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

October 1, 2010

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, FEBRUARY 26-27, 2009—ROCKVILLE, MD

The Subcommittee Chairman has certified the minutes of the subject meeting, dated February 26-27, 2009, as the official record of the proceedings of that meeting. I have attached a copy of the certified minutes.

Attachment: As stated

cc: E. Hackett
A.Dias

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

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

FROM: Charles H. Brown, Chairman
Digital I&C Systems Subcommittee

SUBJECT: CERTIFICATION OF THE MINUTES OF THE MEETING OF THE ACRS SUBCOMMITTEE ON DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS, FEBRUARY 26-27, 2009—ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting, dated February 26-27, 2009, are an accurate record of the proceedings for that meeting.

/RA/ ***October 1, 2010***

Charles H. Brown, Chairman Date
Digital I&C Subcommittee

Certified on: October 1, 2010
By: Charles Brown

MEETING MINUTES
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
MEETING OF THE ACRS SUBCOMMITTEE ON
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS
FEBRUARY 26-27, 2009—ROCKVILLE, MD

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on February 26-27, 2009, 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 discuss the subcommittee the updated ISGs on ISG #5, Section 3 on Manual Operator Actions and currently issued ISG #6, Digital I&C Licensing Process, the progress associated with the research on diversity strategies of NPP I&C, the regulatory guide on cyber security, and the operational experience insights on common cause failure (CCF) on Digital I&C and the Diverse Actuation System (DAS) risks and benefits.

Ms. C. Antonescu 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 February 26, 2009, and adjourned on February 27, 2009 at 11:30 am.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman
J. Stetkar, Member
D. Bley, Member
C. H. Brown, Member
J. Sieber, Member
M. Bonaca, Member
S. Guarro, ACRS Consultant

ACRS Staff

C. Antonescu, Designated Federal Official and Lead Staff Engineer

Principal NRC Speakers and Consultants

R. Sydnor, RES
K. Sturzebecher, RES
S. Morris, NSIR
S. Arndt, NRR
D. Hermann, NRO
M. Waterman, RES
E. Miller, NRR
B. Kemper, NRR
D. Santos, RES
J. Grobe, NRR
P. Hiland, NRR
S. Bailey, NRR
D. Desaulniers, NRR
S. Morris, NSIR
E. Eagle, NRR
L. James, NRO
J. Wermiel, NRR

Principal Industry Speakers

J. Naser	T. Quinn
J. Riley	R. Wood
P. Craig	B.Geddes

Other members of the public attended this meeting. A complete list of attendees is available from the ACRS upon request.

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. Specifically, during the February 26-27, 2009, the subcommittee reviewed the updated ISGs on ISG #5, Section 3 on Manual Operator Actions and currently issued ISG #6, Digital I&C Licensing Process. Also, the staff briefed the ACRS on progress associated with the research on diversity strategies of NPP I&C and the regulatory guide on cyber security.

DISCUSSION OF AGENDA ITEMS

Specifically the NRR staff discussed two ISGs DI&C-ISG-05, "Highly- Integrated Control Room–Human Factors Issues," and draft DI&C-ISG-06, "Licensing Process."

Mr. David Desaulniers gave a presentation **on DI&C-ISG-05 "Highly- Integrated Control Room–Human Factors Issues**." This ISG is guidance on how to demonstrate through suitable human factors engineering (HFE) analysis that manual operator actions can be performed inside the control room are acceptable in lieu of automated backup functions. Also, this guidance can be used to demonstrate the acceptability of operator actions required in less than thirty minutes. Specifically, a new Section 3 of this ISG was developed to provide an alternative process to the thirty-minute criterion to determine the conditions under which operator actions can be credited.

Action Items: The subcommittee recommended that DI&C-ISG-05, Section 3, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," be revised to incorporate additional guidance on the estimation methods of the time required for operator action.

Also, part of the Committees recommendation, the staff was tasked to 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 discussion under Staff Position should be revised to clearly state that the degree of validation for acceptance of credit should be more stringent for this situation. ISG-5 addresses a difficult problem. The subcommittee **commended** the staff for developing a thoughtful and coherent approach.

Ms. Lois James presentation was on draft final **ISG-6, "DI&C Licensing Process."** This ISG provides guidance for the NRC staff's review of DI&C systems in accordance with current licensing processes. Also, this ISG describes the information and documentation the NRC staff will need for its review of license amendment requests (LARs) for DI&C upgrades in operating

plants and when the information should be provided. ACRS reviewed a previous version of this Draft ISG during our 551st meeting on April 10-12, 2008. Subsequently, it was revised to incorporate the lessons learned from the Oconee and Wolf Creek DI&C system upgrades.

DI&C-ISG-06 clarifies the licensing criteria that the staff will use for nuclear plant license amendments in confirming that a proposed design meets applicable requirements. Specifically, the industry and vendors have requested clarification regarding what documents need to be provided to the staff for each phase of its review, which documents need to be on the docket, and which documents do not need to be docketed but should be available for staff review during the audit. The draft DI&C-ISG-06 incorporates the lessons learned from the Oconee and Wolf Creek DI&C system upgrades. Specifically, the staff has incorporated several issues in the ISG, including the need to: 1) interface early with the licensee on key technical issues such as defense-in-depth and diversity; 2) provide for more frequent feedback on the progress of the review; and 3) provide for a phased approach to the submittal of important documents for staff review.

The staff presented this draft final ISG that clarifies the licensing criteria that the staff will use for nuclear plant license amendments in confirming that a proposed design meets applicable requirements. The staff intends to continue working with stakeholders in refining the interim guidance and in developing final guidance. Specifically, the staff has undertaken an effort to more clearly describe the process for licensing digital I&C system modifications to an operating plant under Task Working Group 6 (TWG-6). This effort was necessitated by licensee concerns regarding the level of detail required in submittals for staff review and questions regarding the applicability of the guidance in Standard Review Plan Chapter 7 to digital I&C systems. The outcome from this effort will be interim guidance (ISG-6) for licensees to use when planning a license amendment request. Also the guidance identifies the documentation needs and timing for the various aspects of the staffs review effort with the aim of reducing regulatory uncertainly.

The staff started this effort last year, but due to the press of other activities (primarily the Oconee review) delayed this effort. It was determined that the first draft of the ISG was not an effective starting point so the TWG started down a new path taking advantage of the lessons learned from the Oconee and Wolf Creek digital I&C system modifications which are currently under review.

Action Item: During the meeting the subcommittee also recommended that draft DI&C-ISG-06 not be issued until Sections C and Section D are revised to require sufficient design detail to ensure deterministic behavior and independence of each DI&C safety train.

Also, the staff has identified several issues for incorporation in the interim guidance including the need to 1) interface early with the licensee on key technical issues such as defense-in-depth and diversity, 2) provide for more frequent feedback on the progress of the review, and 3) provide for a phased approach to the submittal of important documents for staff review. The staff has restarted the effort and is currently having numerous interactions with NEI and licensees to incorporate comments and receive input as the guidance is developed. The current plan is to complete an initial draft of the digital I&C system review process guidance in May of 2009. The staff would like to have the ACRS input into the development of this guidance.

Mr. Karl Sturzebecher of NRC staff discussed the **Draft Final Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities,"** and NRC staff's resolution of stakeholders' comments. 10 CFR 73.54 establishes performance-based requirements to ensure that the functions of critical systems and critical digital assets are protected from cyber

attack using a graded approach. RG 5.71 conveys NRC staff positions for developing a program that provides an effective protection mechanism against cyber attacks. It also provides NRC staff positions regarding the minimum set of elements needed within a program to protect a facility, the networks within it, the plant systems, the digital assets that implement system functions, and operating systems and applications within those digital assets that accomplish the functions to be protected. A generic cyber security plan template, NEI-08-09, is also being jointly-developed between staff and industry for later consideration as a reference in RG 5.71.

Action Items: The subcommittee recommended that RG 5.71 be revised to: (i) provide a reference Digital I&C (DI&C) computer, communication, and network security framework that identifies assets, associated plant functions, vulnerabilities, and interaction and access pathways; (ii) include examples and more specific guidance on how the stated requirements can be met; (iii) ensure that the guidance distinguishes between DI&C system and non-real-time information technology system architectures; and (iv) address the issues of threat assessment, dependency analysis, and the use of probabilistic risk assessment (PRA).

Also during this meeting, representatives of the staff and Nuclear Energy Institute (NEI) stated that there were three main reasons for having the content of the guide at the current high level:

- Sensitivity to public disclosure of detailed information concerning nuclear power plant systems.
- Rapidly changing nature of digital technology that also may bring equally rapidly changing nature of the security threats.
- Preference for performance-based regulatory criteria

In return the subcommittee made the following comments:

- There are ways of addressing the sensitivity issue. For example, a generic reference framework for cyber security (with sufficient detail and scope) could be described in RG 5.71 that would specify the required information and level of analysis that a licensee should provide without disclosing specific facility and system details. This generic framework for security that could help define the minimum technical attributes regarding:

    1. the critical digital assets (CDAs),
    2. the associated functions,
    3. asset interactions and pathways,
    4. infrastructure services that support the CDAs,
    5. defensive measures that address the cyber security threats,
    6. the consequences of an intrusion, and
    7. protective provisions.

- Although the digital and network technology is changing at a rapid pace, this change does not affect significantly the internal functional environment of digital controls and data pathways that are of concern for a typical plant.

- The performance requirements stated in this guide are not numerical; a description of a minimum threshold of quality and information content of such strategies is needed.

Also, regarding threat assessment a systematic delineation of threat scenarios (e.g., using event-sequence diagrams or other similar risk-assessment tools) is a useful method to identify vulnerabilities and pathways that could compromise CDAs.

In addition, along with the generic reference framework, examples of characteristics of strategies and procedures that are acceptable to the NRC should be included in RG 5.71.

The **NUREG/CR on Diversity** serves to document baseline diversity strategies for nuclear power plant I&C systems within a systematic classification framework (i.e., Strategies A, B, and C with several justified options within each), the technical basis justifying the baseline diversity strategies is established by the research findings documented in the NUREG/CR, and the NUREG/CR documents assessment tools that have been developed to support review.

Specifically **Mr. Mike Waterman**, RES talked about the assumptions he used into the research, about how to use the data, about the sources of data that he looked at, and the data evaluation method that he proposed out of this. At the end he summarized the results of the evaluation, talked a little bit about constraints on using the evaluation method, and then summarized the presentation.

One of the issues is that the regulatory guidance and requirements do not define what constitutes adequate diversity. There's no guidance in how much diversity is enough in a safety system design. And because nobody's really defined how much is enough, we've got licensing uncertainty out in the industry, because everyone has all these different interpretations of what we mean by adequate. So the NRC and the industry really needed to start coming with a common ground to work in with regard to how much diversity is enough.

This issue was identified further in the Task Working Group 2, which focus was on diversity in defense-in-depth, and question number came up too, "How much diversity is enough? After you identify a need for diversity, how much is enough?"

What RES does not address is whether or not diversity is needed, which was already done. So RES got a research program that is addressing the question of how much diversity is enough.

The staff talked about the issues that are to be addressed by the research, the diversity attributes and criteria that they are using. The staff went into some operating experience considerations briefly and then talked about the sources of data they are using, and talked about some of the research assumptions that they used when they did the research.

The research assumptions were discussed on the use diversity positions and designs used by other people on the basis that they probably used operating experience and judgment in developing those designs that RES would then try to correlate that information with NUREG/CR-6303, diversity attributes and criteria. And by doing that, RES should be able to develop an evaluation process that they could apply the design to. And then they would try to capture some better perspectives out of industry and nuclear power plant operating experience and see if that could help develop this method.

RES took the NUREG/CR-6303, diversity criteria and attributes transferred that data into a spreadsheet format. They used Microsoft Excel spreadsheet and by taking those diversity criteria they were ranked in NUREG/CR-6303 developed a simple weighting system that would give more emphasis to more effective criteria and less emphasis on less effective criteria. RES is doing this to develop a method of evaluating proposed diversity approaches.

Also, the question that always comes up is when a design is proposed and then they don't know whether that design is diverse enough to meet all the criteria it needs to meet, have sufficient diversity. Because there's been a lot of uncertainty, regulatory uncertainty as licensees propose designs and the regulator says that they don't know if that's enough.

The easiest way to do that is if you have some numerical range to start out with, then you can screen out diverse designs that just don't fit into the range.

Overall the mission is to address common-cause failures, not just to build diverse systems. The idea of a diverse system is to address some potential range of common-cause failures. That's where operating experience can help out and where engineering judgment can help out, is to identify the common-cause failures that have to be addressed. So any diversity strategy should be focusing on where they have got a common-cause failure microprocessor. What they are really trying to develop is a ranking that would give you a numerical metric or a numerical ranking of how effective is the diverse system you've designed at taking care of, or addressing common-cause failures?

In addition, the two NEI reports on Operating Experienced insights on Common-Cause Failures and Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions Reports were delayed to be discussed at the DI&C subcommittee meeting in August 2009.

More details regarding the meeting can be found in the Transcripts.

REFERENCES:

(1) U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-ISG-5 Rev 1, “Highly-Integrated Control Room-Human Factors Issues,” dated November 3, 2008, Rev.1 (ML082740440)

(2) U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-Draft ISG-6, “Licensing Process,” dated January 14, 2009 (ML090130273)

(3) U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-ISG-2, “Diversity and Defense-in-Depth Issues,” dated September 26, 2007 (ML072540118)

(4) NUREG-0800 Chapter 7 Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Rev. 5, dated March 2007 (ML070550072)