regulatory Guides 1.200 and 1.206, and Standard Review Plan
- NRC Interim Staff Guidance COL/DC-ISG-003
  - ASME PRA Standard (AMSE-RA-Sb-2005) high level requirements and Capability Category 1 supporting requirements "should generally be acceptable for DC or COL application"
- Independent peer review not required for DC PSA

PSA Quality and Level of Detail (continued)

- Models consistent with actual plant design
- Relevant industry operating experience and data
- Bounding assumptions for incomplete detail
- Special attention
  - Passive design features
  - New or unique equipment
  - Digital instrumentation and control systems
  - Thermal / hydraulic uncertainties (e.g., for passive system success criteria)

PSA Documentation

- Purpose and use of PSA
  - What is it used for at this stage of licensing?
  - What limitations does it contain for potential or planned future applications?
- Document all assumptions
- Document models and data in enough detail to support conclusions and reviews
- Uncertainty, importance, sensitivity analyses
- Full PSA available for NRC audits

ACRS Reviews

- Independent review of NRC Staff safety evaluation
- Public meetings with applicant and NRC Staff
- Focus on technical quality
  - PSA methods
  - Supporting analyses
  - Quality and level of detail consistent with applications
  - Results supported by models and data

ACRS Reviews (continued)

- Focused spot checks
  - Completeness / level of detail
  - Consistency with available design information
  - Success criteria and supporting analyses (Level 1 and Level 2)
  - Event tree / fault tree logic, failure modes, common cause failures
  - Assumptions
  - Data (initiating events, component failures, common cause)
  - Human reliability analysis
  - Links between Level 1 and Level 2
  - Treatment of internal hazards / external events
  - Treatment of low-power, shutdown modes

John Stetkar
Backup / Reference Material

PSA Issues for
Advanced Nuclear Power Plant Designs

Digital Instrumentation and Control

- System / subsystem failure modes
  - Valid response to untested input
  - Unintended response to valid input
  - Spurious signals
- Software reliability models
- Level of detail in hardware models
- Impacts from support system failures
- Common cause failures (hardware, software)
- Operator interactions
- Data

Passive Failure Modes

- "Traditional" screening criteria may not apply
- Functional testing not available at DC stage
  - Component status verification (flow, pressure, etc.)
  - Test intervals
- Equipment / failure modes
  - Spurious closure, opening of manual valves
  - Battery failure, degraded output
  - Explosive valve detonators
  - Plugged, fouled filters
  - Non-condensable gas intrusion

Support System Dependencies

- Incomplete information at DC stage
- DC power
  - Active equipment actuation
  - Digital instrumentation and control
  - Control room displays
- Room cooling / HVAC
  - Digital instrumentation and control equipment rooms
  - Main and emergency control rooms
- Support system initiating events
  - Screening / level of detail / grouping
  - Initiating event frequencies

Common Cause Failures

- Equipment types and failure modes
  - Passive components (e.g., check valves, batteries, etc.)
  - Digital instrumentation and control
- Common cause failure groups
- Data for new, unique components

Human Reliability Analysis

- Procedures and training information not available at DC stage
- Details of digital systems interface, control room layout, and displays may not be available at DC stage (DAC items)
- Operator reliance on automated responses
- Operator confidence in software
- Identification of error-forcing context and potential operator response

Testing and Maintenance

- Testing and maintenance procedures, programs, and schedules not available at DC stage
- Unplanned unavailability
  - All causes (e.g., repair, corrective maintenance, trouble-shooting, etc.)
  - Combinations allowed by Technical Specifications
- Planned unavailability
  - On-line preventive maintenance and overhaul
  - Coordinated by equipment divisions

Internal Hazards

- Quantification of internal floods is required
- Internal fires
  - Simplified methods allowed (e.g., EPRI FIVE)
  - Quantitative methods available (e.g., NUREG/CR-6850)
  - Lack of cable routing and room layout data at DC stage
  - Functional impacts from hot shorts
  - Likelihood of single, multiple hot shorts (e.g., considering CAROLFIRE experiments)

External Events

- Site-specific hazards not known until COL stage
- External events can be bounded at DC stage
  - Confirm bounding analyses remain valid for COL site
  - Re-analysis of hazards that are not bounded by DC PSA
  - Analysis of new site-specific hazards
- Seismic events
  - Seismic margins analysis allowed (1.67 x design-basis SSE)
  - Quantitative seismic PSA methods available
  - Both methods require seismic hazard, fragility analyses
  - Integrated Level 1 / Level 2 impacts
  - May be significant contributor to overall risk

Low Power / Shutdown Modes

- Outage plans not available at DC stage (and probably not at COL stage)
- Definition of Plant Operating States
- Status of automatic signals
- Shutdown testing and maintenance alignments
- Human-induced initiating events
- Definition of core damage / fuel damage
- Containment status and Level 2 models

Level 2 PSA

- Passive Containment heat removal
  - Thermal / hydraulic analyses and success criteria
  - Spectrum of accident scenarios
  - Experimental data
  - Impacts from non-condensable gases, debris, etc.
- Severe Accident Mitigation Guidelines
- Containment sump blockage
- Containment venting
- Performance of molten core retention systems