EDO Principal Correspondence Control

FROM: DUE: 06/30/08   EDO CONTROL: G20080377
                                                        DOC DT: 05/19/08
                                                     FINAL REPLY:
William J. Shack, ACRS

TO:

    Chairman Klein

FOR SIGNATURE OF :   ** GRN **   CRC NO: 08-0311

    Borchardt, EDO

DESC: ROUTING:

    Draft NUREG/CR-6962, "Approaches for Using   Borchardt
    Traditional Probabilistic Risk Assessment Methods Virgilio
    for Digital Systems," and Related Matters   Mallett
    (EDATS: SECY-2008-0327)   Ash
                                                        Ordaz
                                                        Cyr/Burns
DATE: 05/29/08   Leeds, NRR
                                                        Johnson, NRO
ASSIGNED TO: CONTACT: McKirgan, OEDO
                                                        ACRS File
        RES   Sheron

SPECIAL INSTRUCTIONS OR REMARKS:

    Prepare response to ACRS for the signature of the
    EDO. Add the Commission and SECY as cc's. USE
    SUBJECT LINE IN RESPONSE.

Electronic Document and Action Tracking System

EDATS Number: SECY-2008-0327   **Source:** SECY

General Information

Assigned To: RES   **OEDO Due Date:** 6/30/2008 5:00 PM

Other Assignees: **SECY Due Date:** NONE

Subject: Draft NUREG/CR-6962, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," and Related Matters

Description:

CC Routing: NRR; NRO

ADAMS Accession Numbers - **Incoming:** NONE   **Response/Package:** NONE

Other Information

Cross Reference Number: G20080377, LTR-08-0311   **Staff Initiated:** NO

Related Task: **Recurring Item:** NO

File Routing: ACRS   **Agency Lesson Learned:** NO

       Roadmap Item: NO

Process Information

Action Type: Letter   **Priority:** Medium

       Sensitivity: None

Signature Level: EDO   **Urgency:** NO

OEDO Concurrence: NO

OCM Concurrence: NO

OCA Concurrence: NO

Special Instructions: Prepare response to ACRS for the signature of the EDO. Add the Commission and SECY as cc's. USE SUBJECT LINE IN RESPONSE.

Document Information

Originator Name: William J. Shack   **Date of Incoming:** 5/19/2008

Originating Organization: ACRS   **Document Received by SECY Date:** 5/29/2008

Addressee: Chairman Klein   **Date Response Requested by Originator:** NONE

Incoming Task Received: Letter

PAPER NUMBER:	LTR-08-0311	**LOGGING DATE:**	05/28/2008
ACTION OFFICE:	EDO		

AUTHOR: William Shack

AFFILIATION: ACRS

ADDRESSEE: Dale Klein

SUBJECT: Draft NUREG/CR-6962, approaches for using traditional probabilistic risk assessment methods for digital systems and related matters

ACTION: Appropriate

DISTRIBUTION: RF

LETTER DATE: 05/19/2008

ACKNOWLEDGED No

SPECIAL HANDLING:

NOTES:

FILE LOCATION: ADAMS

DATE DUE: **DATE SIGNED:**

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

May 19, 2008

The Honorable Dale E. Klein
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT NUREG/CR-6962, "APPROACHES FOR USING TRADITIONAL
PROBABILISTIC RISK ASSESSMENT METHODS FOR DIGITAL SYSTEMS,"
AND RELATED MATTERS

Dear Chairman Klein:

During the 552nd meeting of the Advisory Committee on Reactor Safeguards, May 8-9, 2008, we
reviewed the draft NUREG/CR-6962, "Approaches for Using Traditional Probabilistic Risk
Assessment Methods for Digital Systems." Our Digital Instrumentation and Control (DI&C)
Systems Subcommittee also reviewed this matter during a meeting on April 17, 2008. During
these reviews, we had the benefit of discussions with representatives of the NRC staff and its
contractor Brookhaven National Laboratory. We also had the benefit of the documents
referenced.

Conclusions and Recommendations

1. Draft NUREG/CR-6962 provides convincing evidence that "traditional" probabilistic risk
   assessment (PRA) methods are not sufficient to adequately identify failure modes of
   DI&C systems.

2. Before publication of NUREG/CR-6962, it should be revised to state clearly that its
   methods do not address software failures and that it employs simulation in addition to
   traditional PRA methods. The revised NUREG/CR report should focus on failure mode
   identification only.

3. The distinction between traditional and non-traditional methods of modeling and analysis
   is artificial and should be abandoned. The staff should establish an integrated program
   that focuses on failure mode identification of DI&C systems and takes advantage of the
   insights gained from the investigations on traditional PRA methods and on advanced
   simulation methods.

4. The quantification of the reliability of DI&C systems should be given a low priority until a
   good understanding of the failure modes is developed.

(

Discussion

The current NRC research plan on DI&C follows a two-pronged approach in the DI&C reliability and PRA areas, namely, one effort focused on "traditional" methods and the other on "advanced" methods. The former refers to the event tree/fault tree PRA methods and includes Markov models. The latter refers to simulation-based methods. Draft NUREG/CR-6962 is a product of the study on traditional methods.

The stated purpose of this study is to determine whether traditional PRA methods are sufficient to develop and quantify reliability models for DI&C systems. A major limitation is the fact that it deals only with the hardware components of the DI&C system and ignores potential failures of the software. This severe limitation should be stated explicitly at the beginning of the report. During our previous meetings, we have commented on the significance of errors in software logic design and specification requirements, and the role they have played in digital software failures recorded in other industries.

This study has demonstrated that, even with the exclusion of software failures, traditional PRA methods are not sufficient for the identification of the failure modes of a DI&C system. In order to determine the impact of specific failure modes of the hardware parts on the system, the investigators had to employ a dynamic simulation analysis of the DI&C system including its software. This is a computationally intensive combinatorial approach that can involve millions of fault sequences.

The draft NUREG/CR report contains a discussion on the development of reliability models for DI&C systems and the collection of data for parameter estimation. It is premature to attempt to develop such models when our understanding of the failure modes of DI&C systems is still evolving. We also have serious concerns about the usefulness of the failure rate data sources cited. The sections dealing with probabilities should be drastically reduced or deleted altogether.

This study, as well as the work on simulation methods that we reviewed in the past, leads us to conclude that, as a community, we have a poor understanding of the potential failure modes of DI&C systems, and that attempting to develop reliability models is premature.

The staff should establish an integrated program that focuses on failure mode identification of DI&C systems. The distinction between traditional and non-traditional methods of modeling and analysis should be abandoned, since this distinction is at best artificial and, in practice, it may even be counterproductive. The important question that should be answered is:

> What methods and tools are effective in identifying DI&C system software-related and hardware-related failure modes including their important mutual interactions and their response to changes in process variables?

Draft NUREG/CR-6962 provides valuable information on a digital feed-water control system (DFWCS). This system has also been investigated in the NRC research project, "Dynamic Risk Modeling" that employs "advanced" methods. It can, therefore, be used as a benchmark study in the integrated program. The traditional-methods project plans to investigate a second system, the reactor protection system (RPS). The investigation of an actuation system should also be part of the integrated program.

The draft NUREG/CR-6962 contains an appendix (Appendix C) that has some useful ideas on how DI&C systems fail. These ideas should be explored in the recommended integrated program. We have been told by the staff that Appendix C will not be included in the final NUREG/CR report.

We look forward to interacting with the staff on these important matters.

Sincerely,

/RA/

William J. Shack
Chairman

References

1.   Draft NUREG/CR, "Approaches for Using Traditional PRA Methods for Digital Systems," with the following attachments, February, 28, 2008:

- 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"

2.   T. Aldemir, M. P. Stovsky, J. Kirschenbaum, D. Mandelli, P. Bucci, L. A. Mangan, D. W. Miller, X. Sun, E. Ekici, S. Guarro, M. Yau, B. Johnson, C. Elks, and S. A. Arndt, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments," NUREG/CR-6942, The Ohio State University, ASCA, Inc., University of Virginia, and U.S. NRC, October 2007.