U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

ACRS MEETING WITH THE U.S. NUCLEAR REGULATORY COMMISSION

October 2, 2014

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Overview

John W. Stetkar

Accomplishments

- **Since our last meeting with the Commission on March 7, 2014, we issued 14 Reports**

- **Topics:**
  - **Human Reliability Analysis Models**
  - **Review and Evaluation of the Nuclear Regulatory Commission Safety Research Program**

- **Topics (cont.):**
  - **Proposed Revisions for 10 CFR 50.55a to Incorporate by Reference IEEE 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"**
  - **SECY-14-0087, "Qualitative Consideration of Factors in the Development of Regulatory Analyses and Backfit Analyses"**

- **Topics (cont.):**
  - **Chapters 3 (Partial) and 14 of the Safety Evaluation Report with Open Items for Certification of the US-APWR Design**
  - **Chapters 3 (Partial), 9, and 14 of the Safety Evaluation Report with Open Items for the Comanche Peak Nuclear Power Plant, Units 3 and 4, US-APWR Reference Combined License Application**

- **Topics (cont.):**
  - **Supplemental Safety Evaluation Report on the General Electric-Hitachi Nuclear Energy Application for Certification of the Economic Simplified Boiling Water Reactor (ESBWR) Design**
  - **Report on the Safety Aspects of the DTE Electric Company Combined License Application for Fermi Unit 3**

- **Topics (cont.):**
  - **Revised Fuel Cycle Oversight Process**
  - **Standard Review Plan Chapter 19 and Section 17.4**
  - **Peach Bottom Atomic Power Station, Units 2 and 3, Extended Power Uprate License Amendment Request**
  - **SECY-14-0016, "Ongoing Staff Activities to Assess Regulatory Considerations for Power Reactor Subsequent License Renewal"**

- **Topics (cont.):**
  - **Draft Final Design Specific Review Standard for mPower iPWR Chapter 7, Instrumentation and Control Systems**
  - **Generic Letter 20XX-XX, "Monitoring of Neutron-Absorbing Materials in Spent Fuel Pools"**

Ongoing / Future Reviews

- **New Plants**
  - **Design Certification Applications and SERs for US EPR and US-APWR**
  - **Adequacy of Long-Term Core Cooling Approach for US EPR and US-APWR**
  - **Reference COLAs for ABWR and US EPR**
  - **Subsequent COLAs for AP1000 and ESBWR**

Ongoing / Future Reviews

- **Watts Bar Unit 2**
- **PSEG Early Site Permit**
- **SHINE Medical Radioisotope Production Facility**
- **License Renewal**
  - **Callaway**
  - **Sequoyah**
  - **Byron / Braidwood**

Ongoing / Future Reviews

- **Technical Issues for Subsequent License Renewal**
  - **Concrete Structures**
  - **Reactor Vessel and Internals**
  - **Electrical Cables**
  - **Others as Identified**
- **South Texas Project Risk-Informed Resolution of GSI-191**

Ongoing / Future Reviews

- **Fukushima Proposed Rulemaking**
  - **Mitigation Strategies for Beyond-Design-Basis External Events**
  - **BWR Filtering Strategies**

Ongoing / Future Reviews

- **Risk-Informed Regulatory Framework**
  - **Risk Management Regulatory Framework**
  - **Risk Prioritization Initiative / Cumulative Effects of Regulation**
  - **Updated Regulatory Analysis Guidance**

Ongoing / Future Reviews

- **Level 3 PRA**
- **Human Reliability Analysis Methods**
- **Transitions to Risk-Informed Fire Protection Programs**
- **Westinghouse Realistic Full Spectrum LOCA Methodology**
- **Quality Assessment of Selected NRC Research Programs**

Human Reliability Analysis Models

John W. Stetkar

SRM-M061020 November 8, 2006

- **"The Committee should work with the staff and external stakeholders to evaluate the different Human Reliability models in an effort to propose either a single model for the agency to use or guidance on which model(s) should be used in specific circumstances."**
- **Staff concluded that development of a single hybrid methodology is the best approach**

ACRS Reviews

- **Subcommittee Meetings on April 7, 2010; October 18, 2010; April 20, 2011; December 14, 2011; January 16, 2013; April 24, 2013; and January 15, 2014**
- **Committee review during May 2014 meeting**
- **Letter Report issued May 14, 2014**

Work In Progress

- Work remains to refine the proposed methods and models into a form that can be used for practical human reliability analysis
- ACRS reviewed two interim work products

Psychological Foundation for HRA (NUREG-2114)

- Valuable information to improve understanding of the theoretical basis for human cognitive performance and causes for human errors
- Structured framework to assess contributions to errors in the context of evolving event scenarios
- Report should be published

IDHEAS (Integrated Decision-Tree Human Event Analysis System) Methodology

- **Elements of the methodology will enhance documentation of the human reliability analysis process, reduce analyst-to-analyst variability in its use, and improve traceability of the bases for differing assessments**

IDHEAS Recommendation 1

- **IDHEAS report should document the rationale for excluding specific cognitive mechanisms and performance influencing factors delineated in draft NUREG-2114 from explicit consideration in assessment of each crew failure mode**

IDHEAS Recommendation 2

- **Qualitative assessment guidance should emphasize need to develop operational narratives that adequately describe the entire context of the evolving event scenario**
- **Examples of good operational narratives should be provided**

IDHEAS Recommendation 3

- **A formal and complete expert elicitation process should be conducted to develop human error probabilities and associated uncertainty distributions for each combination of contextual factors**

IDHEAS Recommendation 4

- **Uncertainties in the human error probabilities should be derived directly from the expert elicitations**

IDHEAS Recommendation 5

- **Guidance for estimation of the available time window and the time required to perform each action should include explicit evaluation of the uncertainties in those times**
- **The probability that an action cannot be completed within the available time window should be included as a contribution to the overall HRA results**

IDHEAS Recommendation 6

- **Formal pilot testing of the IDHEAS methodology should be performed**
- **The testing should be conducted by multiple teams of analysts who have a range of practical experience with evaluating human performance in PRA applications**

IDHEAS Recommendation 6 (Cont.)

- Teams should include members with expertise in nuclear power plant engineering, operations, and the plant-specific PRA, as well as human performance and HRA
- Each team should evaluate the same set of PRA event scenarios that cover a range of human actions and anticipated crew failure modes

Staff Response to ACRS Recommendations

- **Staff agrees with all ACRS recommendations on the IDHEAS methodology and will address them in an update to the report**
- **Staff plans to conduct formal pilot testing of the methodology**

NRC SAFETY RESEARCH PROGRAM

Michael Corradini

Scope

- **The current safety research program organized by the Office of Nuclear Regulatory Research (RES)**
- **Fukushima: Understanding Severe Accident Progression**
- **Findings for specific RES topics**

General Observations

- The NRC has succeeded over the last few years in its effort to tie research activities it undertakes to near-term issues being confronted by its line organizations (NRO, NRR, NMSS, NSIR, and FSME).
- In some cases, research focused on organization needs may be terminated prematurely precluding appropriate and needed efforts that would be of use for future regulatory issues.

Collaborations in the Conduct of Research

- **The ACRS continues to encourage RES collaborations with other federal agencies, industry, universities, and international partners to effectively share knowledge and experience that contribute to intermediate- and long-term research objectives.**

Fukushima Forensics: Understanding Severe Accident Progression

- **The ACRS recommends that the NRC proactively engage with the Department of Energy, Japanese research organizations, and others in the international community, to focus on the forensics of the Fukushima accident.**
- **Such efforts offer a unique opportunity to better understand BWR severe accident progression, and to develop better measures for mitigating beyond-design basis events.**

Specific Research Recommendations

- **Digital I&C: We continue to recommend integration of control of access, safety, and cyber security in the design stage and licensing to ensure secure Digital I&C safety systems.**
- **Fire Safety: Initiate R&D to include: early detection of incipient fire, effects from fire damage and heat on fiber optic cable, cabinet fire heat release rates.**
- **Reactor Fuel: Extended burnup and fuel performance simulation will require RES to develop analytical methods to evaluate proposed changes in fuels.**

Specific Research Recommendations

- **Materials & Metallurgy: We continue to support the active participation in international efforts relating to materials degradation, such as International Cooperative Group on Environmentally Assisted Cracking (ICG-EAC).**
- **PRA: RES initiate efforts to ensure that an appropriate characterization of uncertainty is performed in all agency analyses.**
- **Thermal-Hydraulics: RES should maintain independent confirmatory capabilities that keep pace with such developments in industry; e.g., CFD and advances in computer simulation.**

Proposed Revision to 10 CFR 50.55a - Incorporate by Reference IEEE Std 603-2009 Criteria for Safety Systems for Nuclear Power Plants

Charles H. Brown, Jr.

Fundamental Principles of Instrumentation Safety and Reliability + 1

- Redundancy
- Independence
- Determinancy
- Defense-in-Depth and Diversity
- Control of Access +
- Simplicity

Fundamental Principles (cont.)

- **Nuclear plants are being designed with computer-based DI&C systems and networks as the backbone for protection, control, alarm, display, and monitoring**

Fundamental Principles (cont.)

- **Computer-based systems allow enhanced performance but:**
  - **result in a higher degree of functional integration and**
  - **have new design and failure issues; e.g., less inherent inter-division communication independence, signal processing that is not inherently deterministic, software complexity, verification &validation, and control of access vulnerabilities**

Fundamental Principles (cont.)

- **Also, networks are used for communication between plant systems and control spaces and to external site and corporate networks resulting in potential compromised control of access from sources external to the plant**

Fundamental Principles (cont.)

- **The use of microprocessors or field programmable gate arrays in nuclear plant safety systems does not compromise the determination of the fundamental principles of redundancy, defense-in-depth and diversity, and simplicity.**

- **Their use does introduce new vulnerabilities that potentially compromise**

  - **division-to-division independence,**
  - **determinant safety signal processing behavior, and**
  - **control of access to plant safety systems from sources external to the plant.**

Fundamental Principles (cont.)

- **Thus, use of computer-based systems need new design requirements that:**
  - **are specified by rule in the Code of Federal Regulations as is done for analog systems**
  - **ensure the fundamental principles that are potentially compromised, namely independence, determinant signal processing, and control of access from external plant sources, are captured in the DI&C architecture**
  - **ensure all are detailed during the licensing phase**

Present Rule 10 CFR 50.55a

- **10 CFR 50.55a currently specifies that nuclear power plant I&C systems must comply with IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations"**
- **The 1991 standard does not provide criteria that are sufficient for designs based on computer-based technology**

Proposed 10 CFR 50.55a Revision

- NRR recognized this and has proposed updating 10 CFR 50.55a to IEEE 603-2009 which includes expanded requirements for computer-based designs.
- NRR also recognized that there were additional needs that were absent from the 2009 standard.

Proposed 10 CFR 50.55a Revision (cont.)

- **Thus the draft revision proposes to incorporate by reference IEEE 603-2009 subject to the following:**
  - **Imposes additional technical conditions for the use of IEEE 603-2009**
  - **Establishes conditions for applicability of the new and previous versions of the standard**
  - **Retains the incorporate by reference of earlier versions of the standard**
  - **Provides clarifying definitions for several terms in the standards and the proposed regulation**

ACRS Comments

- The proposed draft revision should be published after incorporation of our recommendations with respect to
  - Independence
  - Determinant signal processing
  - Control of access

ACRS Comments

- **Independence - Independence in digital applications is not inherently ensured by the existing rule requirement for electrical isolation.**
  - **The proposed rule does not incorporate a condition that prevents this loss of independence.**

ACRS Comments

- **Determinant Signal Processing - Determinant behavior depends on program cycle design which can include operating system, operator, or other external interrupts. The proposed rule incorporates a condition for predictable and repeatable operation.**
  - **The phrase "predictable and repeatable" in the proposed rule is not clear relative to its actual application to real plant systems from sensor data inputs to control device actuation and should be clarified.**

ACRS Comments

- **Control of Access - Connections between internal plant safety networks and networks external to the plant through a firewall (typically software-based and software-controlled) can enable remote access that is not under the control of the plant operators.**
  - **The proposed rule does not contain any provision that prevents this loss of access control.**

ACRS Recommendations

- **We agreed with the proposed draft revision subject to incorporation of three recommendations:**
  - **Revise 10 CFR 50.55a(h)(5)i, Independence, to specify an independent hardware-based monitor for common safety system voting processing units that produces a trip if the common unit ceases operation or "locks-up" (ceases to respond). The trip should be independent of the processing unit and executed by the hardware-based monitor.**

ACRS Recommendations

- **Section 10 CFR 50.55a(h)(4), System Integrity, of the proposed rule should be clarified to state that "both predictable and repeatable" means processing from sensor data input to safety control device actuation and independent of any redundant portions of the safety system or other external input.**

ACRS Recommendations

- **Section 10 CFR 50.55a(h) of the proposed rule should specify an additional condition addressing Section 5.9 of IEEE Std 603-2009, Control of Access. The condition should specify that communications external to the plant should be accomplished using one-way, hardware-based (transmit only) devices. These devices should neither be software configurable nor capable of alteration by external commands or any surreptitious means.**

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

SECY-14-0087, "Qualitative Consideration of Factors in the Development of Regulatory Analyses and Backfit Analyses"

Harold B. Ray

Background

- SECY-14-0002, "Plan for Updating the U.S. Nuclear Regulatory Commission's Cost-Benefit Guidance"
- Staff proposes developing a set of methods that could be used for the qualitative consideration of factors within the regulatory analysis process

Background (cont.)

- The guidance would:
  - Establish a systematic process for the qualitative consideration of factors that cannot be evaluated quantitatively
  - Increase the transparency of how the staff's recommendation qualitatively considered such factors in relation to the quantitative analysis
  - Increase consistency in the qualitative consideration of factors for regulatory analyses

Issues

- **How to improve the quantitative analyses that are performed**
- **How to apportion the balance between quantitative and qualitative arguments, especially in the case where uncertainties are large**

ACRS Recommendations

- **Recommends approval of the staff proposal in SECY-14-0087**
- **The proposed guidance should seek to provide a single, comprehensive decision-making approach and not be limited to only separate qualitative and quantitative methods**

ACRS Recommendations (cont)

- **The staff should meet with the Committee periodically during development of the updated guidance to enable us to review and comment on the planned consideration of qualitative factors**

Abbreviations

ABWR	Advanced Boiling Water Reactor
ACRS	Advisory Committee on Reactor Safeguards
APWR	Advanced Pressurized Water Reactor
AP1000	Advanced Passive 1000
BWR	boiling water reactor
CFD	computational fluid dynamics
CFR	Code of Federal Regulations
COLA	combined license application
DTE	DTE Electric Company
DI&C	digital instrumentation & control
EPR	Evolutionary Power Reactor
ESBWR	Economic Simplified Boiling Water Reactor
FSME	Office of Federal and State Materials and Environmental Programs
GSI	generic safety issue
HRA	human reliability analysis
IDHEAS	integrated decision-tree human event analysis system
IEEE	Institute of Electrical and Electronics Engineers
iPWR	integrated pressurized water reactor
LOCA	loss-of-coolant accident
NMSS	Office of Nuclear Materials Safety and Safeguards
NRR	Office of Nuclear Reactor Regulation
NRO	Office of New Reactors
NSIR	Office of Nuclear Security and Incident Response
NUREG	NRC technical report designation
PRA	probabilistic risk assessment
PSEG	Public Service Enterprise Group Incorporated
R&D	research and development
RES	Office of Nuclear Regulatory Research
SECY	Office of the Secretary
SER	safety evaluation report
SRM	staff requirements memorandum
US	United States