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

October 20, 2010

Mr. R. W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT FINAL DIGITAL INSTRUMENTATION & CONTROL INTERIM STAFF GUIDANCE-06: LICENSING PROCESS

Dear Mr. Borchardt:

During the 576th meeting of the Advisory Committee on Reactor Safeguards, October 7-9, 2010, we reviewed Draft Final Revision 50 to Digital Instrumentation and Control (DI&C) Interim Staff Guidance (ISG)-06, "Licensing Process." Our DI&C Systems Subcommittee also reviewed this matter during a meeting on September 8, 2010. During these reviews, we had the benefit of discussions with representatives of the NRC staff and Nuclear Energy Institute (NEI). We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. ISG-06 should be issued subject to incorporation of Recommendations 2 and 3.

2. Section B should be revised to include a discussion that while process is important, it is not a substitute for a detailed review of the hardware and software architectures to ensure that they meet the fundamental principles identified in the discussion. These principles should be emphasized in this Section.

3. Section D should be revised to emphasize the need to review the design from an integrated hardware/software perspective in order to develop a clear understanding of the overall complexity of the system.

4. Software Failure Modes and Effects Analysis (FMEA) methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable DI&C performance.

5. The staff should develop an integrated process that ensures that the DI&C system will be able to meet, with reasonable assurance, the combined requirements associated with plant safety and cyber security threats.

BACKGROUND

ISG-06, "Licensing Process," provides guidance for the NRC staff's review of DI&C systems in accordance with current licensing processes. This ISG also describes the information and documentation the NRC staff will need for their review of license amendment requests (LARs) for DI&C upgrades at operating plants and when the information should be provided. The ISG

was previously reviewed by the Committee in April 2009. A Committee letter was issued on April 21, 2009. A subsequent review was performed by our DI&C Systems Subcommittee on August 19-21, 2009. Substantial revisions have been incorporated since the August 2009 review as a result of numerous public meetings and extensive industry comments.

DISCUSSION

ISG-06 clarifies the scope of information that is required for the NRC staff review of DI&C upgrades at operating plants. Section C of ISG-06 divides the licensing review process into four phases: Phase 0 - Pre-Application Meetings, Phase 1 - Initial Application, Phase 2 - Continued Review and Audit, and Phase 3 - Implementation and Inspection. Within this structure, the ISG lays out three tiers, each corresponding to an expected level of complexity and correspondingly higher level of review. Tier 1 would apply for LARs using a previously approved system with no deviations. Tier 2 would apply for LARs using a previously approved system with deviations to suit the plant-specific situation. Tier 3 would apply for LARs using a totally new system with no generic approval.

ISG-06 is intended to provide a timely and efficient licensing approach for completing reviews of applications for installing DI&C system upgrades at operating plants by identifying a uniform set of expectations relative to documentation and detail design information.

During our reviews, numerous issues were raised. Examples are as follows:

Section B, “Purpose,” has been significantly expanded to describe the philosophy and principles of the NRC review. Section B.1 states that, “The NRC staff does **not** perform an independent design review of the DSS [Digital Safety System]. Instead, the staff reviews the design process and design outputs to determine that the process is of sufficiently high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants. Therefore, a major portion of the NRC staff review is of documentation of plans and processes which describe the life-cycle development of the software to be used by and/or in support of the DI&C system. The NRC staff will sample the design process with the intent of determining that the process described is the process that was used, that the process was used correctly, and that it was used in such a manner as to produce software suitable for use in safety-related applications at nuclear power plants. For this reason, the DSS design must be complete and the system tested to demonstrate that it will perform its safety function.”

This seems to imply that the review is primarily about process without the requisite need for an independent review and understanding of the detailed hardware and software design. Conversely, Section D, “Review Areas,” indicates that a significant amount of detail is required for the staff to complete their licensing review.

Section B is the opening message for the entire ISG and should set the tone to ensure understanding that while process is important, it is not a substitute for a detailed review of the hardware and software architectures to ensure that they meet the four fundamental principles of redundancy, independence, determinate behavior, and diversity and defense in depth, as well as the more subjective principle of simplicity of design. These principles should be given significant emphasis in this Section.

Section B should also emphasize that the inclusion of commitments to meet requirements is not a substitute for detailed designs which actually meet those requirements. We understand that

the staff does not need to perform an independent design review of the entire system. However, sufficiently detailed functional diagrams and explanatory discussion must be provided so that a detailed review can be accomplished to ensure that the four fundamental principles are inherent in the hardware and software DI&C architectures.

Section D, “Review Areas,” primarily emphasizes the software design perspective which is process oriented. However, hardware design decisions can drive software complexity and, thus, exacerbate potential common cause failure concerns. For example, when plant parameters are input to a processor whose digital output is sent to a separate processor-based voting unit, the system is sending digital data to another digital processing platform; whereas, if the same data were sent to an analog platform, a different software interface would be needed. The sections describing the hardware and software architectures should emphasize the need to review the design from an integrated hardware/software perspective in order to develop a clear understanding of the overall complexity of the system.

Section D addresses FMEA primarily with reference to hardware. The staff stated that software is not generally addressed by industry in their FMEAs. The staff stated that the NRC has partitioned software failures into two types. If it is a single failure within a box, that would be enveloped by the worst case failure of the hardware in that box. If it is a failure that would cause multiple boxes to fail at the same time, then that is addressed by the Diversity and Defense-in-Depth (D3) analysis of the common cause software failure.

There are characteristics of software that could result in failure modes that are not anticipated in the classic hardware FMEA sense. For example, software incorporates programming functions, such as global variables or interrupts, that, if used and not applied in a well controlled manner, could result in mal-operation of the software and possibly affect multiple divisions depending on the hardware architecture used in the overall design. Software FMEA methods should be investigated and evaluated to examine their suitability for identifying critical software failures that could impair reliable and predictable DI&C performance.

During our meeting, the issue of ensuring that the final design has the means to provide barriers to internal and external cyber security threats was discussed. The staff stated that the Office of Nuclear Security and Incident Response (NSIR) is responsible for assessing the security aspects of the design. Their assessment of the resistance to threats is addressed with the licensee after the design is complete. The staff stated that the review performed by the Office of Nuclear Reactor Regulation focuses on the ability of the design to perform its reactor protection and engineered safeguards functions.

We do not agree that separate reviews of the DI&C systems in isolation are prudent. The September 9, 2005, Staff Requirements Memorandum (SRM) stated that advanced nuclear power plants should integrate the expectations for security and safety. It is reasonable to expect the same integration to apply to new DI&C system designs that are developed for operating plants. Delivered systems could result in a design that is not amenable to incorporating protection to threats. The staff should develop an integrated process that ensures that the DI&C system will be able to meet, with reasonable assurance, the combined requirements associated with plant safety and cyber security threats.

We commend the staff for their efforts to bring this important ISG to completion. The staff has been responsive to our comments and issues. We look forward to future interactions with the staff as their pilot program and refinements continue.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

References:

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-Draft ISG-6, "Licensing Process," Draft 50, 08/17/2010 (ML102310002)

2. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-Draft ISG-6, "Licensing Process," 01/14/2009 (ML090130273)

3. SRM-SECY-05-0120, "Security Design Expectations for New Reactor Licensing Activities," 09/09/2005 (ML052520334)

We commend the staff for their efforts to bring this important ISG to completion. The staff has been responsive to our comments and issues. We look forward to future interactions with the staff as their pilot program and refinements continue.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

References:

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-Draft ISG-6, "Licensing Process," Draft 50, 08/17/2010 (ML102310002)

2. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-Draft ISG-6, "Licensing Process," 01/14/2009 (ML090130273)

3. SRM-SECY-05-0120- Security Design Expectations for New Reactor Licensing Activities, 09/09/2005 (ML052520334)

Distribution:
See next page

Accession No: ML102850357 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☐ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	CSantos	EHackett	EHackett for SAbdel-Khalik
DATE	10/20/10	10/20/10	10/21/10	10/21/10	10/21/10

OFFICIAL RECORD COPY

Letter to the Honorable Gregory B Jaczko, Chairman, NRC, from Said Abdel-Khalik, Chairman, ACRS, dated October 21, 2010

SUBJECT: DRAFT FINAL DIGITAL INSTRUMENTATION & CONTROL INTERIM STAFF GUIDANCE-06: LICENSING PROCESS

Distribution:
ACRS Staff
ACRS Members
B. Champ
A. Bates
S. McKelvin
L. Mike
J. Ridgely
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter