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

ACRSR-2168

November 21, 2005

Luis A. Reyes
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington DC 20555-0001

SUBJECT: DRAFT NRC DIGITAL SYSTEM RESEARCH PLAN FOR FY 2005 - FY 2009

Dear Mr. Reyes:

During the 527th meeting of the Advisory Committee on Reactor Safeguards, November 3-4, 2005, we met with representatives of the NRC staff to discuss the draft NRC Digital System Research Plan for FY 2005 - FY 2009. Our Subcommittee on Digital Instrumentation and Control Systems discussed the details of the research plan during meetings on June 14-15 and October 20-21, 2005. We also had the benefit of the documents referenced.

CONCLUSION

The Digital System Research Plan for FY 2005 - FY 2009 is well directed toward meeting agency needs. The plan can be further refined by considering the following recommendations.

RECOMMENDATIONS

1. The plan should include a research project to develop an inventory and classification, e.g., by function, of the various types of digital systems that are used and are likely to be used in nuclear power plants in the future.

2. The research plan should include a more detailed identification of current and future regulatory needs and possible benefits of the planned research to the regulatory system.

3. The plan should acknowledge the existence of two different aspects of software safety. The overall thrust of the proposed research is “software-centric.” The “system-centric” aspect should receive more consideration than it is currently given.

4. Research in Section 3.6, Advanced Nuclear Power Plant Digital Systems, should be given higher priority.

BACKGROUND

Analog instrumentation and control systems in nuclear power plants are becoming obsolete and replacement parts are difficult to obtain. Licensees are replacing these systems with digital systems that are more flexible and have the potential to increase reliability and improve operational performance. Digital technology, however, brings a number of challenges. It can introduce new failure modes to the system, the rapid pace of change in digital technology

requires the agency to update its knowledge base frequently, and new methods and acceptance criteria are needed to assess the safety and security of the systems.

The Office of Nuclear Regulatory Research has developed a plan for digital instrumentation and control systems research for Fiscal Years FY 2005 - FY 2009. This plan updates the previous plan for Fiscal Years FY 2000 - FY 2004. The plan has been reviewed by the Office of Nuclear Reactor Regulation, the Office of Nuclear Material Safety and Safeguards, and the Office of Nuclear Security and Incident Response.

DISCUSSION

The draft plan divides the research into six areas:

- System aspects of digital technology
- Software quality assurance
- Risk assessment of digital systems
- Security aspects of digital systems
- Emerging digital technology and applications
- Advanced nuclear power plant digital systems

The proposed research areas are comprehensive.

The applicability of the methods being investigated can vary greatly across the spectrum of possible systems. There is, therefore, a need for an inventory and classification, e.g., by function, of the various types of digital systems that are used or likely to be used in nuclear power plants in the future. Such a classification, along with a concurrent examination of the failures that have occurred in digital systems, should provide information on what types of tools may be best suited for different assessments. This classification could be the key to understanding the limitations of current methods of assessment and to guiding future efforts. For example, the analytical tools required to evaluate the performance of systems with simple actuation software are expected to be simpler than those required to evaluate systems with feedback and control software.

The plan discusses the shortcomings of the current regulations and the potential improvements that the proposed research is expected to produce. The plan would benefit by better identifying regulatory needs and anticipated benefits across all research areas. During our meetings, it was evident that the staff had thought through most of these issues, but its thinking was not well documented in the plan. Such documentation should be included.

As stated in the additional comments to our June 9, 2004, letter, the literature on digital software indicates that there are two main approaches to software reliability. The first approach views “failure” as a property of the software itself, just as the failure modes of hardware are considered properties of the components. This first approach is “software-centric.” The second approach is “system-centric,” in that the software is considered part of the system and the focus is on system failures.

Although the staff is aware of the two approaches to digital system reliability, the plan appears to be heavily focused on the software-centric view. For example, one objective of the research

project described in Section 3.3.3, “Investigation of Digital System Characteristics Important to Risk,” is said to be the calculation of the risk-importance of generic digital systems. This project seems to focus on the software more than the overall system. Although such a calculation may be meaningful for software in actuation systems such as the reactor protection system, it is unclear whether this can be done in more complex cases. Similarly, the term “digital system reliability” is used repeatedly in Section 3.3.4, “Investigation of Digital System Reliability Assessment Methods.” A system-centric analysis focuses on the reliability of the broader system, not just the digital part. Such an approach to reliability should receive more consideration in the plan. The digital system classification in Recommendation 1 will assist the staff in determining when each approach is appropriate.

The research plan includes a program to investigate advanced nuclear power plant digital systems (Section 3.6), but this work has not begun. Due to the rapidly increasing interest in new reactors and the anticipated regulatory needs, this research should be given higher priority than it currently has.

In conclusion, we found the Digital System Research Plan for FY 2005 - FY 2009 to be well developed. The planned research programs should provide important inputs to the regulatory process. We look forward to continuing discussions with the staff on these programs as work progresses.

Sincerely,

/RA/

Graham B. Wallis
Chairman

References:

1. Memorandum from Michelle G. Evans, Chief, Engineering Research Applications Branch, Division of Engineering Technology, Office of Nuclear Regulatory Research, to John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards, “Transmittal of Material to Support the November 3 and 4, 2005, ACRS Meeting,” September 29, 2005. (Pre-decisional).
2. Letter dated June 9, 2004 from Mario V. Bonaca, Chairman, Advisory Committee on Reactor Safeguards, to Luis A. Reyes, Executive Director for Operations, Nuclear Regulatory Commission, Subject: Digital Instrumentation and Control Research Program.

project described in Section 3.3.3, “Investigation of Digital System Characteristics Important to Risk,” is said to be the calculation of the risk-importance of generic digital systems. This project seems to focus on the software more than the overall system. Although such a calculation may be meaningful for software in actuation systems such as the reactor protection system, it is unclear whether this can be done in more complex cases. Similarly, the term “digital system reliability” is used repeatedly in Section 3.3.4, “Investigation of Digital System Reliability Assessment Methods.” A system-centric analysis focuses on the reliability of the broader system, not just the digital part. Such an approach to reliability should receive more consideration in the plan. The digital system classification in Recommendation 1 will assist the staff in determining when each approach is appropriate.

The research plan includes a program to investigate advanced nuclear power plant digital systems (Section 3.6), but this work has not begun. Due to the rapidly increasing interest in new reactors and the anticipated regulatory needs, this research should be given higher priority than it currently has.

In conclusion, we found the Digital System Research Plan for FY 2005 - FY 2009 to be well developed. The planned research programs should provide important inputs to the regulatory process. We look forward to continuing discussions with the staff on these programs as work progresses.

Sincerely,

Graham B. Wallis
Chairman

References:

1. Memorandum from Michelle G. Evans, Chief, Engineering Research Applications Branch, Division of Engineering Technology, Office of Nuclear Regulatory Research, to John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards, “Transmittal of Material to Support the November 3 and 4, 2005, ACRS Meeting,” September 29, 2005. (Pre-decisional).
2. Letter dated June 9, 2004 from Mario V. Bonaca, Chairman, Advisory Committee on Reactor Safeguards, to Luis A. Reyes, Executive Director for Operations, Nuclear Regulatory Commission, Subject: Digital Instrumentation and Control Research Program.

*See previous concurrence.

DOCUMENT NAME: E:\Filenet\ML053260586.wpd
To receive a copy of this document, indicate in the box: "C" = Copy without attachment/enclosure "E" = Copy with attachment/enclosure "N" = No copy Accession #: ML053260586

OFFICE	ACRS/ACNW	Y	ACRS/ACNW	Y	ACRS/ACNW	Y	ACRS/ACNW	Y	ACRS/ACNW	Y	ACRS/ACNW	Y
NAME	EThornsbury		MSnodderly		MScott		AThadani		JLarkins		JTL for GBW	
DATE	11/18/05*		11/18/05*		11/21/05*		11/21/05*		11/21/05*		11/21/05*	

OFFICIAL RECORD COPY