



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

November 1, 2007

MEMORANDUM TO: ACRS Members

FROM: Charles G. Hammer, ACRS Senior Staff Engineer */RA/*

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS
SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL
SYSTEMS, APRIL 18, 2007 - ROCKVILLE, MARYLAND

The Subcommittee Chairman has certified the minutes of the subject meeting, issued October 31, 2007, as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated
electronic cc: FGillespie SDuraiswamy C. Santos

October 31, 2007

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

FROM: Charles G. Hammer, ACRS Senior Staff Engineer **/RA/**

SUBJECT: WORKING COPY OF THE MINUTES OF THE MEETING OF THE ACRS
SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL
SYSTEMS, APRIL 18, 2007 - 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 and Control Subcommittee Members
CSantos

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
MEETING MINUTES - APRIL 18, 2007
ROCKVILLE, MARYLAND

INTRODUCTION

The ACRS Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on April 18, 2007, in Room T-2B3, 11545 Rockville Pike, Rockville, MD. The purpose of this meeting was to review issues related to digital I&C systems used in nuclear power plants. Gary Hammer was the Designated Federal Official for this meeting. The Subcommittee received no written statements or requests for time to make oral statements from the public. The Subcommittee Chairman convened the meeting at 8:30 a.m. on April 18, 2007, and adjourned at 4:29 p.m.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman
T. Kress, Member
S. Guarro, Consultant

S. Abdel-Khalik, Member
O. Maynard, Member

ACRS Staff

G. Hammer, Designated Federal Official

Principal NRC Speakers and Consultants

S. Arndt, RES A. Kuritzky, RES
P. Loeser, NRR C. Doust, NRR

Dr. Tunc Aldemir, Ohio State University

Principal Industry Speakers

A. Marion, NEI K. Keithline, NEI
EPRI

Other members of the public attended this meeting. A complete list of attendees is in the ACRS Office File and is 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

Dr. George E. Apostolakis, Chairman of the ACRS Subcommittee on Digital I&C Systems convened the meeting at 8:30 a.m. Chairman Apostolakis stated that the purpose of this meeting was to discuss the NRC staff and industry activities for digital I&C systems. He stated that the Subcommittee would hear presentations by the NRC's Office of Nuclear Regulatory

Research (RES), the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), and the Nuclear Energy Institute (NEI). 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 March 28, 2007. Chairman Apostolakis acknowledged that the Committee had received no written statements or requests for time to make oral statements from members of the public.

DISCUSSION OF AGENDA ITEMS

NRC Staff Activities Regarding Digital I&C Systems

Mr. Michael Mayfield with the NRO staff made a brief introduction and provided a short background on the current digital I&C activities.

Mr. Alex Marion and Ms. Kimberly Keithline with NEI made a brief presentation regarding the industry perspective on the NRC staff activities for research and guidance development on digital systems. They stated that they are working closely with the staff via steering committee activities, and they believe the NRC research is generally appropriate in most key areas. However, they expressed that they do not support modeling of non-safety digital system backups to determine reliability. They stated there would be enough reliability without it, and that the result would be to add unnecessary complexity to the systems. They stated that NEI/EPRI will be developing several technical papers on the diversity and defense-in-depth (D3) issue over the next few months. They stated that NRC senior staff are steering committee members, and industry representatives also actively participate in all of the meetings. The next meeting will be on June 19-22, 2007.

Representatives of Constellation and AREVA also made statements which indicated that they do not believe a success path will result from the NRC modeling research, that there is no need for modeling of digital systems in PRAs, and that a good engineering design which operates well should provide the needed reliability of a digital system.

The staff made several presentations on digital I&C systems in the areas of: the current regulatory position on D3, short-term activities for D3 issues, D3 research activities, dynamic reliability modeling for PRAs, traditional modeling methods, and the development of regulatory guidance for risk-informing digital system reviews.

The staff outlined safety concerns with both digital I&C software and hardware. They pointed out that the 1997 National Academy of Sciences (NAS) study recommended that NRC retain the position that common mode software failure is credible and that diversity in digital systems is needed. However, they also pointed out that the SRM to SECY 93-087 states that common mode failures are beyond design-basis events; therefore, analysis of such events should be on a best-estimate basis, which means that D3 could be performed by a non-safety system. NUREG/CR-6303 provides the acceptable method for performing D3 analyses, which involves comparing attributes in: design, equipment, functionality, human process, signals, and software. The acceptance criteria for ensuring adequate D3 are provided in BTP 7-19, which references 10 CFR 100 limits.

The staff made a presentation on short-term activities to address D3 issues. One of the overall issues identified is that the available guidance does not explicitly identify acceptable means for achieving D3. This has resulted in several subparts of the issue, called “problem statements” which are directed to specific issues, such as: credit for manual actions and leak detection capability, common cause failures, other system functions (or “echelons”) which separately achieve a safety I&C function, and how common cause failures relate to the single failure criteria. The staff noted that these clarifications are needed because of advances in technology, even though there is already a regulatory basis for D3 for new reactors. The staff is in agreement with the industry that the use of digital I&C has the potential of providing greater safety, but that there are challenging issues in various detailed areas.

The staff also made a presentation on the NRC research plans for D3. Key questions for the research to answer include: what are the effects of common cause failures, how much D3 is enough, what would be good engineering practice, and are there existing endorsable standards. The staff has reviewed the use of digital systems in several other countries, industries, and agencies to look for various strategies for determining adequate levels of D3. The staff plans to integrate the results of the research into NRC guidance on D3 by September 2007.

The staff also made a presentation on the risk aspects of the NRC project plan activities for digital I&C. They pointed out that currently the NRC and industry use a deterministic approach to ensuring safety, but the December 6, 2006, SRM indicated that progress should be made in deploying risk-informed digital I&C systems. This resulted in the staff identifying several problem statements. The staff stated that existing guidance is not sufficiently clear on how to model digital systems or how risk insights can be used in licensing actions. Also, in the longer term, there needs to be advancement in the state-of-the-art of detailed modeling which could allow risk-informed decision-making. The staff stated that Problem Statement 1 is for issuing interim guidance on use of current methods in modeling for new reactor licensing, and, in the longer term, updating the SRP and Regulatory Guides. Problem Statement 2 is for developing acceptable approaches for using risk insights, both in the short and long terms. They noted that some new reactor designs have already incorporated modeling of digital systems in their risk assessments, but operating plants have not. They presently conclude that use of PRA in evaluating digital systems presents significant challenges, but that risk insights may provide improved identification of vulnerabilities, including assessing D3.

The staff also made a presentation on the research work regarding dynamic reliability modeling. The 1997 NAS study recommended that digital systems should be evaluated by modeling system interactions in addition to hardware and software modeling. Current plant PRAs use the static event-tree/fault-tree approach. In the near term, the staff plans to determine what can be done using the current static methods and develop advanced methods to account for various hardware, software, and process interactions while using the static method. They plan to develop two “benchmark” test cases (i.e., main feedwater controller and reactor protection systems) to help develop criteria, tools, and methods. The current state of reliability modeling methods is provided in NUREG/CR-6901, which discusses the Markov cell-to-cell mapping technique (CCMT) and the dynamic flow graph modeling (DFM) method. The staff also plans to issue a NUREG/CR very soon on the results of the benchmark studies for dynamic modeling. A comparison of the CCMT and DFM outputs was difficult, but showed high level agreement of failure modes. The next steps in evaluating the methods include incorporation of the models in

existing PRAs for selected initiating events.

The staff also presented the research work on traditional methods for evaluating digital systems. There were four different traditional reliability modeling methods evaluated for six design-specific applications. They found that for all six applications there were limitations which included: lack of systematic failure modes and effects evaluations, lack of failure parameter data, and inadequate quantitative software reliability methods. They determined that the event-tree/fault-tree (ET/FT) and Markov methods were the most powerful and flexible traditional methods for modeling. The staff plans to have an external peer review of the criteria for evaluating reliability models and of the selection of the traditional methods chosen.

The staff also made a brief presentation on proposed regulatory guidance for risk-informing digital systems, which will eventually be developed in the longer term and will incorporate the findings from the ongoing research. The staff currently plans that the regulatory guidance be performance-based in nature.

COMMENTS AND OBSERVATIONS FROM THE SUBCOMMITTEE MEMBERS

- Chairman Apostolakis asked if there are efforts to research the work described in various journal articles relating to how digital systems could be demonstrated, such as is being done in some other countries. Mr. Marion and Ms. Keithline responded that EPRI is coordinating with counterparts in other countries on both deterministic and risk-informed approaches and that the insights will be discussed in NEI white papers.
- Member Kress asked and Ms. Keithline clarified that the term “deterministic” refers to applications involving design-basis accidents which use conservatism and specifications. She also clarified that for evaluating D3 for LOCA mitigation, the acceptance criteria is not 10 CFR 50.46, but is 10 CFR 100 limits.
- Chairman Apostolakis asked and Mr. Arndt clarified that the positions in Branch Technical Position (BTP)-19 may change as a result of interactions between NRC and industry in the task group areas.
- Member Maynard asked if the white papers being developed will be based on current technology or on the 1994 NUREG/CR-6303 (on D3) and what is the schedule. Ms. Keithline and Mr. Marion responded that the white papers will be based on current information and the schedule would be developed over the next month or so.
- Chairman Apostolakis asked what type of common-cause failures can occur in digital systems. Mr. Loeser responded that there can be both hardware and software common-cause failures.
- Chairman Apostolakis asked what problems there are related to D3. Mr. Loeser provided an opinion that there are several aspects: the amount of prior use, the likelihood that complex software will have a problem somewhere. Complex hardware may also have problems, but these problems can be revealed by operational experience.

- Chairman Apostolakis noted that there is not a requirement to find potential common-cause failures. Mr. Loeser added that the current requirements are to build high quality systems which are not likely to have failures, and many common-cause failures are not postulated.
- Member Abdel-Khalik asked what is meant by “sufficient quality” non-safety systems which are credited for backup capability. Mr. Loeser responded that such a capability has not been applied in the past, but he believed that systems similar to that used for ATWS prevention in addressing Generic Letter 85-06, may be adequate. Mr. Kemper further responded that such systems will typically have “augmented” quality wherein certain failures are protected against. Member Maynard commented that important-to-safety systems with augmented quality are reviewed on a case-by-case basis.
- Member Abdel-Khalik commented that the NAS report states that there appears to be no generally applicable effective way to evaluate diversity between two pieces of software performing the same function and that there still needs to be a determination that the two sets of software are diverse. Mr. Loeser responded that there are ways to determine diversity between two sets of software if the sets are completely different in origin, including different human designers.
- Chairman Apostolakis asked if the review of a system for diversity should be diverse as well. Mr. Loeser responded that he thought there should be either independent reviews or a peer review process.
- Chairman Apostolakis asked if an error by humans would be considered as a common-cause failure (CCF) of a system and would a reviewer look for such failure modes. Mr. Eagle and Mr. Anrdt responded that this is considered a CCF. Mr. Loeser added that postulation of CCFs does not consider specific causes. He stated also added that quality in design reduces, but does not eliminate, CCFs and that postulation of CCFs involves assuming that the entire system fails, regardless of the cause.
- Member Maynard asked if credit for operator actions considers what need to be done if a digital system fails and the time required. Mr. Eagle responded yes.
- Chairman Apostolakis and Member Kress asked if credit for leakage detection could be used to eliminate postulation of large LOCAs, similar to credit taken for fire events. Mr. Eagle and Mr. Waterman responded that this is being considered as part of the issue of which operator manual actions can be credited.
- Member Abdel-Khalik asked if credited operator manual actions have to be diverse from any computer-based controls and whether the manual control system must not be digital. Mr. Kemper responded that the manual system must be diverse but would not necessarily have to be digital.
- Member Kress asked what a digital system must have in order to be diverse. Mr. Anrdt and Mr. Eagle responded that this is an issue which is being evaluated.
- Chairman Apostolakis commented that, based on information in some technical papers,

simulators are useful in evaluating the performance of digital I&C systems. Mr. Eagle and Mr. Mayfield responded that the schedule for guidance on simulators is being driven by the need to train operators, but that the technical papers would be reviewed.

- Member Abdel-Khalik asked if D3 can be quantified. Chairman Apostolakis commented that this is difficult. Mr. Arndt added that the issue of D3 is being addressed more with qualitative assessments.
- Chairman Apostolakis commented that review of failure data is important for understanding CCFs and how to mitigate them. Mr. Mayfield responded that the staff would consider this and determine if information may be presented to the full Committee in about two weeks at the May ACRS meeting.
- Member Maynard commented that there may be a negative effect of too much D3, since more complex systems may be less reliable.
- Member Kress asked if the total number of digital systems is known such that failure rates could be determined from numbers of failures. Mr. Waterman responded that this was not yet determined.
- Chairman Apostolakis asked if a past “datastorm” event (too much data received too quickly) resulted in a common-cause failure. Mr. Waterman responded that it did.
- Member Abdel-Khalik asked if a comparison has been made of failure rates for analog vs. digital systems. Mr. Waterman responded that this has not yet been determined.
- Member Maynard asked if it has been determined whether there is a need for more D3 or less. Mr. Waterman and Mr. Kemper responded that the staff is not ready to do that yet, until more interaction with industry and research is complete.
- Chairman Apostolakis, Member Kress, and Member Maynard all asked that an overview of all of the six areas of the project plan be provided so that the Committee may adequately respond to the SRM regarding the adequacy of the project plan.
- Mr. Guarro asked if more detail beyond simple block logic has been considered in evaluating necessary D3. Mr. Kemper responded that this will be considered in the long-term only.
- Chairman Apostolakis asked if NEI objected to modeling of digital systems in PRAs. Mr. Marion responded that they did, because it introduces more complexity with little benefit.
- Member Maynard asked how the interim guidance will be used by industry since they are required to use requirements in effect six months prior to a COL application. Mr. Douthett and Mr. Arndt responded that the interim guidance is intended to only clarify the existing SRP and Regulatory Guidance in effect.
- Chairman Apostolakis commented that it is common that corrective actions are applied to problems which actually occur in I&C systems, but that a small failure rate may be

tolerated with no corrective actions.

- Chairman Apostolakis asked if the answers to key questions will be available in about a year regarding the appropriate way to design digital systems. Mr. Arndt responded that the staff intends this to be a short-term activity.
- Consultant Sergio Guarro commented that a risk-informed approach to design of software is to evaluate the level of testing necessary, based on how often a particular function is required. Mr. Arndt added that this is consistent with approaches in other industries.
- Chairman Apostolakis commented that functional classification and use of fault trees is important for digital systems which only actuate components, such that failures become time-independent.
- Chairman Apostolakis commented that there ought to be a systems-centered approach to solving digital I&C issues.
- Chairman Apostolakis asked if the requirement in RG 1.174 to have defense-in-depth diminished the effect of having a PRA model. Mr. Douth responded that it is necessary to consider this and not require too much as a result of improving guidance.
- In response to Chairman Apostolakis, Mr. Arndt stated that priorities and timelines for resolving issues are being proposed by industry.
- Chairman Apostolakis commented that in dynamic PRA modeling of systems, nuclear control systems are not as complex as in some other applications. He also asked to be provided the resolution to the 180 comments on the dynamic modeling discussed in NUREG-6901.
- Chairman Apostolakis asked about simulators to model dynamic digital system problems. Mr. Arndt responded that a simulator software would have to be linked with a PRA model, but Member Maynard cautioned that the capability of simulators may be limited in this regard.
- Chairman Apostolakis commented that making simplifications to only model key parts of systems will make the process more practical, but it does not demonstrate the need to perform dynamic modeling.
- Chairman Apostolakis asked how many states there are in a typical digital system. Mr. Aldemir responded that there are approximately 100 million, which makes it impractical to model unless the system model combines components into groups. This reduces the number of states to about 2200.
- Chairman Apostolakis commented that if some examples could be found where dynamic modeling identified problems which traditional PRA did not find, this could be an argument for performing dynamic modeling. Dr. Aldemir and Mr. Arndt responded that this is a subjective comparison, but that they would find an example which had been

discussed at an earlier meeting. Chairman Apostolakis added that this could counter an argument that a good non-PRA evaluation could have found similar problems. Mr. Arndt and Dr. Aldemir added that they had also made a comparison of traditional methods with the dynamic flow graph model method and that a report would be available soon.

- Chairman Apostolakis commented that it is important to review operating experience to examine system failures and their source.
- Chairman Apostolakis asked why Markov modeling is used in the traditional method of modeling. Mr. Kuritzky responded that it is used differently than for the dynamic modeling in that it only characterizes the failure probability and does not model complex interactions within the system or with the plant processes.
- Member Abdel-Khalik asked how much the familiarity of the staff with the event tree and fault tree modeling contributed to how well it appeared to perform the modeling. Mr. Kuritzky responded that there could be some bias, but that they tried to be impartial.
- Consultant Sergio Guarro commented that it may not be proper to model hardware, software, and process functions in the same way, which could result in incorrect results.
- Member Abdel-Khalik asked whether an analyst who is familiar with dynamic method modeling could better perform traditional modeling. Mr. Kuritzky responded that he would expect so.
- Mr. Jeff Stone with Constellation interjected a question to Mr. Arndt regarding what is a success path for software modeling. Mr. Arndt responded that for both the dynamic and traditional modeling efforts, software modeling would be included.
- Member Abdel-Khalik commented that based on his interpretation of the NAS report, analog backup systems would be required, because the report concludes that there is no generally applicable effective way to evaluate diversity between two pieces of software performing the same function.
- Member Kress commented that he feels that diversity could be defined to include non-analog backup systems. He also indicated that it would be very difficult to determine the risk implications of various types of diversity. He also doubted if research efforts would do so in the near future, but thought that the proposed research would provide good information. He thought expert judgement and opinion would be necessary to determine needed system attributes to provide necessary levels of safety in a deterministic way.
- Member Maynard commented that analog backup systems may not be necessary. He commented that making systems more complex may make them less safe. He expressed concern that the schedule for resolving issues needs to support future reactor licensing. He did not believe fully digital systems would result in significant changes in risk. He also thought that the use of simulators for dynamic modeling studies would be limited for this purpose.
- Consultant Sergio Guarro commented that if a logic design specification of an analog

backup system is similar to the primary digital system specification, it could have the same failure as the primary system failure, which may result in a lack of diversity. He also commented that there are systems which may not be easily defined as either digital or analog.

- Chairman Apostolakis commented that he would encourage the use of operating experience data and that a collaborative use of the Halden facility simulator may provide useful information.
- Mr. Robert Enzinna with AREVA provided comments regarding application and operating system software reliability. He thought software reliability issues could be improved by researching attributes which could specifically affect backup systems. He also thought that it may not be important to quantify reliability, but that conservative estimates of reliability of the systems he was familiar with, would be high.

SUBCOMMITTEE DECISIONS AND ACTIONS

Following the staff and industry presentations and discussions, Chairman Apostolakis thanked everyone for their contributions and then adjourned the meeting at 4:29 pm.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE PRIOR TO THIS MEETING

1. Memorandum from C.G. Hammer to ACRS Members transmitting status report, proposed schedule, and review materials regarding digital instrumentation and control systems issues, dated April 2, 2007 (ADAMS ML070940344)
2. Minutes of June 27, 2006, meeting of ACRS Subcommittee on Digital I&C Systems (ADAMS ML062630374)
3. Letter from ACRS Chairman Graham B. Wallis to NRC Chairman Nils J. Diaz, transmitting a report entitled, "Review and Evaluation of the NRC Safety Research Program", dated March 15, 2006 (ADAMS ML060810118)
4. Letter from A.L. Vietti-Cook, Secretary NRC to John T. Larkins, Executive Director ACRS, "Staff Requirements - Meeting with ACRS, October 20, 2006...", dated November 8, 2006 (ADAMS ML063120582)
5. Letter from A.L. Vietti-Cook, Secretary NRC to Luis A. Reyes, Executive Director for Operations, "Staff Requirements - Briefing on Digital I&C, November 8, 2006...", dated December 6, 2006 (ADAMS ML063400033)
6. U.S. National Research Council, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, National Academy Press, Washington, DC, 1997
7. Branch Technical Position (BTP) 7-19 - Revision 5, modified February 15, 2007 (ADAMS ML070380094)
8. NUREG/CR-6303 - Method for Performing D3 Analyses of Reactor Protection System, December 1994 (ADAMS 9501180332)
9. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary, and Advanced Light-Water Reactor Designs", Section Q - Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems, dated April 2, 1993 (ADAMS 9304130158)

10. SRM on SECY-93-087, Section 18. II.Q, dated July 21, 1993 (ADAMS 9308270107)
11. Letter from James H. Riley, NEI, to Allen Howe, NRC, dated February 9, 2007, transmitting comments on BTP 7-19, Revision 5 (ADAMS ML070400597 and ML070400598)

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/subcommittee/2006/> or purchase from Neal R. Gross and Co., Inc., (Court Reporters and Transcribers) 1323 Rhode Island Avenue, NW, Washington, DC 20005 (202) 234-4433.