UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

**R-2252**

May 18, 2007

The Honorable Dale E. Klein
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: ACTIVITIES RELATED TO DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

Dear Chairman Klein:

In a November 8, 2006 Staff Requirements Memorandum (SRM), the Commission requested the Committee provide its views on the staff's efforts related to digital instrumentation and controls (I&C) and consider potential means for providing reasonable backup, if appropriate. During the 542nd meeting of the Advisory Committee on Reactor Safeguards, May 3–5, 2007, we met with representatives of the NRC staff and the Nuclear Energy Institute to discuss the ongoing staff and industry activities associated with digital I&C systems. Our Subcommittee on Digital I&C Systems reviewed this matter on April 18, 2007. We also had the benefit of the documents referenced.

## CONCLUSIONS AND RECOMMENDATIONS

1. We concur with the staff's approach to developing a project plan that defines a process to improve deployment of digital I&C technology for new and operating reactors.

2. The staff should develop an inventory and classification (e.g., by function or other characteristics) of the various types of digital and software systems that are being used and are likely to be used in nuclear power plants.

3. The staff should evaluate the operating experience with digital systems in the nuclear and other industries to obtain insights regarding potential failure modes.

4. The information obtained through performing activities in Recommendations 2 and 3 should be used in the development of regulatory guidance on defense in depth and diversity for digital I&C systems.

## BACKGROUND AND DISCUSSION

The staff is responding to a December 6, 2006 SRM, in which the Commission directed that senior NRC managers engage industry to establish an NRC project plan with specific milestones and deliverables to address deployment of digital I&C technology. The staff's draft project plan builds on the ongoing digital I&C research program. The staff has formed a Steering Committee consisting of senior managers to provide oversight and guidance on six key technical and regulatory issues and to interface with the industry. Each key issue is

assigned to a Task Working Group that reports to the Steering Committee. The staff has identified specific deliverables and is in the process of specifying the due dates for these deliverables. We agree with the staff's approach to the development of a process that will facilitate the deployment of digital I&C technology for new and operating reactors.

One of the key technical and regulatory issues is the determination of the degree of redundancy and diversity necessary to protect a safety function against the occurrence of a digital system failure due to a common cause. The staff stated that the principal means for reducing the potential for common-cause failures (CCFs) is the high quality that is demanded of the digital system design process. Even with the assumption of high quality, CCFs cannot be excluded and, therefore, are postulated in the analysis of particular accidents; a judgment is then made regarding the need for diverse means of protection. An example of the latter is the provision of diverse displays and controls in the main control room to enable the manual actuation of components.

Protecting against CCFs is a subjective exercise that relies on the experience and imagination of the analysts. A critical element is the specification of the postulated CCFs. The set of postulated CCFs may be overly conservative in some cases and incomplete in others.

The quality of this process depends on the information available to the analysts regarding the functionality and susceptibility to failures of the digital system. For example, the evaluation of the performance of systems with simple actuation software is expected to be simpler than the evaluation of systems with software used for feedback and control. Therefore, there is a basic need for an inventory and classification (e.g., by function) of the various types of digital software systems that are being used and are likely to be used in the near future in nuclear power plants.

The search for potential CCFs would be enhanced by lessons learned from relevant operating experience for each type of digital system. For example, there have been several well-known accidents in the aerospace industry involving digital software. An evaluation of this experience and its applicability to nuclear systems should provide very valuable insights into potential failure modes. These failure modes would be associated with the various layers of components and functions that constitute a specific type of digital I&C system, including: (1) the host computer or microprocessor hardware; (2) software performing critical background functions, such as timers and clocks, self-test routines, and network communications; and (3) application-specific software (i.e., software that receives input from plant sensors and implements the logic and/or algorithmic functions necessary to control external devices that are part of the physical plant).

While the development of an inventory of the various types of digital software systems and the evaluation of the operating experience will provide useful insights into all six key technical and regulatory issues, we consider it essential in the formulation of regulatory guidance on defense in depth and diversity strategies. This information is also necessary to develop our response regarding the need and potential means for backup.

We look forward to working with the staff as the development and implementation of the project plan proceeds.

Sincerely,

**/RA/**

William J. Shack
Chairman

**References**

1. Letter from A.L. Vietti-Cook, Secretary, NRC, to John T. Larkins, Executive Director, ACRS, "Staff Requirements - Meeting with ACRS, October 20, 2006, Commissioners' Conference Room, One White Flint North, Rockville, MD (Open to Public Attendance)," November 8, 2006

2. U.S. Nuclear Regulatory Commission, Digital I&C Project Plan (draft), April 13, 2007

3. Letter from A.L. Vietti-Cook, Secretary, NRC, to Luis A. Reyes, Executive Director for Operations, "Staff Requirements - Briefing on Digital I&C, November 8. 2006, Commissioners' Conference Room, One White Flint North, Rockville, MD (Open to Public Attendance)," December 6, 2006

4. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, Washington, DC, 1997

5. Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 5, modified February 15, 2007

6. U.S. Nuclear Regulatory Commission/Lawrence Livermore National Laboratory NUREG/CR-6303, "Method for Performing D3 Analyses of Reactor Protection System," December 1994

7. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary, and Advanced Light-Water Reactor Designs," Section Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," April 2, 1993

8. U.S. Nuclear Regulatory Commission/ The Ohio State University NUREG/CR-6901, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," February 28, 2006

We look forward to working with the staff as the development and implementation of the project plan proceeds.

Sincerely,

**/RA/**

William J. Shack
Chairman

**References**


1. Letter from A.L. Vietti-Cook, Secretary, NRC, to John T. Larkins, Executive Director, ACRS, "Staff Requirements - Meeting with ACRS, October 20, 2006, Commissioners' Conference Room, One White Flint North, Rockville, MD (Open to Public Attendance)," November 8, 2006

2. U.S. Nuclear Regulatory Commission, Digital I&C Project Plan (draft), April 13, 2007

3. Letter from A.L. Vietti-Cook, Secretary, NRC, to Luis A. Reyes, Executive Director for Operations, "Staff Requirements - Briefing on Digital I&C, November 8. 2006, Commissioners' Conference Room, One White Flint North, Rockville, MD (Open to Public Attendance)," December 6, 2006

4. National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues," National Academy Press, Washington, DC, 1997

5. Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revision 5, modified February 15, 2007

6. U.S. Nuclear Regulatory Commission/Lawrence Livermore National Laboratory NUREG/CR-6303, "Method for Performing D3 Analyses of Reactor Protection System," December 1994

7. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary, and Advanced Light-Water Reactor Designs," Section Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," April 2, 1993

8. U.S. Nuclear Regulatory Commission/ The Ohio State University NUREG/CR-6901, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments," February 28, 2006


**DOCUMENT NAME**:C:\FileNet\ML071380437.wpd

| **OFC** | ACRS | ACRS | ACRS | ACRS |
|---|---|---|---|---|
| **NAME** | MJunge | CSantos | FGillespie | FPG for WJS |
| **DATE** | 5/18 /07 | 5/18 /07 | 5/18 /07 | 5/ 18 /07 |

**OFFICIAL RECORD COPY**

**DATE: June 8, 2007**

| ROUTING & TRANSMITTAL SLIP | | |
|---|---|---|
| NAME | INITIALS | DATE |
| 1. M. Junge | | /07 |
| 2. C. Santos | | /07 |
| 3. F. Gillespie | | /07 |
| 4. | | /07 |
| 5. | | /07 |
| 6. | | /07 |
| 7. | | |
| SUBJECT: Activities Related to Digital I&C Sys | | |
| RETURN TO: Jessie ACRS/ACNW | PHONE NO. 415-7360 | ROOM NO. T-2E6 |

✓ **"ORIGINAL"**

✓ DOC. NAME:C:\FileNet\ML071380437.wpd
STAFF PERSON: JUNGE
✓ FILE CODE:

**NOTE: THE ATTACHED LETTER WILL BE ENTERED IN "ADAMS" - THANK YOU**