UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 21, 2018

Michael L. Corradini, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: RESPONSE TO THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS' SECOND LETTER ON DRAFT DIGITAL INSTRUMENTATION AND CONTROLS INTERIM STAFF GUIDANCE DI&C-ISG-06, "LICENSING PROCESS," REVISION 2

Dear Mr. Corradini:

During the 655th meeting of the Advisory Committee on Reactor Safeguards (ACRS or the Committee), held on July 11–13, 2018, the Committee met with representatives of the U.S. Nuclear Regulatory Commission (NRC) staff to review the draft Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG) DI&C-ISG-06, "Licensing Process," Revision 2. The DI&C Systems Subcommittee reviewed draft DI&C-ISG-06, Revision 2, and the other documents referenced by the ISG during meetings on May 17, 2018, and June 20, 2018. The Committee stated its views on draft DI&C-ISG-06, Revision 2, in letters to me dated July 18, 2018, and November 8, 2018 (Agencywide Documents Access and Management System (ADAMS) Accession Nos. ML18198A442 and ML18312A392, respectively). This letter is in response to the Committee's letter dated November 8, 2018.

Background

In its letter to me dated July 18, 2018, the Committee provided its conclusion and recommendation regarding draft DI&C-ISG-06, Revision 2. The ACRS letter indicated that DI&C-ISG-06, Revision 2, should be issued for public comment; the draft final DI&C-ISG-06, Revision 2, should be provided for ACRS review following resolution of public comments; and the NRC staff should address hardware configuration control and management issues before final publication.

The discussion portion of the letter also addressed the Committee's concerns regarding Control of Access. The letter noted that the NRC staff has ensured that four of the five fundamental digital design principles are addressed in the ISG. However, the ACRS remained concerned that the fifth critical fundamental design principle for the architecture design of DI&C applications, Control of Access, is not included. The ACRS noted that in addition to using design approaches and administrative controls to restrict internal plant access to systems, Control of Access also means preventing remote electronic access to in-plant systems and networks from sources external to the plant. The ACRS also noted that plant and system data transmission should be configured to be one-way from in-plant to external recipients using only hardware-based processes, which neither use nor are configured by software. The Committee noted that this is a continuing concern and urged the staff to formally incorporate this principle into the licensing design evaluation process.

The NRC issued draft DI&C-ISG-06, Revision 2, for comment on August 7, 2018, and the public comment period closed on September 6, 2018. By letter dated September 11, 2018 (ADAMS Accession No. ML18214A140), the NRC staff responded to the ACRS about the formal recommendations listed in the letter.

In the ACRS letter to me dated November 8, 2018, the Committee requested that the staff provide the documented basis for not incorporating the fifth critical fundamental design principle for the architecture design of DI&C applications (Control of Access) and provide any additional changes that would help ensure the prevention of remote electronic access to in-plant systems and networks from sources external to the plant.

Staff Response

The ACRS concern relates to Control of Access in the context of the safety review and also in the context of cyber security. As explained in more detail in the enclosed response, DI&C-ISG-06 *does* address the Control of Access principle in the safety review of proposed DI&C modifications, and Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3, issued July 2011 (ADAMS Accession No. ML102870028), provides guidance on this principle with respect to both internal and external access. While not designated as a fifth fundamental design principle, the staff has revised DI&C-ISG-06 to explicitly refer to appropriate guidance in RG 1.152.

NRC safety regulations do not require plant and system data transmission to be configured to be one-way from in-plant to external recipients using only hardware-based processes. Having said that, RG 5.71, "Cyber Security Programs for Nuclear Facilities," issued January 2010 (ADAMS Accession No. ML090340159), provides guidance regarding the requirements of 10 CFR 73.54 and recommends that licensees implement "one-way data flows using hardware mechanisms" (RG 5.71, Appendix B.1.4). As described in licensees' NRC approved cyber security plans, the operating reactor licensees implemented deterministic (hardware-based) data diodes to enforce the one-way data flow. The NRC has inspected and accepted the implementation of the deterministic data diodes at all operating nuclear power plants. Accordingly, any changes to this hardware-based data diode that would reduce the effectiveness of the security (isolation), would require a license amendment under 10 CFR 50.54(p)(1). Further, the staff has issued guidance in DI&C-ISG-04, "Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, dated March 6, 2009 (ADAMS Accession No. ML083310185), which states that "[o]n-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment." The enclosed response explains the regulatory treatment of cybersecurity issues, which is governed by 10 CFR 73.54 and 10 CFR 50.54(p).

Path Forward

In response to your concern regarding Control of Access, the NRC staff has revised DI&C-ISG-06 to add a note stating that the NRC reviewer for the license amendment request should communicate with the Office of Nuclear Security and Incident Response staff any cyber security concerns or design features identified during the review of the DI&C modification (e.g., the failure to ensure one way data flows using hardware mechanisms). The staff still intends to issue the final DI&C-ISG-06 this December.

The NRC staff appreciates the Committee's thorough review of draft DI&C-ISG-06, Revision 2.

Sincerely,

/RA Michael R. Johnson Acting for/

Margaret M. Doane
Executive Director
for Operations

Enclosure:
As stated

cc: Chairman Svinicki
Commissioner Baran
Commissioner Burns
Commissioner Caputo
Commissioner Wright
SECY

SUBJECT: RESPONSE TO THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS' SECOND LETTER ON DRAFT DIGITAL INSTRUMENTATION AND CONTROLS INTERIM STAFF GUIDANCE, DIGITAL I&C-ISG-06, "LICENSING PROCESS," REVISION 2 DATED December 21, 2018

DISTRIBUTION: OEDO-18-00600
PUBLIC
JGolla, NRR
MWaters, NRR
DMorey, NRR
SDarbali, NRR
RStattel, NRR
DZhang, NRR
JPaige, NRR
RidsNrrLADHarrison
RidsEdoMailCenter
RidsOgcMailCenter
RidsNrrDlp
RidsNrrDlpPlpb
RidsNroOd
RidsResOd
RidsNrrOd
RidsNrrDe
RidsNrrDeEicb
RidsAcrsAcnw_MailCTR

ADAMS Accession Nos.
PKG ML18318A116
Incoming ML18312A392
Response LTR ML18318A011 ***via e-mail** **EDO-002**

OFFICE	NRR/DLP/PLPB/PM	NRR/DLP/PLPB/LA*	NRR/DE/EICB/BC
NAME	JGolla	DHarrison	MWaters
DATE	11/28/18	11/20/18	11/28/18
OFFICE	NRR/DLP/PLPB/BC	NRR/DE/D	NRR/DLP/D
NAME	DMorey	EBenner	LLund
DATE	11/26/18	11/28/18	11/28/18
OFFICE	NSIR/DPCP/D	OGC – NLO*	QTE*
NAME	SHelton	RWeisman	JDougherty
DATE	11/29/18	12/04/18	11/27/18
OFFICE	NRR/D	EDO	
NAME	HNieh	MDoane (MJohnson for)	
DATE	12/18/18	12 / 21/18	

OFFICIAL RECORD COPY

RESPONSE TO THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS' COMMENT ON CONTROL OF ACCESS AND HOW IT IS ADDRESSED IN DI&C-ISG-06

The Advisory Committee on Reactor Safeguards (ACRS or the Committee) letter dated November 8, 2018 (Agencywide Documents Access and Management System Accession (ADAMS) No. ML18312A392), highlighted the Committee's concerns that Control of Access is not included in Digital Instrumentation and Controls (DI&C) Interim Staff Guidance (ISG) DI&C-ISG-06, "Licensing Process," Revision 2. However, DI&C-ISG-06, Section D.6, "Compliance/Conformance Matrix for IEEE Standards 603-1991 and 7-4.3.2- 2003," references Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Clause 5.9, "Control of Access," which states the following:

> The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

DI&C-ISG-06 Section D.6 provides guidance for evaluating IEEE Std 603-1991 criteria. The U.S. Nuclear Regulatory Commission (NRC) staff can develop an IEEE Std 603-1991 compliance matrix, if one is not provided by the licensee, that includes a compliance position for Control of Access and points to the place within the license amendment request (LAR) that would justify this position. Table D.1 in Section D.6 of DI&C-ISG-06, Revision 2, is an example of how the staff could create such a matrix to show compliance with each of the clauses in IEEE Std 603-1991, including Clause 5.9 on Control of Access.

DI&C-ISG-06, Section D.6, Table D.1, references DI&C-ISG-06 Section D.8, "Secure Development and Operational Environment," as the section that addresses Control of Access. Section D.8 contains the evaluation criteria for secure development and operational environment (SDOE). This guidance refers to Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3, issued July 2011 (ADAMS Accession No. ML102870028). Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std. 7-4.3.2," to NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," also references RG 1.152 as guidance for Control of Access.

Therefore, DI&C-ISG-06, by way of the review guidance in RG 1.152, includes Control of Access.

Prevention of Remote Electronic Access

The ACRS letter states the following:

> In addition to using design approaches and administrative controls to restrict internal plant access to systems, Control of Access also means preventing remote electronic access to in-plant systems and networks from sources external to the plant.

DI&C-ISG-06, Section D.8, relies on the staff's SDOE evaluation using RG 1.152, Revision 3. RG 1.152, Regulatory Position 2.1, "Concepts Phase," states, in part, the following **[emphasis added]**:

> **The licensee should not allow remote access to the safety system.** For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function **from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).**

Therefore, DI&C-ISG-06, Section D.8, by way of the review guidance in RG 1.152, addresses the ACRS concern regarding Control of Access, as it pertains to the safety aspects of prevention of remote electronic access to in-plant systems and networks from sources external to the plant. As stated in RG 1.152, the safety aspects of external access relate to the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life cycle that could degrade its reliable operation. RG 1.152, Revision 3, Section B, explains that cybersecurity is not a subject of the safety review.

Use of Only Hardware-Based Processes

The ACRS letter states that "plant and system data transmission should be configured to be one-way from in-plant to external recipients using only hardware-based processes, which neither use nor are configured by software."

The NRC regulation pertinent to this subject is 10 CFR 50.55a(h), which incorporates by reference the IEEE Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." As indicated above, IEEE Std 603-1991, Clause 5.9, "Control of Access," requires administrative controls, supported by provisions within the safety systems, or by provision in the generating station design to control access to safety system equipment. IEEE Std 603-1991 does not require the exclusive use of hardware-based processes to control access to safety system equipment. Nonetheless, NRC guidance recommends the use of hardware mechanisms to control access to safety system equipment.

Specifically, RG 5.71, "Cyber Security Programs for Nuclear Facilities," issued January 2010 (ADAMS Accession No. ML090340159), provides guidance to applicants and licensees on satisfying the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communication Systems and Networks." RG 5.71 states that the licensee or applicant is responsible for "implementing one-way data flows using hardware mechanisms" (Appendix B.1.4). However, DI&C-ISG-06 describes the staff's process for determining whether a LAR meets safety requirements and does not include security concerns regulated under 10 CFR Part 73, "Physical Protection of Plants and Materials."

Further, DI&C-ISG-04, "Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, dated March 6, 2009, contains the following clauses that address the Committee's recommendation:

> On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment.

> The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.

RG 1.152 provides guidance for securing plant data communication systems. RG 1.152, Section B, states, in part, the following **[emphasis added]**:

> Controls should address access through both network connections and maintenance equipment. Additionally, **the design of the plant data communication systems should ensure that the systems do not present an electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators**….
>
> The considerations for **hardware access control** should include physical access control, configuration of modems, **connectivity to external networks, data links**, and open ports. The licensee can provide an SDOE for digital safety systems by (1) designing features that will meet the licensee's secure operational environment requirements for the systems, (2) … (3) **maintaining a secure operational environment for digital safety systems in accordance with the station administrative procedures and the licensee's other programs to protect against unwanted and unauthorized access or changes to these systems**.

Additionally, RG 1.152, Regulatory Position 2.5, "Test Phase," states, in part, the following **[emphasis added]**:

> Testing includes **system hardware configuration (including all connectivity to other systems, including external systems)**....
>
> T**he developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity.**

Thus, RG 5.71, RG 1.152, and DI&C-ISG-04 provide guidance that addresses the Committee's concerns regarding Control of Access.

Cyber Security Reviews

In regard to the cyber security program, the regulatory framework for the protection of DI&C against malicious access and attacks is addressed by the programmatic approach for the protection of digital computer and communication systems and networks under the NRC regulations in 10 CFR Part 73, which requires power reactor licensees to implement a cyber security program (CSP). Specifically, 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," directs all power reactor licensees to implement a CSP that is incorporated as a component of the facilities' physical protection programs. The regulation requires licensees to submit a CSP for the NRC's review and approval. The CSP must describe how the licensee-implemented CSP will comply with 10 CFR 73.54. License conditions govern the implementation of the physical protection program, which includes the CSP, and changes to the CSP are governed by the requirements of 10 CFR 50.54(p).

In the CSPs, licensees included a defensive architecture that isolates safety and security critical digital assets from external networks using a deterministic boundary device that enforces one-way data flow. Specifically, the licensees implemented deterministic (hardware-based) data diodes to enforce the one-way data flow. The NRC has inspected and accepted the implementation of the deterministic data diodes at all operating nuclear power plants. Any change to the isolation of safety and security critical digital assets from external networks that would reduce the effectiveness of the CSP would require a license amendment under 10 CFR 50.54(p)(1). Nonetheless, a safety review of a proposed DI&C modification does not need to determine whether the safety systems are isolated from the external networks for cybersecurity purposes. Moreover, through inspection, the NRC verified and validated that licensees have already implemented deterministic data diodes to isolate the plant networks from external networks, and licensees rely on them for cybersecurity purposes.

DI&C-ISG-06, via the guidance in RG 1.152, notes that the licensee needs to comply with 10 CFR 73.54 and identifies RG 5.71 as an acceptable way of meeting 10 CFR 73.54. As mentioned above, RG 5.71 does state that the licensee or applicant is responsible for "implementing one-way data flows using hardware mechanisms." Verification of the implementation of RG 5.71 guidance is performed by the Office of Nuclear Security and Incident Response (NSIR) through cyber security program reviews and inspections. The I&C staff will communicate with NSIR any cyber security concerns or design features identified during the review of the DI&C modification (e.g., the use of one-way data flows using hardware mechanisms).

Proposed Changes to DI&C-ISG-06 to Address the ACRS Concern (underlined)

D.8 Secure Development and Operational Environment

D.8.1 Information To Be Provided

The LAR should demonstrate that the proposed DI&C system is adequately robust to perform its safety function under design-basis conditions, including in normal and adverse environments. The LAR should provide information describing a secure environment, including any issues that may affect the secure environment and the DI&C equipment.

For the Tier 1, 2, and 3 Review Process, the LAR should provide information describing the vulnerability assessment and the SDOE controls that address Regulatory Position 2.1, "Concepts Phase," through Regulatory Position 2.5, "Test Phase," of RG 1.152.

For the Alternate Review Process, the LAR should provide the following information to address RG 1.152:

a. a description of the vulnerability assessment;
b. a description of the secure development environment controls; and
c. the System Requirements Specification (see Section D.2.2.2 of this ISG) for the Sequence of Events (SOE) controls.

All SDOE and software information identified in RG 1.152, Regulatory Position 2, including the test phase specifications and results validating the requirements for the SOE, should be available for NRC staff review. The need to submit any of this information should be determined during the licensing review.

Documentation detailing how the licensee implemented (or will implement, in the case of the Alternate Review Process) SDOE controls should be available for NRC staff review.

D.8.2 Evaluation

The reviewer should determine whether the LAR conforms to the guidance of RG 1.152, Regulatory Position 2, for the SDOE of the system under review, and complies with the requirements of Clause 5.9 of IEEE Std 603-1991, Control of Access. For Tier 1 and the Alternate Review Process, the review is limited to the application software and hardware.

The NRC staff should review the licensee's vendor- and system-specific vulnerability assessment description and verify that the assessment identifies those vulnerabilities that could affect the secure development and reliable and secure operation of the digital safety system. RG 1.152, Section B, page 5, discusses vulnerabilities that could affect the reliability of the system. RG 1.152, Section C, Regulatory Position 2.1, contains guidance for performing the vulnerability assessment.

The NRC staff should review the information provided to determine that the digital safety system:

a. was designed in a secure development environment, and was (or will be, in the case of the Alternate Review Process) developed, and tested in a secure development environment; and
b. will be protected from inadvertent actions in an SOE as defined in RG 1.152.

The I&C staff in NRR reviews the safety aspects of the LAR while NSIR staff evaluates the adequacy of cyber security features for compliance with 10 CFR 73.54. The I&C staff should communicate with NSIR any cyber security concerns or design features identified during the review of the DI&C modification (e.g., the use of one-way data flows using hardware mechanisms).