



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

June 3, 2004

MEMORANDUM TO: ACRS Members

FROM: Marvin D. Sykes, Senior Staff Engineer */RA/*
Technical Support Staff
ACRS/ACNW

SUBJECT: CERTIFICATION OF THE MINUTES OF THE ACRS PLANT
OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL
INSTRUMENTATION AND CONTROL ON MARCH 26, 2004 AT
ROCKVILLE, MARYLAND

The minutes of the subject meeting, issued on June 1, 2004 have been certified as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated

cc: J. Larkins
H. Larson
S. Duraiswamy
ACRS Staff Engineers



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

June 1, 2004

MEMORANDUM TO: John D. Sieber, Chairman
Plant Operations Subcommittee

FROM: Marvin D. Sykes, Senior Staff Engineer **/RA/**
Technical Support Staff
ACRS/ACNW

SUBJECT: WORKING COPY OF THE MINUTES OF THE ACRS PLANT
OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL
INSTRUMENTATION AND CONTROL, MARCH 26, 2004 -
ROCKVILLE, MARYLAND

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

Attachment: Minutes (DRAFT)

cc w/o Attachment:

J. Larkins
H. Larson
S. Duraiswamy
ACRS File



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

MEMORANDUM TO: Marvin D. Sykes, Senior Staff Engineer, ACRS

FROM: John D. Sieber, Chairman
Plant Operations Subcommittee

SUBJECT: CERTIFICATION OF THE SUMMARY MINUTES OF THE ACRS
PLANT OPERATIONS SUBCOMMITTEE MEETING ON DIGITAL
INSTRUMENTATION AND CONTROL, MARCH 26, 2004 -
ROCKVILLE, MARYLAND

I hereby certify, to the best of my knowledge and belief, that the minutes of the subject meeting on March 26, 2004, are an accurate record of the proceedings for that meeting.

/RA/

June 3, 2004

John D. Sieber, Date
Plant Operations Subcommittee Chairman

CERTIFIED

6/03/04

By John D. Sieber

Issued: 6/01/04

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

On March 26, 2004, the ACRS Plant Operations Subcommittee held a meeting in Room T-2B3, 11545 Rockville Pike, Rockville, Maryland. The purpose of the meeting was to discuss Office of Nuclear Regulatory Research activities related to digital instrumentation and control (I&C) system reliability modeling.

The meeting was open to the public. No written comments or requests to make oral statements were received from members of the public related to this meeting. Mr. Marvin Sykes was the Designated Federal Official for this meeting. The meeting was convened at 8:30 a.m. and adjourned at 3:55 p.m. on March 26, 2004.

ATTENDEES:

ACRS MEMBERS/CONSULTANTS/STAFF

Jack Sieber, Chairman	George Apostolakis, Member
Mario Bonaca, Member	Tom Kress, Member
Peter Ford, Member	Stephen Rosen, Member
Sergio Guarro, ACRS Consultant	James White, ACRS Consultant
Marvin Sykes, ACRS Staff	

ATTENDEES

Steven Arndt, RES	Michael Mayfield, RES
Jiang Hong, NRR	Mike Waterman, NRR
Roman Shaffer, RES	Dean Overland, RES
Doug Tiffit, RES	Tekia Govan, RES
Michelle Evans, RES	Barry Johnson, Univ. of Virginia
Carol Smidts, Univ. of Maryland	Tsong - Lun Chu, BNL
Jerry Mauck, Framatone ANP	Ming Li, Univ. of Maryland
Thomas Roberts, Dept. of Energy	Peter Wilson, RES

The presentation slides and handouts used during the meeting and a complete list of attendees is attached to the Office Copy of these Minutes. The presentation to the Subcommittee is summarized below.

Opening Remarks (Subcommittee Chair)

Mr. Jack Sieber, Chairman of the Subcommittee on Plant Operations convened the meeting by providing introductory remarks and later introducing Mr. Michael Mayfield of the Office of Nuclear Regulatory Research (RES) to begin the staff presentation.

Staff Introduction

Michael Mayfield provided brief opening remarks on behalf of the RES staff and introduced Steven Arndt to begin the discussion.

Digital I&C Research Program, State-of-the-Art in Digital System Reliability, Modeling, and PRA Modeling Program

Mr. Arndt began the presentation by providing an overview of the Digital I&C Research Program Plan, discussed in SECY-01-0155. According to Mr. Arndt, the plan addressed several recommendations highlighted in the National Academy of Science (NAS) review. He noted that the goal of the plan was to develop methods for reviewing digital system reliability models to improve the staff's analytical capabilities, and fundamental knowledge of digital technology as demonstrated by the development of analytical tools and techniques. These tools may be used for estimating digital system failure probabilities and for analyzing digital system reliability models. The use of such models is expected to increase overall confidence and reduce uncertainty.

Mr. Arndt explained that the staff has allocated funds for five general research projects for evaluating software reliability. Four of the five projects involved contractual agreements with the University of Virginia (UVA), University of Maryland UMD), Halden Project, and Brookhaven National Laboratories. The fifth projects is an in-house RES effort aimed at developing a working database of reliability information that may assist the staff in the review and validation of licensee assumptions used to justify plant design changes and license amendment requests. It is anticipated that the products of these research studies will assist in improving the NRC's understanding of digital system failure mechanisms and the strengths and limitations of the available digital system modeling techniques.

Mr. Arndt introduced Barry Johnson, UVA and Carol Smidts, UMD to provide more detailed information on their respective research activities.

Digital Systems Modeling Using Fault Injection Methods (UVA)

Mr. Barry Johnson, Director of the Uva Center for Safety-Critical Systems discussed the integrated digital system modeling project to develop a safety assessment process for digital systems. The process uses commercial-of-the-shelf (COTS) hardware and software and fault injection techniques to evaluate reliability. The trial results are statistically correlated to produce measures of software reliability that may be used to assess the reliability and fault tolerance of the integrated digital systems. This approach and the tools that support this approach have been used extensively to assess digital railway control systems and according to Mr. Johnson, the process has already been successfully applied to several other commercial applications. Modeling of the Calvert Cliffs Digital Feedwater Control System is ongoing.

Mr. Johnson also noted that this research project is expected to provide an assessment method that can be used by the NRC staff to independently assess digital system safety and provide additional information on digital system failure modes and reliability that will inform the review process and guidance. The latest application of this assessment method and the input for the associated risk-informed review guidance will be completed in FY 2005.

Metrics Development and Software Reliability Modeling (Umd)

Professor Carol Smidts, UMd discussed the ongoing software metrics project to develop and pilot a systematic framework that can be used by the NRC staff to independently assess and predict software quality and reliability. This assessment tool uses software metrics to predict software quality and reliability under varying operational conditions. The metrics cover the four aspects of software development, which include requirements specifications, software design, software implementation (coding), and software testing. The quantitative results from this study may be used by the NRC to inform the current review guidance and improve the understanding of software quality and reliability. Large-scale demonstration of this tool in a high reliability nuclear application is planned for completion in early FY 2006.

BNL Research Activities

Steve Arndt briefly discussed the BNL research efforts. BNL is currently engaged in the development of a processor level Markov model for one of the three currently approved platforms to identify the supporting analysis and data needed to model digital design features; development of quantitative methods for assessing software reliability; and digital failure database review.

According to Mr. Arndt , the staff expects to contract with BNL in the future to generate suggestions for improving the integration of digital system risk models into existing PRAs and to develop quantitative methods for reviewing safety-critical systems in PRA-based submittals.

Halden Project

Mr. Arndt explained that the staff is also involved in ongoing work at Halden which includes analysis of operational data related to COTS digital systems, the risk assessment of man-machine interfaces, and the development of tools to assist in combining qualitative and quantitative information in reviews.

Future Plans for Digital System Reliability Modeling

Mr. Arndt provided additional information on future RES plans for continuing and new research projects that will investigate different aspects of risk analysis of digital systems and continually review current and evolving methods. He noted that coordination within the program and with other digital system research in the nuclear and non-nuclear fields is critical.

He restated the scope of the ongoing research activities at UVA, UMd, and BNL and some future proposals. Specifically, he mentioned the proposed research aimed at developing detailed PRA models of sample digital systems, determining the most effective method for digital system modeling, and developing NRC review guidance.

Mr. Arndt closed the presentation by providing information on the expected completion dates for some of the ongoing research studies.

UMd	Early FY 2006 - Intermediate results are to be published in FY 2004.
UVa	FY 2005 - Intermediate results are available.
BNL	FY 2005 - Results of the integration of pilot models into current plant PRAs.

Committee Comments

In general, the Subcommittee recognized that the staff was making considerable progress in developing tools for the evaluation of digital systems that may be used in existing and future plants.

Dr. Apostolakis expressed concern that the RES program may not be on the right path and pondered whether the staff is focusing their efforts on research activities that are most important to the agency. He questioned the staff assertions that the current analysis methods are sufficiently mature because they have been successfully used in other industries. He also critiqued the staff's review of available reliability models to identify strengths and weaknesses of each prior to selecting Markov modeling for the BNL research.

Mr. Rosen questioned the staff approach to evaluating reliability and development of review guidance. He stressed that the NRC staff should develop detailed guidance and acceptance criteria that clearly delineates what must be included in applications related to digital system reliability. The guidance should also indicate how the applications will be evaluated by the staff. This will alleviate the concerns that he staff has regarding what the applications will look like.

Dr. Kress applauded the bold and proactive efforts that RES has undertaken and thought that the program was well-conceived, and the various parts fit together nicely. Dr. Kress urged continued use of international expertise in this area and suggested that the industry, through EPRI or NEI, get more active in this area. For the UMD study, he suggested that the researchers may need to do more to evaluate the metric data dispersion and factor that into the reliability rankings. The rankings should also be updated as more information is accumulated.

Dr. White agreed that the RES program contents were generally in alignment with recommendations made by the National Academy of Science panel and that the program should provide help in answering the questions expected to be asked about how the NRC will do an assessment. He also noted that it was not apparent whether there were enough such programs to allow the development of comprehensive guidance. He supported the idea of mining Licensee Event Reports to get an idea of the frequency and the mode of digital system failures in existing nuclear plants.

Dr. Guarro noted that the approach taken by the UMD software metrics program was reasonable and the expected results could be used to generate quantitative evaluations of software that could eventually be used in PRA quantification. However, he expressed a belief that there are limitations to the validity of the results. He stated that it was unclear if the "reliability predictive model" and associated ranking for each of the metrics considered would remain confirmed for software with different types of functions and/or programming language.

For the studies conducted at BNL, Dr. Guarro suggested that the staff may need to develop a more in-depth, direct understanding of what the existing analytical methods are good for, or not good for. One way of achieving this may be the performance of benchmark analyses with various methods and for a range of possible use objectives. One may in fact argue that more attention should be given to processes and methods that support multiple uses related to risk assessment, e.g., identifying effective software testing strategies, identifying system / software interface failure modes, enabling bounding quantification for PRA use, etc.

Staff Commitments

During the meeting subcommittee members requested copies of several documents. Some were available while others were in the developmental stages. The staff committed to provide copies of each of the following documents:

1. NUREG/CR-6734, Digital Systems Software Requirements Guideline, Vol. 2
2. EPRI Defense-in Depth and Diversity Topical Report, January 2004 [DRAFT]
3. Brookhaven National Laboratories - Report on the Review of Current Methods and Tools for Modeling Digital Systems, Expected April 2004
4. Brookhaven National Laboratories Review Guidance for Risk-Informed Digital Submittals, Expected Summer 2004

Subcommittee Decisions and Follow-up Actions

The Subcommittee Chairman will make a report to the full Committee during the April 2004 meeting. The Chairman's report will summarize the discussions and make recommendations regarding the need for future discussions on this matter.

Background Materials Provided to the Committee

1. License Renewal Application for the R. E. Ginna Nuclear Power Plant, dated July 30, 2002.
2. Safety Evaluation Report with Open Items Related to the License Renewal of the R. E. Ginna Nuclear Power Plant, October 2003.
2. NRC Inspection Report 50-244/03-010, Scoping and Screening Methodology, dated August 22, 2003.
3. NRC Audit of the R. E. Ginna Nuclear Power Plant Aging Management Programs, dated September 8, 2003.

NOTE:

Additional details of this meeting can be obtained from a transcript of this meeting available in the NRC Public Document Room, One White Flint North, 11555 Rockville Pike, Rockville, MD, (301) 415-7000, downloading or view on the Internet at <http://www.nrc.gov/reading-rm/doc-collections/acrs/> can be purchased from Neal R. Gross and Co., 1323 Rhode Island Avenue, NW, Washington, D.C. 20005, (202) 234-4433 (voice), (202) 387-7330 (fax), nrgross@nealgross.com (e-mail).