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, OCTOBER 23, 2009—ROCKVILLE, MD

The Subcommittee Chairman has certified the minutes of the subject meeting, dated October 23, 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, OCTOBER 23, 2009—ROCKVILLE, MARYLAND

I do hereby certify that, to the best of my knowledge and belief, the minutes of the subject meeting, dated October 23, 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
OCTOBER 23, 2009—ROCKVILLE, MD

INTRODUCTION

The Advisory Committee on Reactor Safeguards (ACRS) Subcommittee on Digital Instrumentation and Control (I&C) Systems held a meeting on October 23, 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 Draft Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities and the status of the Cyber Security Assessment Team and the NERC/FERC MOU. 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 October 23, 2009, and adjourned on October 23 at 3:00pm.

ATTENDEES

ACRS Members

G. Apostolakis, Subcommittee Chairman
J. Stetkar, Member
D. Bley, Member
J. Sieber, Member
S. Guarro, ACRS Consultant

ACRS Staff

C. Antonescu, Designated Federal Official and Lead Staff Engineer

Principal NRC Speakers and Consultants

R. Sydnor, RES
R. Costello, NSIR
S. Morris, NSIR
E. Lee, NSIR
C. Erlanger, NSIR
C. Sturzebecher, RES
G.Wilson, NRR

Principal Industry Speakers

M.Schinn
E.Cole
B.Gross

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, the subcommittee was to discuss Draft Final Regulatory Guide 5.71 ”Cyber Security Programs for Nuclear Facilities” and other security matters.

DISCUSSION OF AGENDA ITEMS

The DI&C Subcommittee met with representatives of the NRC staff to discuss the draft final Regulatory Guide (RG) 5.71 and the major changes to this draft final guide since the March 5th ACRS meeting. During the presentation the staff described the changes in the November 2009 version of RG 5.71. These changes included discussions (1) to address ACRS' comments in their March 19, 2009 letter and (2) the expanded guidance how to establish, implement, and maintain a cyber security program. Also, during the meeting the Office of Nuclear Regulatory Research (RES) and Office of Nuclear Security and Incident Response (NSIR) staff described the new detailed guidance and examples for the selection process of critical systems and critical digital assets and with specific characteristics when employing the critical digital assets within a defensive architecture. The selection of security controls incorporates an acceptable method for the licensee/applicant when addressing the cyber vulnerabilities. The security controls were adapted from the National Institute of Standards and Technology (NIST) cyber security standards as well guidance from the U.S. Department of Homeland Security (DHS). The guidance also addresses the management of potential vulnerabilities, weaknesses, and cyber risks introduced by changes in the system, network, environment, or emerging threats. In addition the regulatory guide includes a generic cyber security plan template where the licensee/applicant accounts for the site-specific conditions that affect implementation of Regulatory Guide 5.71.

During the meeting the Subcommittee concluded that RG 5.71 requires that the licensees produce policies and plans for cyber security without providing guidance as to their adequacy. Also after implemented in nuclear facilities for about a year, RG 5.71 should be revised to include the resulting insights and provide guidance regarding the adequacy of cyber security and polices. In addition longer-term research projects should be initiated by the RES in the following areas: exploration of the use of PRA insights, in particular those regarding accident sequences, in cyber security; development of better guidance on the interaction between cyber security and safety; and investigation of supply chain attacks.

Also several other initiatives which relate to RG-5.71 and the relationship between these initiatives were discussed during the meeting: The NERC MOU which is still in draft form (this effort defines cyber security inspection roles/responsibilities for NRC and NERC at power plants); The Cyber Security Assessment Team (CSAT) charter and procedures is a cross agency initiative related to responding to serious cyber security incidents on NRC IT systems as well as at nuclear power plants, and the inter-office effort (between NRO and NRR) intended to update RG-1.152.

Specifically the action items during the meeting were:

1. Insufficient guidance on how licensees can identify their CDAs. No guidance provided the method. NUREG/CR –6849 (Appendix C) provided some guidance on how to group digital assets into CDAs as a start. During the meeting the discussion centered on providing a detailed guidance for analyzing the assets, associated plant functions, vulnerabilities, interaction, and access pathways and will reference an acceptable method for licensee in determining the critical digital assets (CDAs). Also, the staff has

been working with the industry to develop a generic cyber security plan "template" as part of Appendix A of RG 5.71 that will provide licensees with a detailed framework for cyber security plant at nuclear facilities.

2. Specifically the staff was asked to include more examples and specific guidance in the final RG 5.71 and cyber security template.

3. The Staff agreed to provide more detailed guidance to distinguish between information technology system architectures and DI&C systems with real examples in Section 3.5 of RG 5.71 and cyber security template.

4. The Subcommittee asked the staff to develop a set of deterministic security controls based on NIST cyber security standards that are based on threats, vulnerabilities and attacks. Also, in Appendix A (i.e. the generic cyber security plan template) of the final RG 5.71 the dependency analysis of a CDA for plant infrastructure support service needs to be included. In addition as far as the use of a PRA, the cyber threat is assumed to exist for the identified CDAs.

5. Inconsistency with the industry control system security guidance as developed by NIST (NIST 800-53/800-82), specifically where the reg guide claims its security controls are based on NIST 800-53/800-82. Essential to the NIST process of tailoring security controls is the assessment of the cyber security vulnerabilities and risks for each system in question. NIST 800-82, Section 4.2.6, Perform Risk and Vulnerability Assessment, calls for organizations to perform a risk assessment for each system and then perform a detailed vulnerability assessment for high risk systems. In sharp contrast, RG 5.71 requires the application of a predefined set of NIST security controls to all safety, security and emergency preparedness (SSEP) systems without any tailoring based on risk. No clear cut guidance is provided to conduct risk or vulnerability assessments on each system. Also, there is no method for prioritizing the implementation of security controls for CDAs at the highest risk of cyber exploitation and no method for prioritizing the implementation of those security controls that are most effective at reducing cyber security risk. As a result, licensee implementation of cyber security controls is likely to be difficult and NRC will have a hard time to conduct meaningful and cyber security inspections.

During the meeting the subcommittee main concern was for the staff to incorporate a reference nuclear plant digital network framework that would serve as a basis upon which to support the discussions regarding network vulnerabilities, interactions, and access pathways. Such a framework would serve to better illustrate the application of the topical material presented. The new revision should contain such a model framework, it has been enhanced with numerous examples of acceptable methods for implementing 10 CFR 73.54 and with clear definitions of terms that appear to be consistent with their use in the NIST Special Procedures identified as bases and reference documents. The more abundant use of these acceptable methods as examples helps to provide consistent guidance that conveys the applicability of the concepts described.

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

REFERENCES:

(1) RG 5.71 “Cyber Security Programs For Nuclear Facilities”, November, 2009 (ML092670517)

(2) NRC Cyber Security Tasks: The Relationships between NRC Cyber Security Regulatory Initiatives

(3) NERC Memorandum of Understanding (MOU)

(4) The Cyber Security Assessment Team (CSAT) Charter and Procedures (ML0924603050.doc, ML0915502630.doc, ML0915502730.doc, ML0915502900.doc).

(5) Cyber Security Overview: Cyber Security for Nuclear Reactors)

(6) NIST SP 800-53, Rev. 3, “Recommended Security Controls for Federal Information Systems,” National Institute of Standards and Technology, Gaithersburg, MD, August 2009