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

August 30, 2007

MEMORANDUM TO: ACRS Members

FROM: Girija Shukla, Senior Program Manager **/RA/**
Technical Support Branch, ACRS

SUBJECT: TRANSMITTAL OF STATUS REPORT, PROPOSED SCHEDULE, AND ADDITIONAL MATERIAL FOR DIGITAL INSTRUMENTATION AND CONTROL SUBCOMMITTEE MEETING ON SEPTEMBER 13, 2007

The Digital Instrumentation and Control (I&C) Subcommittee will meet on September 13, 2007 to discuss digital I&C system issues. The full Committee will review this issue during the 546th ACRS meeting October 4 - 6, 2007.

Attendance by the following members is anticipated at the September 13, 2007, Subcommittee meeting:

Apostolakis	Maynard
Abdel-Khalik	Bonaca

Dr. Sergio Guarro is a consultant who will be reviewing the review materials and submitting a report with comments prior to the meeting.

To prepare for this meeting, the following information is attached:

1. Status Report
2. Proposed Schedule for September 13, 2007, Subcommittee meeting
3. Proposed Schedule for October 4-6, 2007, full Committee meeting

In addition, Regulatory Guide 1.152, Revision 2 is being transmitted.

The following review materials were provided on August 22, 2007:

1. A description of NRC Steering Committee activities for digital I&C
2. The current Digital I&C Project Plan
3. The current draft Interim Staff Guidance (ISG) for the major digital I&C issues

If you have any questions, please contact me at (301) 415-8439 or by email at gss@nrc.gov.

cc w/o Attachments: F. Gillespie
S. Duraiswamy
C. Santos

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS SUBCOMMITTEE MEETING
ROCKVILLE, MD
SEPTEMBER 13, 2007

STATUS REPORT

PURPOSE

The purpose of this meeting is to review the ongoing digital instrumentation & control (I&C) system program issues. During the meeting, the Subcommittee will be expected to review the interim staff guidance being developed by the staff for review of digital I&C applications. The full Committee will also discuss this matter during the 546th ACRS meeting in October 2007.

BACKGROUND

The Committee ACRS last reviewed the staff activities related to Digital I&C issues at the May 2007 meeting. The staff presented information regarding the Digital I&C Project Plan and the Steering Committee activities involving several ongoing issues. The Committee issued a letter to the Chairman Klein dated May 22, 2007, which provided the Committee's view on the staff's activities. The letter provided three recommendations:

- The staff should develop an inventory and classification (e.g., by function or other characteristics) of the various types of digital and software systems that are being used and are likely to be used in nuclear power plants.

- The staff should evaluate the operating experience with digital systems in the nuclear and other industries to obtain insights regarding potential failure modes.

- The information obtained through performing the above two activities in should be used in the development of regulatory guidance on defense-in-depth and diversity for digital I&C systems.

The Committee also met with the Commission on June 7, 2007 to discuss these and other issues. The Commission then met with the staff on July 18, 2007 to discuss the staff activities on the digital I&C issues. The Commission issued an SRM to the staff on June 22, 2007, which adopted the ACRS letter recommendations and directed the staff to develop interim guidance for the major issue tasks by September 30, 2007. Another SRM issued on August 3, 2007, added that the staff should continue to work with domestic and international working groups to address the digital I&C areas and leverage international experience.

DISCUSSION

The Digital I&C Project Plan (Reference 1) defines the roles and responsibilities of the Steering Committee and the Task Working Groups (TWGs). It describes the process to develop Interim Staff Guidance (ISG) for the review of digital I&C technology for operating reactors, new reactors, and fuel cycle facilities. The Project Plan accounts for issues related to the review of anticipated licensing actions including: digital upgrades at operating reactors and fuel cycle facilities, new reactor Design Certification and Combined License (COL) applications.

The specific short-term objective of this plan is to identify digital I&C technical and regulatory issues for which ISG can be developed in time to support the review of the anticipated licensing actions. The long-term objectives of this plan are to continue stakeholder interactions to refine and enhance digital I&C regulatory guidance or identify consensus standards that could be endorsed as regulatory guidance. The deliverables associated with the long-term objectives are to develop recommendations that will be used to update the Standard Review Plan (SRP) and Branch Technical Positions (BTPs), and other regulatory documents, e.g., NUREGs or Regulatory Guides (RGs), and revise regulations, as appropriate, through established agency processes.

The digital I&C Task Working Groups (TWGs) were established to include technical staff from appropriate NRC offices to focus on six key areas. The TWGs interact with industry counterparts to facilitate discussion of technical and regulatory issues and the development of recommendations for each TWG area. The NRC line organizations perform tasks identified in the individual TWG project plans and interface with the TWGs and report to the Steering Committee. The TWGs have developed an individual TWG project plan for each of the six key areas:

TWG #1: Cyber Security
TWG #2: Diversity and Defense-in-Depth
TWG #3: Risk-Informing Digital I&C
TWG #4: Highly-Integrated Control Room–Communications
TWG #5: Highly-Integrated Control Room–Human Factors
TWG #6: Licensing Process

The draft Interim Staff Guidance (ISG) has currently been developed by the TWGs in four of these areas (#1, #2, #4, and #5) and are briefly described below. ISGs #3 and #6 are scheduled to be available by approximately November 2007, and January 2008, respectively.

Summary of draft ISG #1 - Cyber Security

This ISG states that the proposed Nuclear Energy Institute document NEW-04-04 Rev. 2, “Cyber Security Program for Power Reactors,” August 4, 2007, adequately incorporates and addresses Regulatory Positions 2.1 - 2.9 of Regulatory Guide 1.152 Rev. 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” January 2006 (Reference 2). Nonetheless, the ISG states that NEW 04-04 Rev. 2 does not establish minimum standards of acceptable risk and lacks the specific measures needed to mitigate such risks. In addition, NEW 04-04 does not establish quantifiable metrics to enable a meaningful assessment of cyber security program effectiveness. Due to its performance-based (i.e., non-prescriptive) nature, NEW 04-04 does not provide the type of directive statements typically found within NRC regulatory guidance documents. As such, NEW 04-04 leaves licensees and applicants open to develop their own criteria and standards. The NRC staff is concerned that this lack of specificity will result in standards that are inconsistently determined and applied throughout the industry. As such, the staff plans to develop a Regulatory Guide, in support of the ongoing 10 CFR 73.55 rulemaking effort (physical protection against radiological sabotage), to assist licensees, permit holders, and applicants in understanding how to meet the acceptable standards.

Summary of draft ISG #2 - Diversity and Defense-In-Depth (D3)

The ISG on D3 states that in order to demonstrate that vulnerabilities to a common cause failure (CCF) have been adequately addressed, a D3 analysis should be performed. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 1994, and BTP-19 are an acceptable means for a D3 analysis. If the D3 analysis determines the system or systems are subject to a CCF, an analysis of the plant responses to all Chapter 15 events calculated using best-estimate methods with realistic assumptions should be preformed to determine the time frame for necessary protective actions. In those instances where the protective action is required in less than 30 minutes, an independent and diverse automated backup, achieving the same or equivalent function, should be required. This independent and diverse automated backup function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. These independent and diverse automated backup systems should be similar in quality to the systems required by the Anticipated Transient Without Scram (ATWS) rule (10 CFR 50.62). In those cases where plant response analysis shows that the protective action is not required for at least 30 minutes, the protective action may be performed by manual operator actions. The ISG further states that the licensee will be required to demonstrate that sufficient information and controls (safety or non-safety), independent and diverse from the RPS discussed above, are provided in the main control room, and that the information displays and controls are not subject to the same CCF. In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as required backup capabilities, the displays and controls should be hard-wired downstream of the lowest-level software-based components.

Summary of draft ISG #4 - Highly-Integrated Control Room - Communications

This ISG addresses issues in the following four basic areas of interest:

1. Interdivisional Communications: communications among different safety divisions[1] or between a safety division and a non-safety entity. The ISG includes 20 criteria including: independence of safety channels, data content and storage, fault effects, and other criteria.

2. Command Prioritization: selection of a particular command to send to an actuator when multiple and conflicting commands exist. The ISG includes 10 criteria including ensuring highest priority for safety-related commands and command software design.

3. Multidivisional Control and Display Stations: use of operator workstations or displays that are associated with multiple safety divisions and/or with both safety and nonsafety functions. The ISG includes several criteria including ensuring independence and isolation and limiting the effects of spurious actuations.

4. Digital System Network Configuration: the network or other interconnection of digital systems that might affect plant safety or conformance to plant safety analysis assumptions. The ISG

states that interconnections among safety divisions or between safety and nonsafety divisions should also satisfy the guidance provided for interdivisional communication.

Summary of draft ISG #5 - Highly-Integrated Control Room - Human Factors

This ISG addressed the minimum inventory of human system interfaces (i.e., alarms, controls, and displays) needed to implement the plant's emergency operating procedures, bring the plant to a safe condition, and to carry out those human actions shown to be important from the applicant's probabilistic risk assessment. The ISG also provides additional review guidance for computer-based procedures and procedure systems.

EXPECTED SUBCOMMITTEE ACTION

During the upcoming meeting on September 13, 2007, the Subcommittee will be expected to review the currently issued ISGs in the staff Project Plan and report its recommendations to the full Committee for its consideration at the 546th ACRS meeting in October 2007.

References:

1. Project Plan for Digital Instrumentation and Control dated July 12, 2007
2. Regulatory Guide 1.152 Rev. 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," January 2006

Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems Subcommittee Meeting
Rockville, MD
13 September 2007

- Proposed Schedule -

Cognizant Staff Engineer: Girija Shukla (301-415-8439, gss@nrc.gov)

	Topic	Presenter(s)	Time
	Opening Remarks	G. Apostolakis, ACRS	8:30 - 8:35 am
I	NRC Digital I&C Steering Committee Activities	Belkys Sosa, NRR	8:35 - 8:45 am
II	Industry Perspective on Digital Safety Systems Issues	NEW	8:45 - 9:45 am
Break			9:45 - 10:00 am
III	Interim Staff Guidance (ISG) on Highly Integrated Control Rooms - Digital Communication Systems	William Kemper, NRR Paul Rebstock, RES	10:00 - 11:15 am
	ISG on Diversity and Defense-in-Depth (D3) for Digital Safety Systems	Ian Jung, NRO Michael Waterman, RES Paul Loeser, NRR	11:15 - 12:00 pm
Lunch			12:00 - 1:00 pm
III	Status of Evaluation of Digital Systems Operating Experience and Inventory and Classification	Ian Jung, NRO Michael Waterman, RES	1:00 - 2:00 pm
	ISG on Cyber Security	Mario Gareri, NSIR	2:00 - 2:30 pm
Break			2:30 - 2:45 pm
III	ISG on Human Factors	Michael Marshall, NRO	2:45 - 3:15 pm
IV	Subcommittee Discussion	G. Apostolakis, ACRS	3:15 - 4:00 pm

Notes:

- Presentation time should not exceed 50% of the total time allocated for a specific item.
- Number of copies of presentation materials to be provided to the ACRS - 35.

Advisory Committee on Reactor Safeguards
NRC Staff Activities for Digital Instrumentation and Control Systems
October 4-6, 2007
Rockville, MD

- Proposed Schedule -

Cognizant Staff Engineer: Girija Shukla, gss@nrc.gov 301-415-8439

Topics	Presenters	Time
Opening Remarks	G. Apostolakis, ACRS	5 minutes
Industry perspective on digital I&C system issues	A. Marion, NEW	15 minutes
Staff presentation on NRC activities related to digital instrumentation (I&C) and control systems issues	B. Sosa, NRR	55 minutes
Committee Discussion	G. Apostolakis, ACRS	15 minutes

Note

- Presentation time should not exceed 50 percent of the total time allocated for specific items. The remaining 50 percent of the time is reserved for discussion.

- 35 copies of the presentation materials to be provided to the Committee.