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

March 11, 2004

MEMORANDUM TO: J. D. Sieber, Chairman, Plant Operations Subcommittee
G. Apostolakis, Chairman, Reliability and PRA Subcommittee

FROM: Marvin D. Sykes, Senior Staff Engineer, ACRS

SUBJECT: REVIEW MATERIALS FOR THE UPCOMING PLANT OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL INSTRUMENTATION AND CONTROLS

The purpose of this memorandum is to forward background materials for your use in preparing for the upcoming Plant Operations/Reliability and PRA Subcommittee joint meeting scheduled Friday, March 26, 2004 to discuss digital instrumentation and control research activities, including development of digital system reliability models, with representatives of the Office of Nuclear Regulatory Research and other interested parties.

Attendance by the following members and consultants is anticipated and reservations have been made at the following hotels for March 25, 2004, as indicated:

Bonaca	Residence Inn	Ford	Residence Inn
Sieber	Ramada Inn	Apostolakis	Residence Inn
Kress	Residence Inn	Rosen	Residence Inn
Shack	Residence Inn	Guarro	Residence Inn
White	None		

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) U.S. Department of Energy Report from The Instrumentation, Control and Human-Machine Interface (IC&HMI) Technology Workshop, May 2002.

4) National Research Council Report, “Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues,” 1997.

5) Presentations from the Halden Workshop on Risk/Safety Assessment of Digital Systems, November 7-8, 2002

6) Arndt, S. A., E. A. Thornsbury, and N. O. Siu, “What PRA Needs From a Digital Systems Analysis,” Probabilistic Safety Assessment and Management, Elsevier Science Ltd., June 2003.

7) Presentation from the NRC's Nuclear Safety Research Conference, October 20-22, 2003 titled "Reliability and Safety Assessment of Digital Systems Using Fault Injection Techniques"

8) Technical Approach for "Large Scale Validation of a Methodology for Assessing Software Quality"

For additional information, please call me at (301) 415-8716 or e-mail MDS1@NRC.GOV.

Attachments: As stated

cc w/attachments: Plant Operations Subcommittee, ACRS
Reliability and PRA Subcommittee, ACRS

cc w/o attachments: J. Larkins
H. Larson
S. Duraiswamy

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
PLANT OPERATIONS SUBCOMMITTEE MEETING
DIGITAL INSTRUMENTATION AND CONTROLS
MARCH 26, 2004
ROCKVILLE, MARYLAND

- TABLE OF CONTENTS -

I Table of Contents 1

II Proposed Meeting Schedule 2

III Status Report 3

Attachments

- U.S. Department of Energy Report on Instrumentation, Control and Human-Machine Interface (IC&HMI) Technology Workshop, May 2002.
- National Research Council's Report "Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues," 1997.
- Presentations from the Halden Workshop on Risk/Safety Assessment of Digital Systems, November 7 and 8, 2002.
- Arndt, S. A., E. A. Thornsbury, and N. O. Siu, "What PRA Needs From a Digital Systems Analysis," Probabilistic Safety Assessment and Management, Elsevier Science Ltd., June 2003.
- Presentation from the NRC's Nuclear Safety Research Conference, October 20-22, 2003 titled "Reliability and Safety Assessment of Digital Systems Using Fault Injection Techniques."
- Technical Approach for "Large-Scale Validation of a Methodology for Assessing Software Quality."

Cognizant ACRS Members: John Sieber, Chairman
Cognizant ACRS Staff Engineer: Marvin D. Sykes

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
PLANT OPERATIONS SUBCOMMITTEE MEETING
DIGITAL INSTRUMENTATION AND CONTROL
MARCH 26, 2004
ROCKVILLE, MARYLAND

- PROPOSED SCHEDULE -

Cognizant Staff Engineer: Marvin D. Sykes MDS1@nrc.gov (301) 415-8716

	TOPICS	PRESENTERS	TIME
I.	**Opening Remarks**	J. Sieber, ACRS G. Apostolakis, ACRS	8:30 -8:35 a.m. 5 minutes
II.	**General Overview of Digital I&C Research Program and Discussion of the State-of-the-Art in Digital System Reliability**	S. Arndt, RES N. Siu, RES	8:35 -9:30 a.m. 55 minutes
III.	**Digital Systems Modeling Using Fault Injection Methods**	B. Johnson, UVa S. Arndt, RES J. Calvert, RES	9:30 -10:15 a.m. 45 minutes
	BREAK		**10:15-10:30a.m.**
III.	**Digital Systems Modeling Using Fault Injection Methods (Continued)**	B. Johnson, UVa S. Arndt, RES J. Calvert, RES	10:30 -11:15 a.m. 45 minutes
IV.	**Static PRA Modeling Program**	S. Arndt, RES D. Overland, RES	11:15 -12:15pm 60 minutes
	LUNCH		**12:15-1:15 p.m.**
V.	**Software Reliability Modeling**	C. Smidts, UMd S. Arndt, RES	1:15-2:30 p.m. 75 minutes
V.	**Staff Plans for Digital Reliability Models**	S. Arndt, RES	2:30-2:50 p.m. 20 minutes
VI.	**General Discussion and Adjourn**	G. Apostolakis, ACRS J. Sieber, ACRS	2:50-3:00 p.m. 10 minutes

NOTE:

- Presentation time should not exceed 50 percent of the total time allocated for a specific item. The remaining 50 percent of the time is reserved for discussion.
- 35 copies of the presentation materials to be provided to the Subcommittee.

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
PLANT OPERATIONS SUBCOMMITTEE MEETING
DIGITAL INSTRUMENTATION AND CONTROL
MARCH 26, 2004
ROCKVILLE, MARYLAND

- STATUS REPORT -

PURPOSE:

The purpose of this Plant Operations Subcommittee meeting is to discuss digital instrumentation and control (I&C) research activities, including development of digital system reliability models, with representatives of the Office of Nuclear Regulatory Research and other interested parties.

BACKGROUND:

For existing and advanced reactor power plants, designers continue to agree that plant operators must be provided with measurement systems that have maximum stability, reliability, and maintainability to monitor and measure the four fundamental physical variables - temperature, pressure, flow, and nuclear flux - necessary to safely operate and control a power reactor facility. These measurement systems have, in the past, relied primarily on the use of copper wires to transmit data. However, the industrial base has largely moved to digital-based systems and therefore more emphasis has been placed on minimizing the use of copper wire and embracing the use of optical-based and wireless technologies for future plant designs and existing plant upgrades.

Advanced reactor designs in the U.S. are being developed to rely exclusively on digital I&C systems designed to make the advanced plants simpler and safer. As a result, it is increasingly important that the NRC and industry understand the effects of various failure modes, including common cause failures and common mode failures in these systems, since the failure of an I&C system could lead to risk significant events.

DISCUSSION

During a joint subcommittee held October 9, 2003, a request was made for an additional briefing on digital failure assessments methods and system models, specifically in model development and validation. In response to that request, the NRC Office of Research is scheduled to provide additional information regarding the ongoing research projects in I&C system reliability. These studies are included in the ongoing cooperative agreements with the University of Virginia (UVa), the University of Maryland (UMd), and Brookhaven Nation Laboratory (BNL). The projects include:

> The Center for Safety-Critical Systems at UVa study of the use of fault tolerant methods to develop detail digital system fault models that can be used in developing digital system reliability estimates. It is anticipated that the studies in this area will enable the quantification of digital system reliability and safety for advanced complex processor-based safety-critical systems, making it suitable for the modeling and analysis of failures of hardware and software.

The UMd study on the use of software engineering metrics to quantitatively assess software quality and predict "software reliability" of digital systems. UMd has completed small-scale evaluations of risk prediction systems (RPS) for predicting software quality and to a lesser extent, its usability. These studies were necessary to determine whether theoretical and practical roadblocks are present that would impede performing a large-scale validation study of more complex and highly reliable applications. The results of the study provided preliminary evidence that the ranking of software engineering measures for the assessment of the quality of software in safety-critical applications is correct. Large-scale validation is ongoing.

Brookhaven National Lab's (BNL) work on digital system failure modes and effects analysis and PRA integration. This study is to investigate the integration of digital systems into the PRAs for current generation nuclear power plants.

EXPECTED COMMITTEE ACTION

The Subcommittee Chairman will provide a report to the full Committee during the 511th ACRS Meeting summarizing the subcommittee discussions.