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

March 12, 2008

MEMORANDUM TO: ACRS Members

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

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, SEPTEMBER 13, 2007—ROCKVILLE, MARYLAND

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

Attachment:
As stated

cc: F. Gillespie
S. Duraiswamy
C. Santos
G. Shukla

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

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

FROM: George E. Apostolakis, Chairman **/RA/**
Digital Instrumentation and Control
Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, SEPTEMBER 13, 2007—ROCKVILLE, MARYLAND

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

/RA/
George E. Apostolakis, Subcommittee Chairman

March 7, 2008
Date

Certified by: G. Apostolakis Issued: 3/12/2008
Certified on: 3/07/2008

MEETING MINUTES
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
SEPTEMBER 13, 2007—ROCKVILLE, MARYLAND

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on September 13, 2007, at the headquarters of the U.S. Nuclear Regulatory Commission (NRC) 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. Mr. Girija Shukla 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 September 13, 2007, and adjourned at 3:30 p.m.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman	S. Abdel-Khalik, Member
M. Bonaca, Member	O. Maynard, Member
S. Guarro, Consultant	

ACRS Staff
G. Shukla, Designated Federal Official

Principal NRC Speakers and Consultants

M. Waterman, RES	P. Rebstock, RES	R. Sydnor, RES	C. Doutt, NRR
J. Grobe, NRR	W. Kemper, NRR	B. Solsa, NRR	S. Arndt, RES
J. Persensky, RES	P. Loeser, NRR	M. Gareri, NSIR	I. Jung, NRR
M. Boggi, RES	B. Sosa, NRR		

Principal Industry Speakers

K. Keithline, NEI	R. Miller, GE	W. Bowers, Exelon

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 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), Office of Nuclear Reactor Regulation (NRR), and 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 ACRS. The rules for participation in the meeting appeared as part of the notice of the meeting published in the *Federal Register* on August 29, 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 Instrumentation and Control Systems

Presentation on Digital Instrumentation and Control Task Working Groups

Ms. Belkys Sosa, NRR, made a brief presentation on the status of Digital I&C Steering Committee activities. In particular, she discussed the staff's efforts related to digital I&C and the development of four ISG documents in the areas of (1) HICR communications, (2) diversity and defense in depth, (3) human factors, and (4) cybersecurity.

The presentation also included discussions regarding the purpose of "interim" guidance to provide clarity on upcoming upgrades for digital I&C and how that relates to the combined license (COL) applications or the signed certifications that the NRC is expecting. The short-term objective for the ISGs is to identify technical and regulatory issues for which guidance can be developed in time to support the review of new application licenses. The long-term objective is to develop recommendations that will be used to update the regulatory guides (RGs), Standard Review Plan (SRP), NUREG-0800 and other relevant regulatory documents. In addition, the Project Plan for Digital Instrumentation and Control includes a process for developing interim guidance to support the review of a number of COL applications that are anticipated to come in fall 2007, as well as design certification activities for new reactors.

The overall goal for the activities of the Digital I&C Steering Committee is to further refine the ISGs and incorporate that guidance into the NRC's existing regulatory framework, such as the SRP and existing and new RGs. In addition, the Digital I&C Steering Committee will continue to coordinate and interact with stakeholders in the industry to refine and enhance the ISGs by the end of September, 2007.

Ms. Sosa pointed out that in August 2007, the Digital I&C Steering Committee established a new TWG to deal with regulatory issues for fuel cycle facilities and is planning to engage with the Advisory Committee on Nuclear Waste.

Ms. Sosa summarized that the steering committee has functioned effectively, that the project

plan is in place, and that the committee plans to continue to work with stakeholders in the industry through public working group meetings. The staff is on schedule to complete the ISGs by end of September in accordance with the near-term objectives of the project plan.

Presentation—Industry Perspective on Digital Instrumentation and Control Issues

Representatives from NEI also made a presentation, addressing key issues and remaining challenges related to diversity and defense in depth, operating experience, communications, human factors, and cybersecurity. They also provided their thoughts on the four TWGs. NEI feels very encouraged by the creation of the Digital I&C Steering Committee, TWG efforts to resolve issues, and the progress and interactions with the staff. However, Ms. Kimberly Keithline presented four areas in which NEI feels that more work is needed:

(1) TWG 4, "Highly Integrated Control Room Communications," has defined a problem with an annex to Institute of Electrical and Electronics Engineers (IEEE) Std 7.4.3.2 relating to guidance on communications independence that was not endorsed in RG 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," issued January 2006, because of insufficient guidance in the annex. TWG 4 has been working on additional guidance regarding communications and the maintenance of appropriate levels of independence. In addition, the industry began this activity by submitting a white paper on the subject, followed by many meetings and interactions. The TWG has also been working in parallel with IEEE to incorporate the new guidance into IEEE Std 7.4.3.2 so that RG 1.152 would endorse the latest guidance the next time the NRC revises the RG.

(2) TWG 2, "Diversity and Defense in Depth," initially identified the following eight problem statements related to diversity and defense in depth:

- What constitutes adequate diversity?
- How can operator action be used as a defensive measure?
- What are acceptable assumptions for operator response time?
- When are independent displays and controls needed?
- Is component-level actuation possible?
- What effects need to be considered for common-cause failures?
- Are there design attributes that are sufficient to eliminate consideration of common-cause failures?
- Do the four echelons of defense always need to be diverse from each other?

The group also requested additional clarification regarding the acceptance criteria for addressing common-cause failures versus a single failure.

Ms. Keithline also addressed the critical issue regarding the criterion of 30 minutes for determining whether an automatic diverse actuation function is necessary. The ISG states that it is difficult to demonstrate the feasibility and reliability of manual actions within 30 minutes. Therefore, when manual action is required in less than 30 minutes, the ISG identifies the installation of an independent and diverse automated backup system as an acceptable approach. Otherwise, when manual action is not required within 30 minutes, the ISG identifies that manual actions are acceptable.

The industry feels it needs a process to determine, on a case-by-case basis, whether an automated backup system should be installed or manual actions could be credited. Chairman Apostolakis pointed out that NUREG-1852, "Demonstrating the Feasability and Reliability of Operator Manual Actions in Response to Fire," issued October 2007, defines a similar process.

Chairman Apostolakis also noted that, although in principle he agrees with the industry's point of view, the subcommittee recognizes the value of the staff's 30-minute criterion. Therefore, the staff planned to add a sentence to the ISG stating that the methods described in the ISG are not the only methods that the staff may find acceptable; other methods may also be used that require more in-depth staff review.

The industry also believes that another major challenge remains, relating to the use of risk insights when making diversity and defense-in-depth decisions. The Electric Power Research Institute (EPRI) report serves as starting point. In addition, EPRI is considering a probabilistic risk assessment example from a Westinghouse plant. The operating experience data will also be examined to learn more about the failure modes of these components and systems.

(3) TWG 5, "Human Factors," identified four problems:

- minimum inventory of alarms, controls, and displays
- computer-based procedures
- graded approach to human factors
- safety parameter display

In the short term, the industry (i.e., EPRI) will provide reports on the minimum inventory of alarms, controls, and displays and computer-based procedures, to be endorsed by the NRC, before the new regulatory guidance is developed. The industry did submit a report on minimum inventory in late May 2007.

The longer term activities include developing guidance related to a graded approach and the safety parameter display system.

Chairman Apostolakis recommended that the staff examine past operating experience (e.g., Turkey Point in 1994, Pilgrim in 1997, and Palo Verde 2 in 2005). Ms. Keithline commented that the staff made great efforts by considering more than 300 nuclear power plant digital failures that, upon closer examination, were not digital in nature.

Currently, the TWG is also examining Institute of Nuclear Power Operations (INPO) databases to review the nature of failures and determine how many were common-cause failures.

(4) TWG 1, "Cybersecurity," has discussed methods to resolve differences between cyber security guidance in RG 1.152 and NEI 04-04 by conducting a gap analysis to identify where the two documents overlapped or are inconsistent. The industry made some changes to NEI 04-04 based on the gap analysis. In addition, NEI will revise NEI 04-04 to serve as a licensing document as well as a programmatic document, and the ISG will note any slight differences. In addition, the NRC will develop an RG on cyber security.

Finally, Ms. Keithline mentioned that the real test for the ISGs will be its use in licensee submittals. In addition, the staff should review operating experience data by obtaining failure data from domestic databases (NRC and INPO) as well as international databases through COMPSIS.

Presentation—Highly Integrated Control Room Communications Issues

The staff also made presentations on the development of the ISG related to HICR communications issues. The Task Working Group (TWG) was initially formed in the beginning of 2007 and held its initial meeting in February 2007. The TWG comprises NRC members from RES, NRR, NRO, and the Office of Nuclear Material Safety and Safeguards (NMSS). In addition, members of the industry and NEI are participating in the TWG meetings to comment on the interim staff guidance (ISG) documents. The staff has conducted 10 public meetings since the inception of the TWG. The objective is to understand the industry needs in terms of clarifying licensing criteria and applicable communications criteria in operating and new plants; gain new insights into communication issues, independence strategies, and HICRs; and ensure that the ISGs address appropriate design issues.

Chairman Apostolakis asked for a definition of a highly integrated control. The staff responded that this term referred to flat panel displays and computer panels. The staff also suggested that the subcommittee visit both the Westinghouse AP1000 HICR in Pittsburgh, PA (which will provide the design for a simulator), and the General Electric (GE) economic simplified boiling-water reactor (ESBWR).

Mr. R. Miller, GE, described the ESBWR and noted that it is designed to have touch-screen design control. Its four divisions of safety, visual display units are used for control and monitoring for each division, that could include flat panel to ceramic tiles. In response to a question from Dr. M. Bonaca, ACRS, Mr. Miller noted that similarities exist between different designers on current designs with the flat panel displays or video display units.

The staff outlined the HICR communications issues and noted industry concerns that NRC guidance does not define in sufficient level of detail the requirements for interdivisional communications independence. For example, the agency has not provided sufficient guidance on interdivisional communications independence as discussed in IEEE Std 7.4.3.2. RG 1.152 does not provide explicit guidance regarding interdivisional communications independence within digital systems. In addition, Title 10 of the *Code of Federal Regulations* (10 CFR) Section

50.55a(h), “Protection and Safety Systems,” which incorporates IEEE Std 603-1991, does not define at a sufficient level the degree of independence necessary to accomplish a safety function. Finally, the SRP includes conflicting guidance regarding communication independence by referring back to IEEE Std 7.4.3.2, although RG 1.152 does not endorse Annex E of IEEE Std 7.4.3.2.

The industry has requested further clarification for many technical areas concerning communications independence. It consolidated nine high-priority issues, prioritized them, and distilled them into four areas of interest based on common attributes—interdivisional communications, command prioritization, multidivisional control and display stations, and digital system network configuration. The last area applicable to networking was incorporated into the first three.

The staff has developed the ISG on HICR communications to clarify licensing acceptance criteria related to these four major areas of interest. The NRC has received and addressed public comments via the TWG process. The NRC will issue the final ISG by September 28, 2007. The ISG is consistent with existing regulations, and no new policy issues pertain to this guidance. The staff believes the agency and industry are in good alignment on the technical aspects of the ISG. The staff also appreciated the participation by the industry and vendors on this TWG. One technical issue remains unresolved—the need for safety-grade controls and indications for safety-related components. Although this issue is outside the scope of this ISG, it has a significant impact on HICR design.

In a detailed presentation on the ISG, the NRC staff noted that the overall scope of the communications ISG applies between safety divisions and between safety entities and non-safety entities. The guidance is divided into three sections to address different aspects and different implications of those concepts—interdivisional communications, command prioritization, and multidivisional control and display stations.

The staff also presented the rationale that the safety systems have to be independent and reliable as cited in 10 CFR 50.55a(h), which invokes IEEE Std 603-1991, and as cited in RG 1.152, which invokes IEEE Std 7.4.3.2-2003. The NRC has not endorsed the provision for communications independence in IEEE Std. 7.4.3.2-2003 (Annex E) because it is an informative annex and does not receive same kind of voting as the main body of the standard. Therefore, the staff feels that informative annexes are not appropriate for citation in the RG. However, IEEE Std 7.4.3.2 is currently undergoing revision. Since NRC staff members serve on the IEEE committee, the revision is expected to address the contents of the ISG.

The staff noted that the SRP accepts unidirectional communications outbound from the safety system with no reply or interaction with non-safety systems. In addition, the ISG states that there is zero directional communication as far as the safety function processor is concerned. The ISG also shows the communications processor separate from the function processor that handles communication process, and the function processor is dedicated exclusively to performing the safety function. However, access to the function processor for parameters is transferred through the shared memory. There are provisions for certain parameters to be adjusted by the way of the shared memory. In the ISG the staff incorporated the area into the first three.

Presentation—Diversity and Defense in Depth

The staff had significant interactions with the industry on the ISG regarding diversity and defense in depth, including participation from vendors and utilities. The staff plans to refine the ISG as appropriate and will eventually produce a regulatory guidance document. The staff presented seven problem statements regarding diversity and defense in depth. The ISG mainly considers the first two problem statements, regarding adequate diversity and defense in depth, and sufficient diversity and defense in depth for manual action. Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

Chairman Apostolakis pointed out that the ISG states that if an operator has at least 30 minutes, the protective action may be performed by manual operator actions and the licensee must demonstrate that sufficient controls, independent and diverse from the reactor protection system, are provided in the main control room. In response, the staff stated that it selected 30 minutes as a reasonable period of time to give the operator to understand what is occurring. It does not mean that the operator cannot take actions before 30 minutes have elapsed, but in a worst case failure the operator needs sufficient time (30 minutes in the NRC's opinion) to perform the correct action. The staff also selected the 30-minute criterion to identify whether a diverse actuation system needs to be installed in the plant. In addition, if the licensee shows that it has performed its analysis, it will still be within its design basis after 40 minutes.

Chairman Apostolakis and Dr. S. Guarro, ACRS consultant, want to ensure that the ISG will have some criteria to add the 30 minutes and to justify actions for less than 30 minutes, as the guidance evolves. The staff agreed to provide some criteria for how this consideration will go forward.

The staff presented the third problem statement regarding the fourth position in Branch Technical Position 7-19. Further clarification is needed regarding whether credit for specific component-level actuation will be considered sufficient or whether system-level actuation is needed.

The fourth problem statement relates to whether spurious actuation needs to be considered as well as failure to actuate. The spurious actuation is of lesser concern than the unknown failure that will prevent an actuation. Therefore, the ISG should emphasize the failure to actuate rather than spurious actuation.

Regarding the fifth problem statement, the industry asked the staff whether combinations of design attributes, such as degree of simplicity and testability, exist such that if all are incorporated the staff does not have to consider that the system may have a common-cause failure.

The sixth problem statement requests clarification regarding the way the echelons of defense for maintaining the safety functions should factor into the diversity and defense-in-depth analyses. The staff proposes to combine the reactor trip system and engineered safety features actuation system functions into a single digital platform.

Finally, for the seventh problem statement, the industry asked the staff to clarify the requirements regarding single failure as opposed to common-cause failure. The staff concluded that the software common-cause failure does not meet the criteria for a single failure in single-failure safety system designs, and a software common-cause failure is considered a failure beyond the design basis.

In the long term, the staff will consider ACRS recommendations on assessing and collecting operating experience and inventory/classification and revise the SRP.

Presentation—Status of Evaluation of Operating Experience for Diversity and Defense in Depth

The staff made a presentation on the assessment of operating experience in the nuclear and other industries to obtain insights regarding potential failure modes to be used as input in the diversity and defense-in-depth ISG and inventory/classification, as a followup to an ACRS recommendation from the last subcommittee meeting in April 2007.

The staff gave an overview of its short-term activities. It will perform a quick assessment of existing information related to digital system operating experience and inventory/classification to identify insights and findings that may impact the ISG under development. The staff will hold discussions with EPRI and examine other industry, licensee event report, and COMPSYS data. Long-term activities include continuing evaluation of operating experience for impact on RGs and SRP updates.

The staff's main goal is to provide a framework for collecting and analyzing the operational data, translating that information to regulatory guidance, and translating operational data into regulatory guidance related to diversity and defense in depth.

The staff considered different classification schemes, including safety versus non-safety, a European system (for categories A, B, and C), and system-based classification (e.g., Rashby) in terms of how the systems fail. The proposed failure-type classification expands on the work done by Rashby, Perrow, Aldemir, and the National Aeronautics and Space Administration (NASA).

The staff's proposed classification consists of three attributes—complexity of the system, interactions in terms of communications and importance to safety from a risk-informed perspective, and the importance of the system in terms of maintaining defense in depth and the consequence of system failures. Once the classification system structure is sufficiently complete, the staff will conduct a systems inventory to identify the population of failure data. The staff is also planning to analyze the COMPSYS database to help standardize classification on a system and software basis and standardize how the failure data are entered. The staff's preliminary findings show that the availability of quality data is limited.

The staff also concluded that the common-mode failures and common-cause failures are credible. In the process, the staff learned that NASA and the railroad industry also use diverse systems to mitigate the effects of common cause. The ongoing NRC operating experience

programs are extensive and very valuable to collect, analyze, and distribute information regarding lessons learned to the staff, applicants, vendors, and licensees.

On the basis of the assessment of existing classification systems and operating experience data from the various sources of failure information, the staff made the preliminary conclusion that no correction needs to be made to the proposed diversity and defense-in-depth ISG.

Mr. W. Bowers, Exelon, asked if the staff is using the corrective action program data from the utilities. Dr. O. Maynard, ACRS, added that the industry should submit the corrective action program data to the NRC. The staff is working to obtain access to the industry (i.e., EPRI, INPO) databases as well as international databases.

Presentation—Cyber Security

The staff made a presentation on the industry need for clarification of cyber security guidance and the status of the cyber security ISG. Specifically, the industry requested clarification regarding a conflict between Regulatory Positions 2.1–2.9 in RG 1.152, Revision 2, and NRC-accepted NEI 04-04, Revision 1. Therefore, the TWG conducted a gap analysis to identify inconsistencies between the two documents. The staff did not find any conflicts between the two documents, but it found that they complement one another in that they serve different purposes (licensing for RG 1.152, and guidance for the entire cyber security program for NEI 04-04). The ISG will clarify cyber security as it applies to safety systems and will include a correlation table, once the industry and staff reach consensus. The staff will revise the current draft ISG to incorporate a cross-correlation table.

Dr. S. Abdel-Khalik, ACRS, asked about developing cyber security guidance and how to verify the guidance. The staff commented that the NRC requirements are very limited, and that under a separate effort the agency is developing additional guidance to support the proposed rule on cyber security. The scope of the TWG was to address only the specific problem statement.

Presentation—Human Factors

The staff gave a presentation on two human factors ISGs—one on computer-based procedures and one on minimum inventory. To resolve the problem statement, the staff will prepare an ISG that would fill some gaps in NUREG-0700, “Human-System Interface Design Review Guidelines,” issued May 2002.

Chairman Apostolakis asked if it was necessary to computerize the procedure or if it is left up to the operator. The staff responded that the computer-based system will prompt the operator to select or enter a procedure because of the uncertainty that the diagnostic or the computer can diagnose the event. In addition, computer-based procedures should not initiate control actions without first receiving a command from the operator to do so.

The presentation continued regarding the minimum inventory ISG to ensure that operators have at least the minimum inventory alarms, controls, and displays needed to implement the plant’s emergency operating procedures, bring the plants to safety conditions, and carry out those

operator actions shown to be important from the applicant's probabilistic risk assessment both in the main control room and at the remote shutdown panel.

Closing

Following the staff and industry presentations and discussions, Chairman Apostolakis thanked participants for their contributions and then adjourned the meeting at 3:30 p.m.

SUBCOMMITTEE DECISIONS AND ACTIONS

Overall, the subcommittee was pleased with the staff's progress on the ISGs to review anticipated near-term licensing actions on digital I&C. The members were also encouraged by the degree of collaboration between the staff and industry regarding the ISGs.

In the long term, the staff should develop an alternative process to the 30-minute criterion to determine the conditions under which operator actions can be credited as a diverse protective function.

The issue of spurious actuations that may alter the normal progression of automatic plant response warrants further examination. The diversity and defense-in-depth ISG states that potential spurious trips and actuations are of a lesser safety concern than failures to trip or actuate. This assertion may not be justified for spurious signals that automatically reconfigure systems or initiate unintended functions during the progression of a plant transient or accident. While these actuations should be annunciated in the main control room, they may cause unanticipated conditions that require operator intervention to restore the required safety functions.

Subcommittee members should take a trip to see the HICR at the Westinghouse facility in Pittsburgh, Pennsylvania. A trip to the GE ESBWR was also suggested.

The staff should add a preface to the ISGs stating that options to use different methods than those described are available.

BACKGROUND MATERIALS PROVIDED TO THE SUBCOMMITTEE

(1) Project Plan for Digital Instrumentation and Control, July 12, 2007.

(2) RG 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," January 2006

Note: Additional details can be obtained from the transcript of this meeting available for downloading or viewing on the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/acrs/tr/subcommittee/2006/ or for purchase from Neal R. Gross and Co., Inc. (Court Reporters and Transcribers), 1323 Rhode Island Avenue, NW, Washington, DC 20005; telephone (202) 234-4433.