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

September 30, 2008

MEMORANDUM TO: ACRS Members

FROM: Christina Antonescu, Senior Staff Engineer**/RA/**
Reactor Safety Branch B, ACRS

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, APRIL 17, 2008—ROCKVILLE, MD

The minutes of the subject meeting were certified on September 16, 2008, as the official record of the proceedings of that meeting. A copy of the certified minutes is attached.

Attachment: As stated

cc w/o att.: E. Hackett
A. Dias
C. Santos
S. Duraiswamy

cc: w/att.: J. Delgado
N. Mitchell-Funderburk

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

September 30, 2008

MEMORANDUM TO: Christina Antonescu, Senior Staff Engineer
Reactor Safety Branch B, ACRS

FROM: George E. Apostolakis, Chairman
Digital I & C System Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, APRIL 17, 2008—ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting, dated April 17, 2008, are an accurate record of the proceedings for that meeting.

/RA/
George E. Apostolaskis, Subcommittee Chairman

9/30/2008
Date

Certified by: George E. Apostolakis Issued: 9/16/2008
Certified: 09/30 /2008

MEETING MINUTES
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
APRIL 17, 2008—ROCKVILLE, MD

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on April 17, 2008, at the headquarters of the U.S. Nuclear Regulatory Commission (NRC) in the Commission Hearing Room, 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. Mr. Girija Shukla was the designated Federal official for this meeting. The subcommittee received no written requests from the public for time to make oral statements. The subcommittee chairman convened the meeting at 8:30 a.m. on April 17, 2008, and adjourned at 3:30 p.m.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman	J. Sieber, Member
D. Bley, Member	M. Bonaca, Member
M. S. Guarro, Consultant	

ACRS Staff
G. Shukla, Designated Federal Official
C. Antonescu, Cognizant Staff Engineer

Principal NRC Speakers and Consultants

A. Kuritzky, RES	G. Martinez-Guridi, NRR	T.Chu, BNL
M. Cheok, RES	R. Sydnor, RES	

Principal Industry Speakers
None

Other members of the public attended this meeting. A complete list of attendees is available from the ACRS 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 (DI&C), convened the meeting at 8:30 a.m. Chairman Apostolakis stated that the purpose of this meeting was to discuss NRC staff and industry activities for digital I&C systems. Specifically, the subcommittee discussed the progress associated with the research in digital risk assessment methods and heard presentations from the NRC staff and its contractor from Brookhaven National Laboratory on a NUREG report entitled "Approaches for Using Traditional PRA Methods for Digital Systems."

DISCUSSION OF AGENDA ITEMS

NRC Staff Activities Regarding Digital Instrumentation and Control Systems

Presentation on Research on Traditional Probabilistic Risk Assessment (PRA) Methods for Digital Systems

Alan Kuritzky from the Division of Risk Assessment Risk Analysis in the Office of Research discussed the research the staff is doing on the use of traditional PRA methods for modeling digital systems. G. Martinez-Guridi and Louis Chu who accompanied Alan Kuritzky are employees from Brookhaven National Laboratory, the contractor for the Office of Research (RES).

The last talk the RES staff had with the subcommittee on this topic was in April of 2007. At that time, the project was early in its work and the staff was able to discuss only some of the initial activities. The staff came to this meeting to discuss what it has accomplished since April 2007. Additionally, the staff discussed the draft NUREG/CR that it released for review and public comment, and will soon publish as final. The two contractors gave detailed presentations on some of the technical topics.

The staff talked about the objective of the project and the tasks necessary to accomplish the work. The staff also discussed the status of the work in progress. After releasing the NUREG/CR for comment, the staff began performing the next task of the project, applying traditional methods to the benchmark system, which is a digital feed water control system.

The staff cited some preliminary results and insights from the work and the staff discussed the remaining steps of the project.

The objective of this work is to determine the existing capabilities and limitations of traditional methods for modeling digital systems. By using traditional reliability modeling methods, the staff determined that these methods were well-established methods that do not explicitly account for the interactions between the modeling plant system and the plant physical processes. The staff refers to those types of methods that do explicitly account for those interactions, as dynamic methods. The ultimate goal of this work is to try and develop risk-informed decision-making guidance that can be used for digital systems and applications to nuclear power plants, as well as to try and come up with guidance for inputting digital system models into plant PRAs.

The tasks involved in this project, involved developing some draft criteria for what the staff feels should be in a digital system model. The staff and subcommittee discussed the criteria in April 2007. The staff received further feedback from the subcommittee on the draft criteria and has since updated those criteria. Those criteria could eventually support any type of regulatory

guidance that is put out on digital system models or provide the technical basis for doing risk evaluations for either current or new reactors.

The two methods that were selected were the event tree/fault tree method and the Markov method. The idea was that this project scope does not involve major advancements in state-of-the-art technology. What are the capabilities and limitations that exist right now in these traditional methods?

Thus, the staff was not looking towards state-of-the-art advancement. Also, the staff was not looking to further work in areas that were not already well-established. An example is software reliability quantification. Once the staff completes those models for the example systems or what the staff calls benchmark systems, the staff would then compare the results of those models to the criteria that were developed in the first step to see where there may be areas that further research can improve the models.

The last step of this work is to take those models and see how the staff could put them into a PRA. One of the ultimate goals of this work is to get guidance on how to include digital system reliability models in the PRA. On the event tree/fault tree (ET/FT) method, the staff would expect that to be relatively straightforward. For the Markov method it would require a little more creativity to get them integrated to the PRA.

The objective of traditional method research is to determine the existing capabilities and limitations of using traditional reliability modeling methods to develop and quantify digital system reliability models. Also, the goal is to support the development of regulatory guidance for assessing risk evaluations involving digital systems and including digital system models into nuclear power plant probabilistic risk assessments (PRAs).

The NUREG report will do the following:

- Develop of a list of desirable characteristics for reliability models of digital systems.
- Document the process for using the event tree/fault tree (ET/FT) and Markov methods to develop and quantify a reliability model for a digital feed water control system (DFWCS) that is first of two benchmark studies.
- Identify preliminary areas where limitations exist in the state-of-the-art using traditional PRA methods and where additional research and development are needed.
- No detailed analysis and quantification of software reliability

The application of ET/FT and Markov methods to the DFWCS is almost complete.

As part of the list of desirable characteristics for reliability models of digital systems, characteristics were identified and grouped into nine broad categories covering the probabilistic model of a digital system and its documentation. The characteristics are based on knowledge and experience in PRA and analyzing digital systems, and on a literature review of digital systems. Also, the characteristics were revised as the result of an external review panel meeting. In addition, as part of the review of the draft NUREG/CR, the revised characteristics were further reviewed by the NRC user offices, a set of external reviewers, and the public. The characteristics provided input to Interim staff guidance on review of digital system models in new reactor PRAs, and the planning of a Nuclear Energy Agency meeting on digital system reliability to be held later this year.

In the process for using ET/FT and Markov Methods for first benchmark study, the DFWCS was analyzed in detail, including its function, digital features, components, dependencies and interfaces in order to gain a full understanding of the way the DFWCS and each of its relevant

components operate. A failure modes and effects analysis (FMEA) was performed to determine the failure modes of the DFWCS components and the impact of each failure mode on system function. The relevant failure modes of the components and their impacts on the DFWCS helped develop preliminary approaches for constructing and quantifying probabilistic models using the traditional ET/FT and Markov methods and parameters needed for quantifying the probabilistic models. Each method investigated each digital component failure mode. Quantitative software reliability and human reliability analysis are beyond the current project scope.

The capabilities of traditional ET/FT and Markov methods are well-established-methods that are well understood by the reliability community. In general the methods are powerful and are capable of modeling many features of digital systems and capturing many important dependencies of these systems. Also, they must be supported by good engineering analyses, such as identifying failure modes and effects of digital components, and probabilistic data. In particular, ET/FT models can be easily integrated with an existing PRA. The Markov method is capable of explicitly treating some time dependencies and ordering of failures.

The limitations of traditional ET/FT and Markov methods are that these methods do not explicitly account for the interactions between a plant system and the plant's physical processes (i.e., the values of the process variables), nor the timing of these interactions. The ET/FT method does not account for the order in which component failures occur, and the Markov method is vulnerable to "state explosion."

Preliminary areas of additional research based on the current NUREG/CR include:

- identifying the failure modes of the components of a digital system
- determining the effects of a single failure mode or of combinations of failure modes on the system
- the failure parameter database
- a quantitative software reliability model
- the treatment of uncertainties
- a human reliability analysis associated with digital systems and human-system interfaces

The preliminary insights from the first benchmark study is that for the level of detail necessary to capture digital system design features that could affect system reliability, the models may be so complex that it may not be practical to use either the traditional fault tree or Markov methods to identify the component failure mode combinations that lead to system failure. Specifically, a simulation tool is needed to identify the system failure effects of combinations of component failure modes. The output of the simulation tool is the set of the combinations of component failure modes that fail the system. It was found that the order in which failures occur makes a difference. The DFWCS in the benchmark study has a few hundred single failures, tens of thousands of double failures, and few million triple failures, and the process of using the simulation tool is expected to be applicable to any complex system, though it is desirable to further simplify the process used.

<u>ACRS Digital I&C Subcommittee specific recommendations (programmatic) during the meeting:</u>

- The staff should explore the fundamental philosophical aspects of software failures and their use in developing a probabilistic model of a digital system.

- The staff should consider the relevant aspects of developing and evaluating a reliability model of a digital system that integrates hardware and software failures, based on the outcome of the work under item 1 above.
- The staff should take into account that software failures can have an important contribution to the unreliability of a digital system. The work presented in the former Appendix C of NUREG/CR-6962 (now removed from this report) was a good first step in discussing the characteristics of this kind of failure, and should be taken into account in addressing items 1 and 2 above.
- The staff should explore the possibility of combining elements of the BNL work with elements of other methods, such as DFM, to better address the issues associated with developing digital system reliability models.
- BNL's task on integrating the digital system reliability models into the PRA of a nuclear power plant should be delayed until the work mentioned in items 1 and 2 above are completed.

ACRS Digital I&C Subcommittee specific recommendations on NUREG/CR-6962 during the meeting:

- The work on failure modes and their effects and on developing and providing the theoretical basis for evaluating a traditional probabilistic model is valuable and should constitute the main content of the report.
- Because some of the criteria in Section 2 address issues for which current methods may not be available and others are somewhat vague, the staff should revisit these criteria.
- Due to the poor quality of the data available, it is not meaningful to quantitatively evaluate a probabilistic model. Hence, the NUREG/CR-6962 report should discuss the approaches for quantifying the model, but it should not suggest that a meaningful quantification can be carried out at this time.
- The fact that the report does not address software failures should be made very clear at the beginning of the report.

Staff Response to the Subcommittee specific recommendations (programmatic) and undertakings:

- Review draft former Appendix C of draft NUREG/CR-6962 and other various methods to assess software failures.
- Obtain additional non-nuclear data sources to evaluate additional insights on software failures.
- Conduct internal discussions on the fundamental aspects of software failure modeling
- Factor results of above efforts, and other Subcommittee programmatic recommendations, into the development of the new 5-year digital I&C research plan.
- Delay BNL's task on integrating the digital system reliability models into the PRA of a nuclear power plant.

Staff Response to the Subcommittee specific recommendations on NUREG/CR-6962:

- The work on failure modes and their effects constitutes a significant portion of the report.
- The development and provision of the theoretical basis for evaluating software failures probabilistically is out of the scope of the current project.
- The evaluation criteria in Section 2 have been revisited, and the principal change involves re-naming them as "desirable characteristics of digital system reliability

models."
- The report discusses the approaches for quantifying the DFWCS model, but heavily caveats the data used, and specifies that the model is only being quantified to demonstrate the potential uses of the methods and models.
- The fact that the report does not address software failures is made clearer at the beginning of the report.

The staff's next steps for the project is to complete the application of the two traditional methods to the DFWCS by gaining insights into reliability modeling of digital systems, and the major contributors to the failure of the system. The staff must also determine the capabilities and limitations of the methods, and compare the results and insights with those from the parallel studies of the DFWCS using dynamic methods. In addition, prepare a draft NUREG/CR by July 2008. The final step is to apply the two traditional methods to a RPS because the design requirements of safety-related systems are different from those of non-safety-related systems and modeling a protection system may be significantly different.

SUBCOMMITTEE DECISIONS AND ACTIONS

Overall, the Digital I&C Subcommittee made the following conclusions:

- Draft NUREG/CR-6962 does not provide evidence that traditional probabilistic risk assessment (PRA) methods are enough to identify DI&C failure modes.

- Final publication of NUREG/CR-6962 should state that its methods do not address software failures and that it employs simulation in addition to traditional PRA methods.

- The distinction between traditional and nontraditional methods of modeling should be abandoned because it is artificial. The staff should establish an integrated program to include failure mode identification of DI&C systems by including insights gained from investigations on traditional methods and on advance simulation methods.

- Since the software reliability quantification is not within the existing capabilities, it should be pursued in the future when a good understanding of the failure models is obtained.

The committee also stated that the staff decided to remove Appendix C on modeling of software failure. These ideas on how DI&C systems fail should be explored and included in the recommended integrated program. In addition, the committee recommended that investigation of an actuation system should be part of the integrated program.

Based on the Digital I&C Subcommittee recommendations, the staff agrees overall:

The final version of NUREG/CR–6962 should state that a failure modes and effects analysis (FMEA) is insufficient to determine how specific component-level failure modes affect DI&C systems. More sophisticated tools (e.g., simulation tools) should be used to study and analyze the interaction between components of a DI&C and the effects of one or more failures.

At this time, no attempt will be made to quantify probabilistic models of digital systems with publicly available hardware failure data, since it is insufficient for this purpose. Due to the poor quality of the data available, it is not meaningful to quantitatively evaluate a probabilistic model. Therefore, the NUREG/CR-6962 report will discuss the approaches for quantifying the model, but it should not suggest that a meaningful quantification can be carried out at this time. Also, the final version will focus on failure identification, but not software quantification. The quantification will be performed as part of benchmark studies in the integrated program.

The staff will also consider the insights gained from the investigations of both traditional and dynamic methods, as well as the other ACRS recommendations in their updated DI&C Plan.

In addition, the staff agrees that the final version of NUREG/CR-6962 will not provide the failure parameters used in the study. The staff emphasizes that, due to limitations in publicly available failure parameters of DI&C components, the data developed in the study will be used for reliability methods only and not for quantifying models.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE

1. Draft NUREG/CR "Approaches for Using Traditional PRA Methods for Digital System" including the following:

   – Appendix A, "Summary Report of the External Review Panel Meeting on Reliability Modeling of Digital Systems (May 23–24, 2007)"

   – Appendix B, "Detailed FMEA of the DFWCS at Different Levels"

   – Appendix C, "Modeling of Software Failures"

   – Appendix D, "Other Methods for Modeling Digital Systems"