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

October 2, 2009

The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT DIGITAL SYSTEM RESEARCH PLAN FOR FY 2010 – FY 2014

Dear Chairman Jaczko:

During the 565th meeting of the Advisory Committee on Reactor Safeguards, September 10 - 12, 2009, we reviewed the July 28, 2009, version of the draft Digital System Research Plan for Fiscal Years (FY) 2010 – 2014. Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on August 19 - 21, 2009. During these reviews, we had the benefit of discussions with representatives of the NRC staff. We also had the benefit of the documents referenced.

CONCLUSION

The Digital System Research Plan for FY 2010 – FY 2014 is well directed towards meeting the agency needs and achieving the staff's stated purposes.

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.

DISCUSSION

The Office of Nuclear Regulatory Research (RES) has developed a plan for DI&C systems research for FY 2010 - FY 2014. This plan updates the previous one for FY 2005 - FY 2009.

The stated purpose of the research plan is to provide a communication and planning framework that identifies necessary research initiatives that support regulatory decisions. The draft plan divides the research into five areas.

- Safety Aspects of Digital Systems
- Security Aspects of Digital Systems
- Advanced Nuclear Power Concepts
- Knowledge Management
- Additional Carry-Over Projects from Digital System Research Plan for FY 2005 – FY 2009

Individual projects are identified within each area and are prioritized (high, medium, or low) with respect to the project completion date and the basis for the research. For example, projects that support the development of new regulatory positions are assigned a high priority regardless of the completion date. At the other extreme, projects that improve the efficiency of regulatory reviews but have a completion date more than five years are assigned a low priority. Resource limitations necessitate this prioritization.

The five research areas are comprehensive and well directed towards achieving the staff's stated purposes. The prioritization scheme will be useful in the effective allocation of resources. RES has sought input on the plan from the user offices, and the plan has been reviewed by the Office of Nuclear Reactor Regulation, Office of New Reactors, Office of Nuclear Material Safety and Safeguards, and Office of Nuclear Security and Incident Response.

Comments on Selected Research Projects

The following comments are offered with two goals in mind: First, to allow the staff to consider them as the plan is refined and second, to identify early some issues that will be of particular interest to the ACRS during future reviews of ongoing research programs.

Communications Among Plant-Wide Systems

This research project is intended to produce three deliverables:

1. A generic model of a plant-wide digital network that supports staff reviews of licensing requests relating to Highly Integrated Control Room communication protocols for safety and non-safety DI&C systems. The model will identify characteristics that all applications should take into consideration and are applicable to any nuclear power plant.

2. A NUREG/CR on communication processes and review criteria for the exchange of information between plant sensors/actuators and the protection and control systems, and among safety channels (such as for voting).

3. Regulatory guidance on DI&C network characteristics that provide adequate reliability, redundancy, and independence (including adequate separation and isolation) among redundant channels.

The development of a generic model that would still allow for evaluations as required by General Design Criterion (GDC) 24 will be a challenge. GDC 24 deals with the separation of protection and control systems and is cited in the technical basis section of this project. The term “generic” implies a relatively high level of abstraction in the model of the plant-wide digital network with a relatively low level of detail. It is unclear what insights could be gained from such a representation. Demonstration that GDC 24 is met will require a more detailed approach.

One potential approach might be first to consider analysis and evaluation techniques that could be used to demonstrate compliance with the regulations and then define the model using the results of the analyses. For example, I&C diagrams could be transformed into Petri nets where data items could be represented as tokens. Determining whether “allowable” or “unallowable” data paths exist can be achieved by means of a reachability analysis (this is a common use of Petri nets, as well as graphs in general). Other graph-based representations may be useful also. The deliverable would describe how to create the representations and how to analyze them to determine whether the design is acceptable.

Many of the current applications of DI&C use direct data communication between all the safety divisions and the main program loops. For example, some designs submitted for certification incorporate each division's voting logic unit (a software routine) within the main program loop. Other designs share digital sensor data from each safety division to every other safety division through its main program loop. In this case, each division uses a data screening algorithm to determine what data to use for safety function processing. This algorithm is the same in each division. Communications of this nature link data flows among nominally independent safety divisions. Interim Staff Guidance (ISG)-4 recognizes this conundrum but allows licensees to implement this software design approach as long as they can demonstrate that independence is not compromised. To ensure that the staff can adequately evaluate licensee design approaches, it would be very useful if the deliverables of this project included: the identification of data screening and evaluation algorithms that are the most robust at detecting corrupt and invalid data such that they are not injected into the program loop; and the identification of acceptable error detection/correction methods that meet ISG-4 guidance that would "...always reconstruct the original message exactly or to designate the message as unrecoverable."

Safety Assessment of Tool Automated Processes

It is not clear from the description of this project whether the experience of other industries, including aviation and telecommunications, will be reviewed. These industries have developed standards that address automated tools. For example, RTCA DO 178B, a software assurance standard used in the aircraft industry, addresses automated tools for both code generation and verification. The “guidance” (in essence, the defined regulatory approach) in this standard distinguishes between “code generation” and “verification tools”, and also considers whether or not the output of such tools can be manually and independently verified. These standards should be evaluated to help develop regulatory guidance for the use of such tools.

Development of Benchmark and Reliability Data

The stated purpose of this project is to provide a process for evaluation and validation of digital systems using a fault injection process to estimate digital system reliability. We agree that the fault injection method may contribute to our confidence that the system is of high quality by providing evidence of fault detection and recovery capabilities. However, we doubt that this project could lead to meaningful reliability estimates. The project's benefits need to be characterized properly, inasmuch as the results will be neither "benchmark" nor "reliability" data.

Analytical Assessment of DI&C Systems and Digital System PRA

In our report dated May 19, 2008, we offered the following recommendation:

> The distinction between traditional and non-traditional methods of modeling and analysis is artificial and should be abandoned. The staff should establish an integrated program that focuses on failure mode identification of DI&C systems and takes advantage of the insights gained from the investigations on traditional PRA methods and on advanced simulation methods.

We continue to believe that an integrated approach is essential to both the analytical assessment of DI&C systems and digital System PRA.

The draft Digital System Research Plan for FY 2010 - FY 2014 is comprehensive and well directed toward meeting the agency needs and achieving the staff's stated purposes. The planned research projects can provide important inputs to the regulatory process by addressing the digital technology challenges that we cited in the Background Section. We look forward to continuing discussions with the staff on these projects as work progresses.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

REFERENCES

1. U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Draft NRC Digital System Research Plan FY 2010 – FY 2014, dated July 28, 2009 (ML082470725)

2. RTCA Special Committee 167, DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992 (Available from RTCA Inc., 1140 Connecticut Avenue, N.W., Suite 1020, Washington, D.C. 20036) (ML092660601)

3. 10 CFR Part 50, Appendix A, General Design Criteria 24, "Separation of Protection and Control Systems," dated December 23, 1999

4. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Controls, DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues (HICRc) Interim Staff Guidance, Revision 0, dated September 28, 2007 (ML072540138)

5. Letter Report from William J. Shack, Chairman, ACRS, to Dale E. Klein, Chairman, U.S. NRC, Draft NUREG/CR-6962, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," and Related Matters, dated May 19, 2008 (ML081330429)

Development of Benchmark and Reliability Data

The stated purpose of this project is to provide a process for evaluation and validation of digital systems using a fault injection process to estimate digital system reliability. We agree that the fault injection method may contribute to our confidence that the system is of high quality by providing evidence of fault detection and recovery capabilities. However, we doubt that this project could lead to meaningful reliability estimates. The project's benefits need to be characterized properly, inasmuch as the results will be neither "benchmark" nor "reliability" data.

Analytical Assessment of DI&C Systems and Digital System PRA

In our report dated May 19, 2008, we offered the following recommendation:

> The distinction between traditional and non-traditional methods of modeling and analysis is artificial and should be abandoned. The staff should establish an integrated program that focuses on failure mode identification of DI&C systems and takes advantage of the insights gained from the investigations on traditional PRA methods and on advanced simulation methods.

We continue to believe that an integrated approach is essential to both the analytical assessment of DI&C systems and digital System PRA.

The draft Digital System Research Plan for FY 2010 - FY 2014 is comprehensive and well directed toward meeting the agency needs and achieving the staff's stated purposes. The planned research projects can provide important inputs to the regulatory process by addressing the digital technology challenges that we cited in the Background Section. We look forward to continuing discussions with the staff on these projects as work progresses.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

Distribution:
See next page

Accession No: ML092590690 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category? ***See previous**
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS **WW for**	ACRS **CS for**	ACRS
NAME	CAntonescu*	CAntonescu*	ADias/CSantos	EHackett	MBonaca
DATE	9/30 /09	9/30 /09	10/ 2 /09	10/ 2 /09	10/ 2 /09

OFFICIAL RECORD COPY

Letter to the Honorable Gregory B Jaczko, Chairman, NRC, from Mario V. Bonaca, Chairman, ACRS, dated October 2, 2009

SUBJECT: DRAFT DIGITAL SYSTEM RESEARCH PLAN FOR FY 2010 – FY 2014

Distribution:
ACRS Branch A
ACRS Branch B
E. Hackett
H. Nourbakhsh
J. Flack
C. Jaegers
T. Bloomer
B. Champ
A. Bates
S. McKelvin
L. Mike
J. Ridgely
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter