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

June 3, 2005

MEMORANDUM TO: George Apostolakis, Chairman
Digital Instrumentation &Control Systems Subcommittee

FROM: Eric Thornsbury, Senior Staff Engineer /***RA***/

SUBJECT: STATUS REPORT FOR THE MEETING OF THE SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, JUNE 14-15, 2005, IN ROCKVILLE, MARYLAND

The purpose of this memorandum is to forward written materials for your use in preparing for the meeting of the ACRS Subcommittee on Digital Instrumentation and Control Systems on June 14-15, 2005. The purpose of the meeting is to review the status of the draft Digital Systems Research Plan and projects in two sections of the plan. Attached please find the agenda, status report, and background materials.

Attendance by the following members and consultants is anticipated and reservations have been made at the following hotels for June 13-15, 2005, unless otherwise indicated.

Apostolakis	RESIDENCE INN	Guarro	TBD
Bonaca	RESIDENCE INN	White	TBD
Kress	RESIDENCE INN		

Please notify Ms. Barbara Jo White at 301-415-7130 if you need to change or cancel the above reservations.

Attachments:
1. Agenda
2. Status report
3. List of additional attachments

cc: ACRS Members
cc w/o attach: J. Larkins
M. Scott
M. Snodderly
S. Duraiswamy

Attachment 1

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee Meeting
Rockville, MD
14-15 June 2005

- Proposed Agenda -

Cognizant Staff Engineer: Eric Thornsbury (301-415-8716, eat2@nrc.gov)

	Topic	Presenter(s)	Time
June 14			
I	Opening Remarks and Objectives	G. Apostolakis, ACRS	8:30 - 8:45 am
II	Reconciliation of Comments on Draft Research Plan	M. Waterman, RES	8:45 - 10:15 am
	Break		10:15 - 10:30 am
III	Draft Revision of Reg Guide 1.97	G. Tartal, RES	10:30 - 11:30 am
	Lunch		11:30 am - 12:30 pm
IV	Software Quality Assurance (3.2)	W. Kemper, RES	12:30-12:45 am
	Assessment of Software Quality (3.2.1)	S. Arndt, RES N. Carte, RES M. Li, UMd	12:45 - 2:30 pm
		Break	2:30 - 2:45 pm
	Digital System Dependability (3.2.2) Self-testing Methods (3.2.3)	S. Arndt, RES R. Shaffer, RES	2:45 - 5:00 pm
V	Risk Assessment of Digital Systems (3.3)	S. Arndt, RES	5:00 - 5:30 pm
	Recess for the day		5:30 pm
June 15			
	Reconvene		1:00 pm
V	Development and Analysis of Digital System Failure Data (3.3.1)	T. Hilsmeier, RES T. Chu, BNL	1:00 - 1:45 pm
	Investigation of Digital System Failure Assessment Methods, Risk Characteristics, and Reliability Assessment Models (3.3.2, 3, 4)	T. Hilsmeier, RES H. Hamzehee, RES T. Chu, BNL	1:45 - 2:30 pm
		Break	2:30 - 2:45 pm
		S. Arndt, RES T. Aldemir, OSU	2:45 - 4:45 pm
VI	Closing Discussion and Future Plans	G. Apostolakis, ACRS	4:45 - 5:00 pm
	Recess		5:00 pm

Notes:
- (3.X) refers to the corresponding section of the draft research plan
- Presentation time should not exceed 50% of the total time allocated for a specific item.
- Number of copies of presentation materials to be provided to the ACRS - 35.

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee Meeting
Rockville, MD
14-15 June 2005

- Status Report -

PURPOSE

The purpose of the meeting is to review the status of the draft Digital Systems Research Plan, projects from two sections of the plan, and work related to a draft Regulatory Guide. The draft Digital Systems Research Plan was sent from RES to NRR, NMSS, and NSIR for review. Each of these offices has now provided official comments to RES, who is reviewing and addressing them as appropriate. We are also aware of other opinions expressed at the May full Committee meeting by some NRR staff. The current plan is to review the plan in detail at two subcommittee meetings, then bring it to the full Committee for formal review and comment. At this meeting, we will also receive a preview of work on a revision to Regulatory Guide 1.97, which we expect to be forwarded to the Committee for official review soon.

The current plan is to hold another subcommittee meeting later this summer or early fall to receive details on the remaining portions of the research plan. We will then return to the full Committee for formal review and comment. However, the staff is also very interested in receiving informal feedback during the subcommittee meetings to incorporate into their research programs as they proceed.

BACKGROUND AND DISCUSSION

Four topics will be addressed at this subcommittee meeting: reconciliation of comments on the draft Digital Systems Research Plan, the draft revision of Regulatory Guide 1.97, Software Quality Assurance (section 3.2 of the research plan), and Risk Assessment of Digital Systems (section 3.3 of the research plan).

Reconciliation of Comments on the draft Digital Systems Research Plan

At the May full Committee meeting, we received an overview presentation of the draft Digital Systems Research Plan. At that time, RES staff had received comments from NSIR and NMSS, and was awaiting official comments from NRR. Within NRR, various opinions existed regarding the value of the research proposed in the plan, and they were exercising their processes for resolving these differences. The day of the full Committee meeting, NRR transmitted its official comments to RES. These are included in the attached memo from J. Dyer to C. Paperiello.

As part of the internal NRR review process, a nonconcurrence memo was sent from Jose Calvo, chief of the Electrical & Instrumentation and Control Branch, to Michael Mayfield, director of the Division of Engineering. The internal NRR review of the comments in the nonconcurrence memo “found some of them to be technically warranted, but the general tone of the comments was unnecessarily negative and, in some cases, the comments reflect a fundamental lack of understanding of the RES role in the NRC’s mission and the strategic goals of risk-informed regulation.” The formal comments transmitted to RES contained revised

versions of those comments with technical merit. The comments from the nonconcurrence memo and the formal office response are attached.

During Topic II of the subcommittee meeting, RES will discuss their review of the official comments from NRR, NMSS, and NSIR. We are also designating a few minutes for Mr. Mayfield to discuss the official NRR comments and how the nonconcurrence memo was dispositioned. Mr. Calvo will also be scheduled for a few minutes to add any comments to his previous statements and written memorandum. Discussions with the RES staff indicate that they are now meeting regularly with NRR staff in Jose's branch and receiving real-time feedback on changes to the research plan. NSIR will also make some brief comments on the plan Wednesday, as they are unable to attend Tuesday. NMSS has declined the opportunity to make formal statements to the Committee.

Regulatory Guide 1.97

Draft Revision 4 of Regulatory Guide 1.97 endorses IEEE Std. 497-2002, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations" (subject to the issues listed in the regulatory positions) and is intended for licensees of new nuclear power plants. Previous revisions of this regulatory guide remain in effect for current nuclear power plants. Current nuclear power plants using previous revisions of this regulatory guide are not necessarily affected by Revision 4.

Two quotations from the draft Regulatory Guide provide a good summary.

> With the increased use of microprocessor-based instrumentation systems in advanced design nuclear power plants, a need for developing a more flexible consolidated standard was recognized by the nuclear industry. Instead of providing a list of instrument variables to monitor, as was the case in Revision 3 of Regulatory Guide 1.97, it was recognized that performance based criteria should be provided for selecting variables. Rather than providing design and qualification category criteria for each type of variable, the goal was to standardize the criteria based on the accident management functions of the type of variable. These efforts resulted in the development of IEEE Std 497-2002.
>
> Revision 4 of Regulatory Guide 1.97 is intended for new plants. Consideration has been given to its applicability and usefulness for current plants. The staff recognizes that current plants could be interested in converting post accident monitoring variables from their current licensing basis, namely Revision 2 or 3 of this guide, to the guidance in Revision 4 of this guide. The staff also recognizes that there are a number of differences between Revision 3 and Revision 4 of this guide. These include differences in variable type definitions and associated criteria, removal of design and qualification categories, removal of prescriptive tables of monitored variables, analysis required to produce the necessary design basis documentation, and changes in licensing basis and/or commitments. These differences could have great cost implications for current plants considering conversion and would require a backfit. Therefore, Revision 4 of this guide is not intended for current plants. However, the staff sees no technical reason to prohibit a current plant from voluntarily making this conversion.

The standard provides six types of accident monitoring criteria as follows:

- How to select and categorize variables,
- What performance requirements must be met,
- What design features need to be considered,
- What aspects of seismic and environmental qualification must be met for each variable type,
- What display requirements to assure control room operators are properly informed, and
- What quality assurance requirements should apply.

The staff plans to issue the Regulatory Guide for public comment in August 2005 and request ACRS defer its official review until after that time. However, the staff wishes to present the draft of the regulatory guide at this time to receive informal feedback on its approach before issuing the document for public comment. We expect it to come to ACRS for formal review and comment sometime in early 2006.

Software Quality Assurance

Software Quality Assurance is the topic of Section 3.2 of the draft Digital Systems Research Plan. At this subcommittee meeting, we will hear from the staff regarding ongoing projects in this area.

First, staff will discuss work performed at the University of Maryland on the assessment of software quality. Included in this package is NUREG/CR-6848, "Preliminary Validation of a Methodology for Assessing Software Quality." This report documents the results of research to validate a method for predicting software quality. The method was initially presented in NUREG/GR-0019 and was discussed at a March 2004 subcommittee meeting.

Section 3.2.1 of the research plan continues the development and validation of the research conducted by the University of Maryland and others on the use of software engineering metrics to assess software quality. Included in this status report is NUREG/CR-6848, "Preliminary Validation of a Methodology for Assessing Software Quality," by the University of Maryland. This report documents the results of research to validate a method for predicting software quality. The research was also documented in NUREG/GR-0019 and was discussed at a March 2004 subcommittee meeting. The staff will update the subcommittee on the results of the recent work and the plans for continuing research. The agency is also performing collaborative research with the Halden Research Program to determine the software engineering practices and criteria that are most effective in assuring software quality.

The goal of Section 3.2.2 of the research plan is to develop a state-of-the-art tool and methodology for determining the dependability (and, they claim, the reliability) of nuclear facility digital systems. This work appears to be based on the previous research performed with the University of Virginia on fault injection techniques. Section 3.2.3 addresses the need for review guidance for self-testing features in digital systems. This also appears to be based on the previous University of Virginia work. Note that the UVa work has also been previously discussed with the Committee several times, most recently at a March 2004 subcommittee.

Risk Assessment of Digital Systems

Section 3.3 of the draft Digital Systems Research Plan addresses the need for risk assessments to include the analysis of digital instrumentation and control systems. The goals of the research are to assess the types and causes of failures that can occur in digital systems, characterize the risk-importance of I&C systems, develop digital reliability assessment methods, and collect and analyze the data needed to support this work.

The first part of the presentation will address the research in Section 3.3.1, Development and Analysis of Digital System Failure Data. This research will create and populate a database of digital system failures, both from the nuclear industry and other industries, including international data. This project will then evaluate the data to attempt to identify the frequency, severity, cause, and possible prevention of digital system failures.

The research projects in Sections 3.3.2, 3.3.3, & 3.3.4 investigate digital system failure assessment methods, digital system characteristics important to risk, and digital system reliability assessment methods. The staff will brief us on the work that is beginning in these areas, including work at Brookhaven National Laboratory and The Ohio State University.

EPRI Report

Also included in the attachment is an EPRI report on performing defense-in-depth and diversity assessments for digital upgrades. Following the May full Committee meeting, this report was sent by EPRI to the Committee for background information. The transmittal letter explains the document more fully.

EXPECTED SUBCOMMITTEE ACTION

At the July full Committee meeting, the Subcommittee will need to provide a brief update regarding the activities of this subcommittee meeting. Following a second subcommittee meeting, the staff will appear before the full Committee to receive formal review and comment of the research plan. The Subcommittee should be prepared at that time to make recommendations regarding the digital systems research program.

List of Additional Attachments

Agenda Item	Documents
II	1. Memorandum from J. E. Dyer, Director, NRR, to Carl J. Paperiello, Director, RES, "Comments on Draft, 'NRC Digital System Research Plan, FY 2005 - FY 2009'," 6 May 2005. [ML051020435] 2. Memorandum from Glenn M. Tracy, Director, Division of Nuclear Security, NSIR, to Richard J. Barrett, Director, Division of Engineering Technology, RES, "Office of Nuclear Security and Incident Response Comments on a Draft of 'NRC Digital System Research Plan, FY 2005 - FY 2009'," X XXX 2005. [ML050840481] 3. Memorandum from Robert C. Pierson, Director, Division of Fuel Cycle Safety and Safeguards, NMSS, to Richard J. Barrett, Director, Division of Engineering Technology, RES, "Comments on the Draft 'NRC Digital System Research Plan, FY 2005 - FY 2009'," 30 March 2005. [ML050830122] 4. Email from John Jankovich, Team Leader, MSIB/IMNS/NMSS, to Michael Mayfield, then Director, Division of Engineering Technology, RES, "IMNS/NMS Response to Digital System Research Plan," 16 March 2005. 5. Memorandum from Michael E. Mayfield, Director, Division of Engineering, NRR, to Jose A. Calvo, Chief, Electrical & Instrumentation and Controls Branch, Division of Engineering, NRR, "Response to Non-Concurrence on the Draft 'NRC Digital Systems Research Plan, FY 2005 - FY 2009'," 3 May 2005. [ML051220503] 6. Memorandum from Jose A. Calvo, Chief, Electrical & Instrumentation and Controls Branch, Division of Engineering, NRR, to Michael E. Mayfield, Director, Division of Engineering, NRR, "Non-Concurrence on the Draft 'NRC Digital Systems Research Plan, FY 2005 - FY 2009'," 19 April 2005. [ML051100056]
III	7. United States Nuclear Regulatory Commission, "Draft Regulatory Guide DG-1128 (Proposed Revision 4 of Regulatory Guide 1.97), Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," May 2005. 8. United States Nuclear Regulatory Commission, "Regulatory Guide 1.97, Revision 3, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident," May 1983. 9. IEEE Power Engineering Society,"IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Std 497-2002, 30 September 2002.

IV	10. United States Nuclear Regulatory Commission, “Preliminary Validation of a Methodology for Assessing Software Quality,” NUREG/CR-6848, July 2004. 11. University of Virginia Center for Safety-Critical Systems, “A Numerical Safety Evaluation Process for Safety-Critical Systems,” UVA-CSCS-NSE-001, Revision 2, 1 August 2003. 12. University of Virginia Center for Safety-Critical Systems, “A Technique for Performing Fault Injection Using Simics,” UVA-CSCS-SFI-001, Revision 0, 31 December 2004.
V	13. United States Nuclear Regulatory Commission, “Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments,” Draft Report for Comment, October 2004.
Other	14. EPRI, “Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades,” #1002835, December 2004.