November 21, 2005

MEMORANDUM TO: ACRS Members

FROM: Eric A. Thornsbury, ACRS Senior Staff Engineer **/RA/**

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION & CONTROL SYSTEMS, OCTOBER 20-21, 2005 - ROCKVILLE, MARYLAND

The minutes of the subject meeting, issued November 8, 2005, have been certified as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated

Electronic cc: J. Larkins
A. Thadani
M. Scott
S. Duraiswamy
M. Snodderly

November 8, 2005

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

FROM: Eric A. Thornsbury, ACRS Senior Staff Engineer **/RA/**

SUBJECT: WORKING COPY OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION & CONTROL SYSTEMS, OCTOBER 20-21, 2005 - ROCKVILLE, MARYLAND

A working copy of the minutes for the subject meeting is attached for your review. Please review and comment on them. If you are satisfied with these minutes please sign, date, and return the attached certification letter.

Attachment: Minutes (DRAFT)

cc: Digital Instrumentation & Control Systems Subcommittee Members
T. Kress
J. Larkins
A. Thadani
M. Scott
S. Duraiswamy
M. Snodderly

MEMORANDUM TO: Eric A. Thornsbury, ACRS Senior Staff Engineer

FROM: George E. Apostolakis, Chairman
Digital Instrumentation & Control Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION & CONTROL SYSTEMS, OCTOBER 20-21, 2005 - ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting on October 20-21, 2005, are an accurate record of the proceedings for that meeting.

/RA by George E. Apostolakis**/** 11/17/05
George E. Apostolakis Date
Subcommittee Chairman

CERTIFIED
11/17/05
By George E. Apostolakis
Issued: 11/8/05

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION & CONTROL SYSTEMS
MEETING MINUTES - OCTOBER 20-21, 2005
ROCKVILLE, MARYLAND

INTRODUCTION

The ACRS Subcommittee on Digital Instrumentation & Control Systems held a meeting on October 20-21, 2005, in Room T-2B3, 11545 Rockville Pike, Rockville, MD. The purpose of this meeting was to review the status of the draft Digital Systems Research Plan for FY 2005-2009, projects from three sections of the plan, and a report by EPRI on defense-in-depth and diversity assessments for digital systems. Except for the session on Security of Digital Systems, the meeting was open to public attendance. Eric Thornsbury was the Designated Federal Official for this meeting. There were no written comments or requests for time to make oral statements from the public. The meeting was convened by the Subcommittee Chairman at 8:30 a.m. on October 20, 2005, recessed at 5:50 p.m., reconvened at 8:30 a.m. on October 21, 2005, and adjourned at 11:50 a.m.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman
M. Bonaca, Member
J. Sieber, Member
T. Kress, Member
S. Guarro, Consultant
E. Thornsbury, Designated Federal Official

Principal NRC Speakers

W. Kemper, RES
S. Arndt, RES
C. Antonescu, RES
K. Korsah, ORNL
W. Hines, UT
M. Waterman, RES
R. Shaffer, RES
R. Wood, ORNL
P. Ewing, ORNL

Other Principal Speakers

R. Torok, EPRI
T. Nguyen, EPRI/EdF
J. Stringfellow, Southern Nuclear
D. Blanchard, Applied Reliability

Other members of the public were in attendance at this meeting. A complete list of attendees is in the ACRS Office File and will be made available upon request. The presentation slides and handouts used during the meeting are attached to the office copy of these minutes.

OPENING REMARKS BY CHAIRMAN APOSTOLAKIS

George Apostolakis, Chairman of the ACRS Subcommittee on Digital Instrumentation & Control Systems, convened the meeting at 8:30 a.m. Dr. Apostolakis stated that the purpose of this meeting was to discuss the NRC staff's Draft Digital Systems Research Plan, three specific research programs discussed in the plan, and an EPRI report on defense-in-depth and diversity assessments for digital systems. He said the Subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee. The rules for participation in the meeting were announced as part of the notice of the meeting published in the Federal Register on September 29, 2005. Dr. Apostolakis acknowledged that no written comments or requests for time to make oral statements had been received.

DISCUSSION OF AGENDA ITEMS

Security Aspects of Digital Systems (3.4)

This session was closed to the public pursuant to 5 U.S.C. 552b(c)(3) to discuss Safeguards Information. William Kemper, RES, introduced the presenters the Subcommittee would be hearing and stated that the objective of the meeting was to brief the Subcommittee on the details of the remaining sections of the research plan. He then introduced Mr. Roman Shaffer to discuss the details of this section of the research plan.

Mr. Shaffer discussed the details of the cyber security research program and the regulatory bases for cyber security research. He provided a summary of cyber security research completed during FY 2001 - FY 2004, discussed current potential cyber security concerns, and described the research planned for FY 2005 - FY 2009.

Mr. Michael Waterman provided additional detail through a presentation on the Network Security project. This project addresses secure network design techniques, wireless network security, and firewall security.

EPRI Guidance for Performing Defense-in-Depth & Diversity Assessments for Digital Upgrades: Applying Risk-Informed and Deterministic Methods

Following the previous subcommittee meeting, EPRI requested an opportunity to brief the subcommittee regarding their recent work on defense-in-depth and diversity for digital upgrades. Mr. Ray Torok, representing EPRI, introduced the topic for the subcommittee. Mr. Jack Stringfellow, Southern Nuclear, is the working group chairman, and he provided a discussion of the background behind the project and the interactions thus far between the working group and the NRC staff. The report documenting the work has been submitted to the staff for review, but the staff considers it a draft at this point and has not accepted it for official review yet. Mr. Stringfellow also discussed the regulatory environment and the need for a

stable, predictable, and practical licensing approach for digital upgrades. He noted that digital upgrades are in progress at many plants, for many types of systems, but that the issue of software common-mode failure is still unsettled between the industry and the agency.

Mr. Torok then continued the presentation by reviewing current regulatory guidance and showing where the EPRI method can offer advantages. He provided two examples in which he demonstrated how a risk-informed approach would differ from and improve upon a deterministic approach. Mr. Torok then described the three methods described in the report: an extended deterministic method, a standard risk-informed method, and a simplified risk-informed method. All of EPRI's methods make use of a "defensive measures" approach to examine the digital system's features that limit the effects of any potential failures.

Mr. Thuy Nguyen continued the briefing by describing how digital system failures are related to digital system common cause failures. He used the minefield metaphor to describe what factors influence the behavior of the software in the digital system. He argued that platform software may not be a dominant cause of digital common cause failure due to its more predictable behavior. Mr. Nguyen also discussed the two types of faults likely to occur in application software: specification faults and software implementation faults. His conclusion was that a digital system with appropriate defensive measures can be shown to be at least as reliable as an equivalent analog system.

Mr. Dave Blanchard then concluded the presentation by discussing the methods used to analyze digital systems and the risk insights developed by EPRI. He discussed results from two limited-scope probabilistic risk analysis studies that performed sensitivity studies on digital system failure probabilities and common cause probabilities. The study suggests that the value of defense-in-depth and diversity is dictated by the frequency of the initiating event and the existing electrical and mitigating components in the overall system. During this discussion, Mr. Pete Morris, Westinghouse, added comments that he believes digital systems have shown they are highly reliable in other industries.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked what EPRI wanted the NRC to do with their report. Mr. Torok said that EPRI submitted the report for the staff's review, hoping for an endorsement. Mr. Kemper explained that the staff has several options by which to endorse such a document – for example, through a regulatory guide or a safety evaluation report. Mr. Torok said it could also be endorsed through a regulatory information summary or by reference in the standard review plan. Mr. Kemper said the staff plans to return to the Committee with whichever method is chosen. Mr. Howe, from NRR, also acknowledged the Committee's interest and will return if the report is reviewed by NRR.

- Dr. Apostolakis asked EPRI to clarify their assertion that the staff is not honoring previous SERs. Mr. Torok indicated that the staff is reopening issues addressed in a platform SER, causing difficulties for the utility's schedule and cost. Dr. Apostolakis commented that it can also be difficult for the staff if new adequate protection questions are raised.

- Dr. Bonaca asked if the Chapter 15 FSAR analyses would have to be repeated to ensure consistency with the upgraded systems. Mr. Stringfellow answered that they

would not – the new analyses would only serve to identify those areas where diversity can have the most benefit.

- Mr. Sieber asked how installing a diverse backup system does not improve reliability. Dr. Apostolakis reiterated Mr. Torok's discussion that the reliability of a system is often dominated by the large rotating machinery, so the overall reliability may not be improved with an additional I&C system. Dr. Apostolakis and Mr. Sieber agreed that this is not necessarily a good argument, else much of the plant's equipment could be removed.

- Dr. Bonaca asked about the criteria used for determining how reliable a digital system needs to be. Mr. Torok explained that the risk-informed approach wants to show that the digital system does not dominate the failure probability of the system it is in.

- Dr. Guarro questioned the assertion that the likelihood of specification errors is comparable for equivalent analog and digital systems. He discussed his experience with engineers and software programmers and the different design processes they use.

- Dr. Kress asked the EPRI representatives for their definition of a diverse system. Mr. Torok said that you must have reasonable assurance that it is not subject to the same common cause failure, and that you must look inside the systems and applications at the assumptions to make that case. Mr. Nguyen added that the defensive measures discussed can also help provide that assurance.

Systems Aspects of Digital Technology (3.1)

To begin the review of detailed sections of the Digital System Research Plan, Mr. Steven Arndt and Mr. William Kemper provided an overview of Section 3.1, System Aspects of Digital Technology. The plan describes seven projects in this section; Section 3.1.1, Environmental Stressors, will be discussed in detail later in the meeting. The systems aspects of digital technology involve those factors that affect the performance of a digital system as a whole.

Current environmental stressors projects include work to enhance the technical bases for electromagnetic interference & radio frequency interference, development of regulatory guidance for lightning protection, and development of qualification standards for computers in mild radiation environments. Systems Communications, Section 3.1.2, will gather the information necessary to evaluate complex digital systems for communications issues. Section 3.1.3 will assess the currently available methods for quantitatively determining the acceptability of commercial off-the-shelf (COTS) components.

Mr. Arndt and Mr. Kemper continued to describe the work in this section of the research plan. Project 3.1.4 will improve the agency's understanding of the effects of electrical transmission and distribution disturbances on digital systems. Section 3.1.5 will assess the effects of total harmonic distortion (THD) on digital component performance. Under Section 3.1.6, the staff will study the design aspects, best practices, and failure models of likely operating systems and identify safety-critical design aspects for operating systems.

Project 3.1.7 is the staff's counterpoint to the EPRI work on defense-in-depth and diversity for digital systems that we heard about earlier in the meeting. To address this issue, the staff will

perform case studies of digital system configurations to determine their susceptibility to common mode failure, test the coping strategies in NUREG/CR-6303 to develop best practices, review insights from probabilistic analysis of common mode failure, and verify that the existing guidance in Branch Technical Position HICB-19 is realistically conservative from a deterministic standpoint. The goal of this work is not to oppose that of EPRI, but to enable both groups to work together toward a common understanding of the issue.

Ms. Christina Antonescu and Mr. Richard Wood provided the subcommittee with additional detail on the work under Section 3.1.1, Environmental Stressors. They discussed the three main areas of work: lightning protection, environmental qualification for mild radiation environments, and electromagnetic compatibility. Ms. Antonescu discussed the staff's revision of the draft regulatory guide on environmental qualification for mild environments (DG-1077) and plans to return it to the Committee (as DG-1142) before issuing it.

Ms. Antonescu also discussed the current research on electromagnetic compatibility. In particular, she and Mr. Wood discussed EPRI's request for the staff to modify a particular high-frequency susceptibility test that is difficult for many types of equipment to pass. This particular test is based on plant data and analysis from EPRI, which they now claim were flawed. Under this work, the staff is reviewing the new information from EPRI to determine if changes are justified.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked about the applicability of the research in this section for simple, actuation-only digital systems. Mr. Arndt and Mr. Kemper agreed with the assertion that actuation systems may be simpler, but also noted an example of a more complex system being proposed for possible use that includes communication protocols and other complicating features.

- Mr. Sieber asked about the interpretation of General Design Criteria 24 as it applies to separation between protection and control. Mr. Kemper noted that such separation is not done from a design standpoint, though it is not specifically prohibited. The staff is investigating the communication issues among functions to see if this concept is violated. They also discussed the needed separation between channels. Mr. Loeser added that reviewers examine the defense-in-depth and diversity between protection and control systems, between channels, and between safety functions on a single processor during their review.

- Dr. Apostolakis asked the staff for the current regulatory conditions for total harmonic distortion. Mr. Loeser described the current review process, and the challenges the staff is facing as newer technology uses lower voltages. Dr. Apostolakis emphasized that this kind of information (i.e., the real regulatory needs) should be more evident in the plan.

- Mr. Sieber asked if the staff was planning to obtain additional conducted emissions data related to the high-frequency susceptibility test or use EPRI's new data. Ms. Antonescu and Mr. Wood answered that the staff was reviewing the available data and would acquire new data if necessary.

Emerging Digital Technology & Applications (3.5)

Ms. Antonescu continued the briefing with a discussion of the research under Section 3.5 of the research plan. She was assisted by Mr. Arndt and Mr. Kofi Korsah. Ms. Antonescu pointed out that knowledge about new and emerging technologies is critical for NMSS, NRR, & NSIR to be able to license such technologies in a safe, efficient, and realistic manner. She briefly discussed the three ongoing projects and described the planned future projects. She also noted that the investigation of emerging technologies is based on an NRR user need and is a continuation of a project under the previous research plan. The topics of focus in this research area include sensors & measurement systems, communications media & networking, microprocessors & other integrated circuits, computational platforms, diagnostics & prognostics, control & decisionmaking, and high-integrity software.

Mr. Korsah presented a portion of the briefing to discuss the details of additional research on sensors and measurement systems. He showed the results of work investigating silicon carbide flux monitors, fuel mimic power monitors, Johnson noise thermometry, and radiation-hardened I&C technology. The staff plans to update their reports on emerging digital technology on a triennial basis.

Ms. Antonescu and Mr. Paul Ewing continued the discussion by presenting the staff's recent work on wireless technology (3.5.6). During the first phase of the research, the staff identified the state of wireless systems and investigated the deployment issues associated with wireless systems in nuclear power plants. The second phase, which is ongoing, is conducting confirmatory research on the initial findings and establishing a technical basis for an agency regulatory position. They described the different types of wireless networks and their associated ranges, uses, and governing standards.

Mr. Arndt and Mr. Wes Hines concluded the presentations with a discussion of the recent research on on-line sensor calibration monitoring and effective uncertainty estimation. They discussed the objectives of the research and presented the details of several uncertainty analysis methods. Mr. Hines described a process equipment monitoring toolbox to enable the staff to experimentally verify the assumptions used in the commercial monitoring tools.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Guarro asked if the staff was aware of the issues the aerospace industry has encountered with FPGAs. Mr. Wood and Mr. Korsah stated their familiarity with the issues. Mr. Nguyen also commented on his work to provide solutions to those types of failures. Dr. Guarro offered to provide some references.

- Dr. Kress asked about the ability of wireless communications by radio frequency to be interfered with. Dr. Ewing noted that it is not a matter of shielding, but encryption.

- Dr. Apostolakis asked about the final documents for the on-line sensor work, stressing that the review staff needs clear guidance to aid their review.

Closing Discussions

At the conclusion of the first day, Dr. Apostolakis and other subcommittee members discussed ideas with the staff for improvements to the plan and the presentation to the full Committee. Dr. Apostolakis suggested linking the activities in the plan to the NRC's overall safety mission (public health and safety) in a similar way as the reactor oversight process. He suggested working down from the overall mission, through the strategic performance areas and the cornerstones of safety, to identify the functions and unique characteristics that fit in each category. Other members of the subcommittee joined him in this suggestion.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked the staff what they desire to obtain from the full Committee meeting. Mr. Kemper asked for a letter stating that the plan contains a good research program. Mr. Arndt also welcomed comments on the priorities or resources. Mr. Sieber suggested the Committee write a letter stating that the plan is appropriate to meet the agency's needs.

- Dr. Bonaca commented that it is a good plan and a coherent summary of the planned work. More information on the challenges in the field would be helpful to the Committee.

- Mr. Sieber suggested starting with the changes that will be happening to the plants, how the agency needs to respond to them, the challenges those responses involve, and how the research plan will prepare the agency for those challenges. The other Members agreed.

- Dr. Guarro stated that he was impressed with how comprehensive the plan is.

- Dr. Kress agreed that the plan is well thought out and comprehensive.

- Mr. Sieber expressed worries about knowing what kinds of systems we will actually see in plants. He questioned whether these were the right tasks to direct research resources toward. He believes so, but without much basis.

SUBCOMMITTEE DECISIONS AND ACTIONS

The Full Committee will review and comment upon the draft Digital Systems Research Plan.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE PRIOR TO THIS MEETING

1. US NRC, "A Study of Safety System Isolation from Cyber Attacks," NUREG/CR-XXXX, ORNL/TM-2003/185, May 2004. [SGI document]
2. EPRI, "Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades," #1002835, December 2004. [document provided with June subcommittee meeting materials]
3. Memorandum from Evangelos C. Marinos, Section Chief, Instrumentation and Controls Section, Division of Engineering, NRR, to Steve Dembek, Section Chief, Project

Directorate Section IV-2, Division of Licensing Project Management, NRR, "Review of Siemens Topical Report EMF-2110 (NP), Revision 1, 'Teleperm XS: A Digital Reactor Protection System'," 13 April 2000. [ADAMS ML003703082]

4. Letter from Ron A. Jones, Vice President, Oconee Nuclear Site, to US Nuclear Regulatory Commission, "License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change (TSC) Number 2004-09," 14 February 2005. [ML050550470]- [Cover memo and attachment 3 only]
5. US NRC, "Technical Review of On-line Monitoring Techniques for Performance Assessment, Part I State of the Art," NUREG/CR-xxxx, August 2005.
6. US NRC, "Assessment of Wireless Technologies and Their Application at Nuclear Power Plants," NUREG/CR-6882, July 2005.
7. EPRI, "Guidelines for Electromagnetic Interference Testing of Power Plant Equipment," Revision 3 to TR-102323, November 2004.

****

Note: Additional details of this meeting can be obtained from a transcript of this meeting available for downloading or viewing on the Internet at http://www.nrc.gov/ACRSACNW or can be purchased from Neal R. Gross and Co., Inc., (Court Reporters and Transcribers) 1323 Rhode Island Avenue, NW., Washington, DC 20005 (202) 234-4433.