December 7, 2010

Dr. Said Abdel-Khalik, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: RESPONSE TO ADVISORY COMMITTEE ON REACTOR SAFEGUARDS RECOMMENDATIONS ON DRAFT FINAL DIGITAL INSTRUMENATION AND CONTROL INTERIM STAFF GUIDANCE-06, "LICENSING PROCESS"

Dear Dr. Abdel-Khalik:

In your letter dated October 20, 2010 (Agencywide Documents Access and Management System Accession No. ML102850357), you summarized the views of the Advisory Committee on Reactor Safeguards (ACRS or the Committee) on the staff's interim staff guidance (ISG) on licensing digital upgrades to safety systems in existing nuclear power plants. The staff of the U.S. Nuclear Regulatory Commission (NRC) is committed to working closely and cooperatively with the Committee to resolve the recommendations presented in the ACRS letter.

Your October 20, 2010, letter included the recommendations given below, for which the staff has provided associated responses.

ACRS Recommendation No. 1

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

NRC Response

ISG-6 has been revised to incorporate Recommendations 2 and 3 as described below. The staff plans to issue ISG-06 in late 2010 or early 2011, following review by the Digital Instrumentation and Control (Digital I&C) Steering Committee and the Office of the General Counsel.

ACRS Recommendation No. 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.

NRC Response

Section B and other sections have been revised to clearly indicate that detailed reviews should be performed to ensure that regulatory criteria have been met. For example:

Clarification was added to Section A, “Introduction,” which now states: “Reviews should confirm that the system meets regulatory requirements. Review of any safety system implementation should focus on component and system requirements, system design, and associated validation analyses. Review of digital computer-based systems should also include confirming the acceptability and correct implementation of life-cycle activities.”

The wording in Section B.1, “Background,” identified by the ACRS has been revised to state: “While the NRC staff does not perform an independent design review of the DSS [Digital Safety System], the staff reviews the system design (including hardware and software architectures) and the design process to determine that the design meets regulatory requirements (e.g., independence/redundancy, deterministic behavior, defense-in-depth and diversity,…) and that the process is of sufficient high quality to produce systems and software suitable for use in safety-related applications in nuclear power plants.”

ACRS Recommendation No. 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.

NRC Response

Section D and other sections have been revised to emphasize the review from an integrated hardware and software perspective. For example:

Section D.1.1, “Scope of Review,” now states: “Reviewing the system description allows the NRC staff to understand how the components of the system interact to accomplish the design function; this description should be from an integrated hardware/software perspective in order to develop a clear understanding of the overall complexity of the system. Understanding the system provides a solid foundation for the subsequent detailed reviews and evaluation against the acceptance criteria.”

Section D.9.4.2 and associated subsections address the evaluation performed to ensure that the safety system implements the functional and performance requirements. Section D.9.4.2 now states: “Clause 5 of [Institute of Electrical and Electronics Engineers, Inc.] IEEE Std. 603-1991 requires that the safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established by design basis events. This evaluation should confirm that the general functional requirements have been appropriately allocated to the various system components. The review in this regard should confirm that the system design fulfills the system design basis requirements established; this review should be from an integrated hardware/software perspective.”

Section D.10.1 now states: “Within the context of IEEE Std. 7-4.3.2-2003, the term computer is a system that includes computer hardware, software, firmware, and interfaces.”

Section C.1, “Process Overview,” now states: “It is expected that systems with greater complexity will require greater review effort.”

ACRS Recommendation No. 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 Digital I&C performance.

NRC Response

As part of ongoing research under the fiscal year (FY) 2010 - FY 2014 Digital Systems Research Plan, the Digital I&C Branch of the Office of Nuclear Regulatory Research is investigating the efficacy of Software Failure Modes and Effects Analysis as a method for identifying faults leading to system failures impairing a safety function. This effort has involved expert elicitation from numerous international software system engineering experts from both nuclear and non-nuclear domains. The Staff intends to brief the ACRS Digital I&C Subcommittee on the outcomes and findings of this research.

ACRS Recommendation No. 5

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

NRC Response

The process for reviewing Digital I&C systems associated with plant safety currently is focused on establishment of secure development and operational environments (SDOE) for DSS. During DSS licensing reviews, the staff focuses on ensuring that the development environment for the digital safety system is secure from the introduction of unwanted, unneeded, and undocumented code; the staff will evaluate the applicant's controls placed on its development.

In addition, staff guidance and licensing criteria ensures that a secure operational environment for DSS has been established. During licensing reviews, the staff verifies that a secure operational environment provides protection from undesirable behavior from connected systems and from inadvertent access to the DSS. The staff evaluates the adequacy of the design provisions to address the identified undesired behaviors and verify that the design features were appropriately addressed throughout the development process. The staff also evaluates the adequacy of the provisions and associated supporting design features to preclude inadvertent access to the system.

Any design provisions of a DSS that are intended to serve both a SDOE and cyber security functions would only be evaluated as part of the licensing review for its ability to satisfy the SDOE functions. Any design features that only implement a cyber security function are reviewed only for potential impact on the reliable operation of the digital safety system.

Once the DSS is approved through the licensing process, licensees are required to protect it from cyber security threats by satisfying the provisions of Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," (the NRC Cyber Security Rule). Under the Cyber Security Rule, and as a condition of its license, each licensee must submit a cyber security plan (CSP) to the NRC

for review and approval. The submitted CSP describes additional testing the licensees must perform to ensure that the DSS meets the combined plant safety and cyber security protection requirements prior to installation. The CSP also describes the defense-in-depth architecture the licensee will use to protect the DSS, the programmatic elements of its cyber security program (which includes ongoing design reviews, vulnerability assessments, and identification of cyber threat and attack vectors) and the security controls it will implement. Licensees committed, in their respective CSPs that system developers and integrators of an acquired DSS will create, implement, and document a security test and evaluation plan to ensure that the DSS assets are free from known, testable vulnerabilities and malicious code. The CSP states that this will be accomplished by identifying and eliminating vulnerabilities that may emerge with newer technologies.

Additionally, licensees commit in their CSPs to require the DSS developer to maintain the integrity of the acquired system until the product is delivered to the licensee. Licensees further commit in their CSPs to review and document that security requirements are verified and validated, that any security controls implemented in the product meet the requirements of their CSP, and are tested to ensure that they are effective against cyber attacks, up to and including the design basis threat (DBT).

Licensees also commit in their CSPs to perform security testing of any acquired DSS component before it can be installed in an operational environment, and ensure that they identify any known vulnerability types and address all of the known attack methods the DBT may use. This includes testing the DSS component, any security devices used to protect it, security controls associated with the component, and any other assets to ensure that they do not compromise the component or interconnected system prior to installation. Furthermore, the licensee commits to perform vulnerability scans against DSS components in their integrated state and correct and eliminate any discovered vulnerabilities before the components are put into operation, as well as test them on a regular basis for any new vulnerabilities. (Additional discussion of this is provided in Sections 12 and 13 of RG 5.71.)

Inspection procedures and associated guidance are being developed for the cyber security oversight program. The commitments described above are performed by the licensee prior to DSS operation at the plants. Therefore, the NRC's approach to safety and security begins with design reviews to ensure that the DSS performs its function, assessments of the licensee CSP to ensure it contains the necessary elements for successful development and operation of a security program, and development of an NRC inspection program to verify that the implementation is correct and that the program protects against new vulnerabilities and threat actor capabilities.

The NRC appreciates the comments and recommendations provided by ACRS. We look forward to continuing to work with the Committee.

Sincerely,

/RA Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

The NRC appreciates the comments and recommendations provided by ACRS. We look forward to continuing to work with the Committee.

Sincerely,

/RA Martin J. Virgilio for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Svinicki
Commissioner Apostolakis
Commissioner Magwood
Commissioner Ostendorff
SECY

DISTRIBUTION: G20100651/EDATS: OEDO-2010-0848

Non-public

ACRS Reading file	RidsNsirOd	RidsNrrOd
RidsAcrsAcnw_MailCTR	RidsNrrMailCenter	RidsEdoMailCenter
RidsNrrDe	RidsNroDe	RidsResOd
RidsOgcMailCenter	AFrazier, EDO	

ADAMS Accession Nos.: Pkg: ML103130170 Incoming: ML102950283; Ltr; ML103130193; * via email

OFFICE	NRR/DE/EICB	Tech Ed: *	D: NRO/DE *	D:NRR/DE	NRR/DE	NRR/DE/EICB
NAME	NCarte	KAzariah-Kribbs	TBergman	SArndt	LJames	WKemper
DATE	11/16/10	11/10/10	11/30/10	11/06/10	11/16/10	11/16/10

OFFICE	D:NRR/DE	D:RES/DE	D:NSIR/DSP	OD:NRR	EDO
NAME	PHiland	M.Case (SRichards for)	R.Correia	ELeed (JGrobe for)	RBorchardt (MVirgilio for)
DATE	11/17/10	11/18/10	11/18/10	12/2/10	12/7/10

OFFICIAL RECORD COPY