September 8, 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, JUNE 14-15, 2005 - ROCKVILLE, MARYLAND

The minutes of the subject meeting, issued July 21, 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

July 21, 2005

MEMORANDUM TO: George E. Apostolakis, Chair
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, JUNE 14-15, 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, Chair
Digital Instrumentation & Control Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION & CONTROL SYSTEMS, JUNE 14-15, 2005 - ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting on June 14-15, 2005, are an accurate record of the proceedings for that meeting.

/Original Signed by/ 09/08/05
George E. Apostolakis Date
Subcommittee Chair

Issued: 7/21/05
Certified: 9/8/05

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION & CONTROL SYSTEMS
MEETING MINUTES - JUNE 14-15, 2005
ROCKVILLE, MARYLAND

INTRODUCTION

The ACRS Subcommittee on Digital Instrumentation & Control Systems held a meeting on June 14-15, 2004, in Rooms T-2B1 & T-2B3, 11545 Rockville Pike, Rockville, MD. The purpose of this meeting was 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 meeting was open to public attendance. Mike Snodderly was the Designated Federal Official for this meeting. Eric Thornsbury was the cognizant staff engineer. There were no written comments or requests for time to make oral statements from the public. The meeting was convened by the Subcommittee Chair at 8:30 a.m. on June 14, 2005, recessed at 5:02 p.m., reconvened at 1:31 p.m. on June 15, 2005, and adjourned at 5:23 p.m..

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chair
M. Bonaca, Member
T. Kress, Member
J. White, Consultant
S. Guarro, Consultant
M. Snodderly, Designated Federal Official
E. Thornsbury, Cognizant Staff Engineer

Principal NRC Speakers

W. Kemper, RES
G. Tartal, RES
S. Arndt, RES
H. Hamzehee, RES
S. Morris, NSIR
M. Waterman, RES
N. Carte, RES
R. Shaffer, RES
T. Hilsmeier, RES

Other Principal Speakers

J. Calvo, NRR
C. Grimes, NRR
T. Chu, BNL
R. Torok, EPRI
R. Barrett, RES
M. Li, UMD
T. Aldemir, OSU

Other members of the public were present 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 CHAIR

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, the staff's approach to revising Regulatory Guide 1.97, and two specific research programs discussed in the plan: software quality assurance and the risk assessment of digital systems. He said the Subcommittee would 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 May 31, 2005. Dr. Apostolakis acknowledged that no written comments or requests for time to make oral statements had been received from the public.

DISCUSSION OF AGENDA ITEMS

Reconciliation of Comments on Draft Research Plan

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 various topics contained within the draft research plan. Mr. Kemper commented on the proactive communications with NRR, NSIR, and NMSS to improve the research plan. He then introduced Mr. Michael Waterman to discuss the resolution of comments on the research plan.

Mr. Waterman discussed the goal to make the research plan a “living document” that will be updated in response to communications with the supported offices as new needs are identified. The major focus of the research plan is to augment and supplement the agency’s existing process, such as those in the Standard Review Plan. The purpose of the research is to investigate current and emerging methods and knowledge and, where appropriate, augment and supplement NRC processes to enable NRC staff to evaluate digital systems consistently and effectively. The Office of Research is also trying to incorporate informal comments from NRR into the plan. Mr. Waterman then reviewed the public comments and their resolution section-by-section through the research plan.

Mr. Jose Calvo of NRR also asked to make comments regarding the research plan. He first described the current way NRR performs reviews – to review the process and not the product. They then can perform audits to make sure the system performs consistently. He also discussed the recent reviews the staff has done. He stressed the idea of the offices getting together to discuss the research plan and working out differences. Disagreements still exist, but the offices are moving closer.

Mr. Evangelos Marinos of NRR also added comments regarding the current Standard Review Plan issued in 1997 and the upcoming review of a submittal from Oconee, which will be a good test of the current process. The staff has also monitored international use of the standard review plan process in Taiwan and South Korea. Mr. Marinos believes that concurrence by the NRR/EEIB branch would have constituted a user need request, where the staff did not feel one was necessary. However, the staff does support anticipatory research. Mr. Calvo recommended that the Committee get involved with the upcoming Oconee review.

Mr. Richard Barrett, RES Division Director, commented on the various processes by which RES gains user-office support for research programs. They are sometimes more proactive and do not necessarily wait for user needs from the other offices. Mr. Christopher Grimes, NRR deputy division director, commented on the focus on process improvements, the need for constructive comments from NRR, and the use of TAGs to facilitate ongoing communication.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. White asked about the use of metrics to evaluate the research effectiveness. Mr. Waterman responded that the office has internal reviews of programmatic effectiveness to accomplish this purpose, and that it might be a good topic for a supplemental document.

- Dr. Apostolakis asked about the use of Technical Advisory Groups (TAGs). Mr. Kemper answered that they are examining the use of TAGs, and would likely use one TAG with all offices included (NRR, NMSS, and NSIR).

- Dr. Apostolakis suggested that RES get input from the other offices regarding their urgent needs to help prioritize the work.

- Dr. Apostolakis asked how operating experience, both nuclear and non-nuclear, is being used to develop the plan. Mr. Kemper commented how they are examining operating experience. Different systems in different industries are qualified to different levels of quality, and that is being taken under consideration as they examine operating experience.

- Dr. Apostolakis commented on how the state of digital systems review is similar to the whole regulatory structure from 40 or 50 years ago, where the application of risk assessments found holes in the traditional approaches and improved the overall process.

- Dr. Bonaca commented on the resistance to developing risk-informed approaches in other disciplines, much like here. He commented that often, research such as this must be viewed more long-term than your immediate needs.

Draft Revision of Reg Guide 1.97

Mr. Kemper introduced the session on the draft Revision 4 to Regulatory Guide 1.97, “Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.” The regulatory guide is a work in progress, and the staff asked the Subcommittee for informal comments on the approach. Mr. Kemper described the new regulatory guide’s endorsement of IEEE Std. 497-2002, which describes a new approach to identifying post-accident monitoring instrumentation. The new revision has broader guidance to accommodate non-light-water reactors and other advanced reactor designs. He then introduced Mr. George Tartal to lead the presentation.

Mr. Tartal provided a brief background on the history of accident monitoring, then discussed the current revision, Rev. 3 of Reg Guide 1.97. Then he provided a brief overview of IEEE Standard 497-2002, a revised standard for the selection, performance, design, qualification,

display, and quality assurance criteria for accident monitoring. Mr. Tartal then described the draft guide, DG-1128, focusing on the regulatory positions and the issues the staff addressed in trying to endorse the IEEE standard.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Bonaca commented on the less-prescriptive approach taken in the new revision of the regulatory guide. He expressed concern about piecemeal applications and how that could take plants away from the standardization implemented in the plants today.

Software Quality Assurance (3.2)

Mr. Kemper provided an overview of the upcoming detailed presentations for section 3.2 of the research plan, software quality assurance. He then provided background on the current process for evaluating the software quality of licensee applications using SRP Chapter 7 (Revision 4 issued in 1997). To do this, NRC reviews the developmental process and the measures produced by the licensees. This review depends on qualitative evaluations. The software quality assurance evaluations are done manually, without the aid of computerized assessment tools or other means of obtaining quantitative measures of software quality. Mr. Kemper compared this with the way the agency does independent analysis of fuel designs or probabilistic risk analysis to verify the licensee's conclusions.

Mr. Kemper also discussed the approach to reviewing the software quality assurance methods and tools that exist in other sectors of the process industry. If possible, the staff will adapt these tools for deployment on software systems within the nuclear industry. The research in this area will focus on assessing possible analysis methods currently used in design and analysis of safety-critical software systems.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked why formal methods were not pursued. Mr. Arndt described previous research performed as part of the cooperative agreement with the Halden project. The staff continues to follow the work to provide background information to the research program.

- Dr. Apostolakis asked about the distinction between software quality assurance and risk analysis. Mr. Arndt described the quality assurance issue as an effort to get a higher level of confidence that the software is performing safety functions appropriately. The quality assurance may or may not produce quantitative estimates.

Assessment of Software Quality (3.2.1)

To lead the discussion on this portion of the research plan, Mr. Kemper introduced Mr. Norbert Carte, a member of the RES I&C team. Assisting with the presentation was Dr. Ming Li, of the University of Maryland.

Mr. Carte provided an overview of the Assessment of Software Quality program. The basic issue facing NRC is the increasing size and complexity of software in upcoming submittals. Mr.

Carte described the objective of the project: to perform a large-scale validation of measures identified through previous research to assess the quality of software quantitatively. One challenging portion of the project is the development of acceptance criteria. He also discussed the large literature base supporting the use of software quality metrics, though such use does not eliminate the need for human judgment.

Mr. Carte specifically discussed the issues raised during previous ACRS meetings. The project is now looking at an actual nuclear safety system rather than the low-reliability system examined earlier in the project. He also discussed the ease of obtaining the metrics and the uncertainty in these measurements.

Dr. Li then discussed some technical details of the work. He discussed the connection between software engineering measurements and software quality and two specific measures being used. First he discussed defect density and the techniques to measure the number of defects remaining in software.

Mr. Arndt discussed the multiple roles of the software quality assurance program. First is to understand the system better. Second is to produce a quantitative assessment of software quality.

Mr. Li then discussed his second measure, test coverage. Test coverage is the portion of software statements executed against a set of test cases. Mr. Li stated that the end goal is to produce the probability of failure per demand for software.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis questioned the assumptions underlying the capture/recapture approach to measuring defect density. Mr. Carte further described the process and Dr. Kress noted his acceptance of the methods to correlate the data.

- Dr. Apostolakis asked about the assignment of probabilities to different conditions. He specifically commented that the methods needed to consider accident conditions more than normal operations. Dr. Guarro also cautioned the staff against extrapolating statistics for routine operation to rare accident scenarios.

- Dr. Apostolakis stated his support for the objective of gaining a better understanding of the system, but expressed doubts about calculating probabilities.

- Dr. Apostolakis expressed a concern that the focus seems to be on the number of defects, rather than the kinds of defects and their severity.

Digital System Dependability (3.2.2)

After a brief introduction, Mr. Arndt introduced Mr. Shaffer, who discussed the goals of the research, the motivation for performing the work, some fundamental concepts, and its applicability to the regulatory assessment process. The effort will supplement and augment the current regulatory process by defining objective acceptance criteria for digital technology from a system perspective. Another aspect of this research is to investigate if the data from this

research, such as on failure modes and likelihoods, will be applicable to probabilistic risk assessments.

Mr. Shaffer used several figures to illustrate the modeling approaches being taken to the digital system dependability analysis. He also described tools and models developed at the University of Virginia to perform the fault injection experiments on which this work is based. Mr. Shaffer discussed similar goals as the previous project. First, to gain a better understanding of the system, and then to gain numerical estimates of the dependability of digital systems.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. White asked about the inclusion of common failures (i.e., multiple faults) in the assessment. Mr. Shaffer answered that they do indeed handle multiple faults, and let the assessment determine whether they produce common mode failures.

- Dr. Apostolakis discussed his concern with numerical estimates, particularly due to changes in the software once faults are discovered and corrected.

Self-Testing Methods (3.2.3)

Mr. Arndt provided a brief presentation on the research into self-testing methods. Not a lot has been done yet on this project, so he provided a general overview. He described self-test methods as continuous hardware or software tests done to improve the system's availability. One big issue is the complexity added by these functions. Mr. Arndt said the real issue was the tradeoff between improved system performance and the new failure modes that may be introduced by the self-test features due to the increased complexity.

Risk Assessment of Digital Systems (3.3)

Mr. Arndt provided general background on the overall risk assessment program, including the reasons for doing it, its importance, and the structure of the overall program. He referred to the NRC's PRA policy statement, which encourages the use of PRA to the extent supported by the state-of-the-art and data. The issue for this project is whether the state-of-the-art supports such use for digital systems.

The research in this section of the research plan is oriented toward improving the NRC's knowledge and providing consistent regulatory processes for regulating digital systems. To do so, Mr. Arndt stated that they would gather and understand the data, assess the modeling methods that might be used, and understand the systems that need to be modeled. They will also need to develop regulatory acceptance criteria.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis asked for an example of how the current licensing criteria are difficult to meet. Mr. Arndt described the diversity and defense-in-depth requirements in BTP-19, which requires an analysis of the results of a common mode software failure. Because this is a deterministic analysis with conservative assumptions, meeting it for some design-basis accidents can be difficult. Mr. Torok (EPRI) provided his opinion that the

probability of failure for most systems is dominated by the large rotating machinery, and not the instrumentation and control. Therefore, the requirements that may be imposed by the current licensing structure may not be necessary.

- Dr. Apostolakis reinforced his comments from a previous ACRS letter that we should question the basic assumptions behind any model because the evidence suggests that most problems come from specification errors, requirements, and design-type errors.

Development and Analysis of Digital System Failure Data (3.3.1), Investigation of Digital System Failure Assessment Methods (3.3.2), Investigation of Digital System Risk Characteristics (3.3.3), & Investigation of Digital System Reliability Assessment Models (3.3.4)

To start the second day of the meeting, Mr. Kemper introduced Mr. Arndt, who discussed how this project is being performed in coordination with the RES Probabilistic Risk Analysis branch. The 3.3.1-3.3.4 section is being worked on by two teams; one team is from PRAB, with Brookhaven National Laboratory, and the other team is from the I&C section, with The Ohio State University. He then turned the presentation over to PRAB.

Mr. Hamzehee, the section chief in charge of this work, started the presentation. He stated the goal of the work to develop a probabilistic method for modeling the potential failures of a digital I&C system that can later be integrated with the probabilistic risk assessment using traditional methods. To be able to quantify the reliability of a digital system, we need to have both models and data. He then introduced Mr. Hilsmeier, a member of his staff, to provide more details.

Mr. Hilsmeier presented the details of each task in the Digital Systems PRA Project Plan.

Mr. Torok suggested several questions for the staff to consider. Had looked at the sensitivity of the core damage frequency to how the I&C is modeled in the PRA? What is the target reliability needed from I&C to make it a negligible contributor to risk? How are they using data from other industries? Have they looked at the possibility of comparing the reliability of the analog systems to the digital systems? Mr. Torok also offered to brief the subcommittee on EPRI's method for addressing the risk of digital system upgrades.

For the second part of the presentation, Mr. Arndt provided some background on the work, then stated that the idea behind the work is to look at the different kinds of methods to examine their usefulness. This part of the work focuses on the dynamic interactions in the process. He then introduced Professor Aldemir to provide details of the work.

Dr. Aldemir discussed the differences between analog and digital systems that make them a challenge. Among these differences is the lack of good definition in the potential failure modes of a digital system. He described three types of dynamic methods: continuous time methods, discreet time methods, and visual methods. Dr. Aldemir presented some details of the two methods chosen for further investigation: the dynamic flowgraph methodology and Markov models.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Apostolakis suggested the staff consider soliciting comments from the public on the data collection project before the end. Mr. Hamzehee and Mr. Kemper agreed.

- Dr. Apostolakis asked about the Reliability Analysis Center and access to their data. Mr. Hamzehee and Mr. Chu stated that the data was proprietary, but they had purchased access to the data. If it relied upon heavily during the project, Dr. Apostolakis suggests that we examine it more closely.

- Dr. Apostolakis stated his belief that the data collection task is one of the most important tasks in the program, particularly when it includes real operating experience events. The operating experience also provides a test for the potential methods to see if they can model actual events.

- Dr. Bonaca pointed out that the concern in most applications will be the application code, not necessarily the pre-approved digital platform. Mr. Torok agreed.

- Dr. Apostolakis suggested using the challenges with digital systems as a way to judge the helpfulness of the methods. Also, he suggested measuring them against the needs of the agency and the reviewers.

- Dr. Apostolakis suggested that both groups (PRAB/BNL and OSU) use the same requirements for measuring the usefulness of potential assessment methods. He suggested closer collaboration between the groups overall.

- Dr. Apostolakis warned against the use of the Procrustean bed – taking existing models from reliability and forcing them upon software. This is not typically an acceptable approach (as Hercules demonstrated).

Closing Discussions

Mr. Morris provided comments from NSIR regarding section 3.4 of the draft research plan. Because they look at everything differently from a security standpoint, they are interested in any research that helps promote an understanding of the vulnerabilities that exist and how they could be exploited.

General Comments and Observations From the Subcommittee Members and Consultants

- Dr. Kress stated that he is glad to see research doing this work. He believes it will be badly needed in the near future. He particularly pointed out that he liked the idea of looking for modes of failure first, especially from operating experience. He liked the thought about looking at whether one can declare digital systems better than analog systems, and therefore declare them not risk-significant or bound them with analog values. He also stated that since these failures are not random events, they will be sequence dependent. This leads to difficulty finding a failure probability. Overall, he believes the research will bear fruit and be very useful.

- Dr. Bonaca stated that the work on Reg Guide 1.97 is good, but he has questions about backfitting the Reg Guide to older plants. He stated that he was somewhat confused by the software quality presentations and is not too convinced about it yet. He agreed with Dr. Kress regarding the overall need for this work. He stated that he would like to have us involved in the Oconee upgrade. He thinks the research plan is quite significant and he hopes the offices can work out their differences. He believes the agency should continue to look ahead on these issues.

- Dr. Apostolakis agreed with Dr. Kress and Dr. Bonaca that he is pleased that the staff is pursuing this work. Overall, he feels it is a very good program plan, though he feels there are still some fundamental issues that need resolved.

SUBCOMMITTEE DECISIONS AND ACTIONS

The Full Committee will review and comment upon the draft Digital Systems Research Plan. We also expect Regulatory Guide 1.97 to come to the Committee for review soon.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE PRIOR TO THIS MEETING

0. Subcommittee status report, including agenda.
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'," 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]
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.
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.
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.
14. EPRI, “Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades,” #1002835, December 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/reading-rm/doc-collections/acrs/tr/ or can be purchased from Neal R. Gross and Co., Inc., (Court Reporters and Transcribers) 1323 Rhode Island Avenue, N.W., Washington, DC 20005 (202) 234-4433.