FINAL REPORT FOR THE STRATEGIC ASSESSMENT OF THE

DIGITAL INSTRUMENTATION AND CONTROL REGULATORY INFRASTRUCTURE

I. INTRODUCTION

In the Staff Requirements Memorandum (SRM) to SECY-15-0106, "Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Standard, 603-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16056A614), the Commission directed the Nuclear Regulatory Commission (NRC) staff to develop an integrated strategy to modernize the NRC's digital instrumentation and control (I&C) regulatory infrastructure. In response to this SRM, the NRC staff developed and subsequently revised the "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure," (ADAMS Accession No. ML19025A312). This plan outlines tactical and strategic activities to implement improvements to the digital I&C regulatory infrastructure. Within this integrated action plan (IAP), Modernization Plans (MPs) #1-4A address the tactical activities identified to modernize the digital I&C regulatory infrastructure. MP #4B, "Broad Assessment for Modernization of Digital Instrumentation and Regulatory Infrastructure," describes how the NRC staff will perform a strategic assessment of the current overall digital I&C regulatory infrastructure and develop recommendations based on the assessment results to modernize the digital I&C regulatory infrastructure over the longer-term. This report documents the recommendations based on the results of the MP #4B strategic assessment.

II. SCOPE AND ASSESSMENT METHODOLOGY

The strategic assessment focused on evaluating the current digital I&C regulatory infrastructure while considering other ongoing and completed NRC efforts on digital I&C including (1) the tactical activities in MP #1-4A; (2) International Electrotechnical Commission (IEC) standards endorsement project, (3) I&C research activities such as those on risk-informed approaches, common cause failure (CCF), and embedded digital devices; (4) NUREG-0800, Standard Review Plan (SRP) modernization initiative; and (5) advanced reactor regulatory framework development effort (i.e., Draft Guide (DG)-1353, "Guidance for Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors"). To avoid duplication in effort, the scope of the strategic assessment is limited to further digital I&C regulatory improvements that will assist operating reactors performing digital I&C modifications and vendors submitting I&C platform topical reports for NRC approval in their demonstration of safety and security.

In performing the strategic assessment, the NRC staff evaluated lessons learned from previous licensing reviews, insights from other safety-critical industries, and international perspectives. The NRC staff also solicited input from internal and external stakeholders to inform the focus of this assessment. This includes impediments to implementing digital technology that were identified by industry stakeholders. The results of stakeholder inputs are under ADAMS Accession No. ML19025A307. During the assessment process, the NRC staff engaged industry stakeholders via public meetings held on January 31, 2019, April 4, 2019, and November 20, 2019, to gain additional feedback and to present initial assessment results. Based on the results of the strategic assessment, the NRC staff developed recommendations to improve the current digital I&C regulatory infrastructure.

To allow for efficiency during implementation, these recommendations are focused on regulatory guidance improvements that do not require rulemaking to implement.

III. RECOMMENDATIONS

The NRC and industry have made significant progress in tactically improving the regulatory framework to support future digital I&C upgrades in the operating fleet under Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.59 and license amendments. Industry has indicated that several upgrades are underway and planned using the improved framework. Based on the strategic assessment results, including stakeholder feedback, the NRC staff developed one broad recommendation to restructure regulatory guidance to further improve NRC's regulatory infrastructure. The NRC staff developed three specific recommendations that are coupled with the broad recommendation. The bases for these recommendations are described in the subsections below.

A. Broad Recommendation

The NRC staff recommends updating and reorganizing the digital I&C regulatory guidance to achieve a simpler and more effective digital I&C regulatory infrastructure. The NRC's regulatory guidance framework is primarily composed of (1) licensing guidance (e.g., regulatory guides (RGs)) that provides one acceptable way for licensees to meet NRC regulations and (2) NRC staff review guidance (e.g., the SRP including branch technical positions (BTPs), NUREGs) that provides review procedures and acceptance criteria for evaluating license applications. Many of the I&C RGs, including those specific to the use of digital technology, endorse outdated standards. For example, RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3 endorses the 2003 revision of the Institute of Electrical and Electronics Engineers (IEEE) Std 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" while the latest revision to this standard was issued in 2016. Endorsing the latest revision to this standard, allows licensees and I&C platform vendors to more readily take advantage of the improved criteria within the new revision that address advances in digital technologies. Maintaining the endorsement of significantly older and obsolete consensus standards creates inefficiencies for NRC staff, licensees, and I&C platform vendors and potentially impedes the use of latest revisions of standards.

Further, the broader I&C community of vendors and developers are transitioning away from the traditional microprocessor-based technologies. Licensing guidance gaps exist for newer digital I&C technologies such as criteria for use of field programmable gate arrays or embedded digital devices. International standards are available for review and endorsement to address these gaps. Similar issues exist for NRC staff review guidance that are highly focused on microprocessor and software-based digital I&C technologies. The last major update to the NRC's SRP, Chapter 7, Instrumentation and Controls, was completed in 2007.

The structure of the NRC's digital I&C regulatory guidance prevents effective navigation and use of the available guidance. This issue originated from the creation of regulatory guidance to address new digital I&C technologies and topics introduced by evolving industry needs, without significant consideration of the structure of the overall I&C regulatory guidance. In addition, a significant portion of individual NRC regulatory guides endorse individual IEEE and International Society of Automation (ISA) standards, and therefore mirror the standard framework chosen by these codes and census bodies. In implementing such an ad hoc approach to creation of regulatory guidance, some of the guidance documents created address topics that could have been integrated or consolidated into one guidance document. For example, RGs 1.168 through

1.173 were created to endorse seven individual IEEE standards related to seven inter-related aspects of software development and verification and validation (V&V). Creation of one RG or revising RG 1.152 to accomplish the same goals of demonstrating adequate software quality can be more efficient and effective for future license applications. Further, since some of the regulatory guidance were created as staff review guidance without a companion regulatory guide, licensees and I&C platform vendors have had to rely on guidance intended to support NRC staff safety evaluations. This is evident in licensees' use of BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" as licensing guidance for addressing software CCFs in digital I&C systems. Therefore, the NRC staff recommends the following process to improve the overall regulatory guidance for digital I&C:

1. Establishing an overall vision for the digital I&C regulatory guidance infrastructure to allow licensees, I&C platform vendors, and NRC staff to effectively navigate and use regulatory guidance; and

2. Restructuring the existing regulatory guidance in accordance with these guidelines by performing, at the minimum, the following activities:

    a) identify gaps, inconsistencies, and duplications in the current regulatory guidance; and

    b) develop guidance to address any identified gaps, correct any identified inconsistencies, and consolidate any duplications in guidance

The NRC staff considers this broad recommendation to be the foundation for implementing the specific recommendations described in the subsections below.

B. Specific Recommendation on Use of Interim Guidance

The NRC staff recommends incorporation of the current set of digital I&C interim guidance into durable I&C regulatory guidance and minimize future use of interim guidance. Interim guidance encompasses many forms of NRC regulatory guidance, including interim staff guidance (ISG), regulatory issue summary (RIS), and BTPs. The NRC staff developed seven digital I&C related ISGs in the late 2000s as part of a collaborative NRC and industry initiative to improve clarity and guidance for new and operating reactor industry needs at that time. Although the original intent for using these interim vehicles was to increase efficiency during the issuance process and allow piloting of the guidance before transferring the interim guidance to durable guidance, recent lessons learned show use of several interim guidance documents is not efficient. While some of these ISGs have been transferred to durable guidance, several digital I&C ISGs continue to exist as interim guidance. This includes DI&C-ISG-06, "Licensing Process," which was revised in 2018 at the request of industry stakeholders under MP #4A to enhance the digital I&C license amendment request review process. The current process for issuing and revising ISGs does not benefit from increases in efficiency as compared to issuing or revising durable guidance since the same process steps apply to both. Further, following any piloting or use of the interim guidance, the NRC staff still needs to incorporate the interim guidance into durable guidance, which creates additional work without comparable benefits. Therefore, the NRC staff recommends developing durable licensing and staff review guidance and minimizing the use of interim guidance. In addition, the NRC staff recommends transferring existing interim guidance such as the digital I&C ISGs to durable guidance (e.g., RGs, the SRP, etc.).

This recommendation should be implemented as part of the broad recommendation for restructuring the I&C regulatory guidance infrastructure.

C. Specific Recommendation on Development of Guidance for Architecture

The NRC staff recommends consolidating and clarifying NRC staff review guidance and developing new licensing guidance for I&C architecture to support licensees in their demonstration of safety and regulatory compliance. The I&C architecture is the organizational structure of I&C systems important to safety. Establishing an effective overall I&C architecture supports maintaining defense-in-depth, including independence among I&C systems, which provide protection against CCF hazards and propagational hazards. The NRC licensing reviews can be more efficient when licensees provide information on the overall I&C architecture and individual I&C systems architecture. Specifically, this information facilitates identification of system internal and external interfaces, and boundaries among various echelons of I&C systems, which supports the NRC staff's determination on whether independence requirements are met for these systems. The NRC has review guidance in DI&C-ISG-06, Revision 2, the SRP, Chapter 7, and the Design Specific Review Standard for NuScale, Chapter 7. However, the NRC staff has recognized that distributing this guidance among many different documents creates inefficiencies for NRC I&C staff reviewers. In addition, the NRC does not have any licensing guidance on acceptable I&C architectures for meeting regulatory requirements which licensees can consider when designing digital I&C systems or preparing licensing application submittals for these systems. This gap in licensing guidance created inefficiencies during past licensing reviews. Therefore, to increase licensing efficiencies, the NRC staff recommends reviewing and endorsing an existing standard with criteria for establishing an I&C architecture as licensing guidance for licensees. This recommendation is aligned with the industry stakeholder's feedback provided during the MP #4B public meetings.

International Electrotechnical Commission (IEC) 61513, "Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems," Edition 2, provides criteria for establishing an overall I&C architecture in Section 5 and individual I&C systems architecture in Section 6.2.2.3.2. The criteria within Section 6.2.2.3.2 are more applicable to licensees of operating reactors performing digital modifications to individual I&C systems. For licensees that intend to modernize multiple I&C systems or human systems interfaces such as the main control room displays and controls, the criteria within Section 5 of IEC 61513 provide additional relevant guidance. The NRC staff recommends developing a new RG or revising an existing RG such as RG 1.152 to endorse these two sections within IEC 61513 for I&C architecture guidance. Further, the NRC staff recommends reviewing existing staff review guidance on I&C architecture to determine the best approach for consolidating this information. The implementation of this recommendation should take into consideration the broad recommendation for restructuring the I&C regulatory guidance infrastructure to ensure this new guidance integrates appropriately with the overall I&C regulatory guidance framework.

D. Specific Recommendation on Revising Guidance for Software to Incorporate a Graded Approach

The NRC staff recommends revising the current regulatory guidance to provide criteria for applying a graded approach for software used in digital I&C safety-related systems. The NRC's current regulatory guidance for software used in digital I&C safety-related systems does not distinguish between software that is of high safety significance (e.g., software for accomplishing reactor trip or engineered safety features actuation functions) versus software with low safety

significance (e.g., software for accomplishing post accident monitoring or heating, ventilation and air conditioning functions). Although the SRP, Chapter 7, and BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," allow a graded approach to be used when reviewing safety-related software, these documents do not provide guidance on how to apply such a graded approach. Further, the NRC's current licensing guidance for software development (e.g., RG 1.168 through RG 1.173) does not include a graded approach for applying the criteria within the guidance. Licensees may therefore apply the same degree of rigor and providing the same level of detail for software that is of high safety significance versus that of low safety significance. Further, IEEE Std 1012-2004, "IEEE Standard for Software Verification and Validation" defines a four-level method of quantifying software integrity levels (SILs), in which Level 4 is the highest and Level 1 the lowest SIL. The standard uses SIL to apply a graded approach on the minimum V&V tasks to be performed. However, the NRC's endorsement of this standard in RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Using in Safety Systems of Nuclear Power Plants," does not adopt the graded approach defined in the standard. Based on the state of knowledge and limited risk insights at the time, RG 1.168 specified that software used in nuclear power plant safety-related systems should be assigned software integrity Level 4, which correlates to the maximum number of V&V tasks specified in this IEEE standard. The number of V&V tasks that need to be perform for software integrity Level 4 continues to increase in newer revisions of IEEE Std 1012. Therefore, the licensees and I&C platform vendors who choose to conform to this RG are dedicating significant resources to V&V activities for software that may be of lower safety significance without receiving comparable safety benefits.

The NRC staff recommends revising the current regulatory licensing guidance to incorporate specific criteria for implementing a graded approach for use of software in safety-related I&C systems. This graded approach should take into consideration the safety significance of the software and any defense-in-depth measures credited by the licensee to address potential failure modes of the software. This licensing guidance should define the minimum set of software development activities that should be performed commensurate with the safety significance of the software. In addition, the NRC's staff review guidance should be revised to incorporate a comparable graded approach for performing reviews where the rigor of the staff's review should be commensurate with the safety significance of the software. While the NRC staff performs such graded reviews on a case-by-case basis by considering past experiences and existing risk information, no formalized guidance or method exists for a graded system. Following the development of this guidance, the NRC staff should also evaluate whether the graded approach should be expanded to the system level of digital designs. By categorizing the I&C system based on its safety significance, the technical and quality criteria can be applied consistently to the software and hardware that compose the system. This approach is also aligned with the categorization scheme in other international nuclear standards (e.g., IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety -Classification of Instrumentation and control Functions"). Therefore, the NRC staff finds that implementation of this recommendation will enhance efficiency and effectiveness for licensing digital I&C systems and harmonize the NRC's I&C regulatory approach with the international nuclear community.

IV. SUMMARY

In accordance with the digital I&C IAP, the NRC staff performed a strategic assessment of the current digital I&C regulatory guidance infrastructure to identify improvements that can facilitate adoption of digital technology in nuclear power plants.

Based on results of this strategic assessment, the NRC staff developed one broad recommendation to improve the regulatory guidance structure and three specific recommendations to improve specific areas in the current guidance. This includes recommendations on use of interim guidance, development of regulatory guidance for I&C architecture, and incorporation of a graded approach to software used in safety-related I&C systems. The NRC staff considers implementation of these recommendations to be instrumental to further increasing the efficiency and effectiveness of NRC staff's licensing reviews of digital I&C applications while reducing impediments identified by industry stakeholders for adopting digital technology.

V. REFERENCES

1. U.S. Nuclear Regulatory Commission, SRM to SECY-15-0106, “Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Standard, 603-2009, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” January 2006.

2. U.S. Nuclear Regulatory Commission, “Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure,” Revision 3, January 2019.

3. U.S. Nuclear Regulatory Commission, “Guidance for Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” Draft Guide (DG)-1353, April 2019.

4. U.S. Nuclear Regulatory Commission, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” RG 1.152, Revision 3, July 2011.

5. Institute of Electrical & Electronics Engineers, IEEE Std 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Piscataway, NJ.

6. U.S. Nuclear Regulatory Commission, “Instrumentation and Control Systems” NUREG-0800, SRP, Chapter 7.

7. U.S. Nuclear Regulatory Commission, “Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants,” RG 1.168, Revision 2, July 2013.

8. U.S. Nuclear Regulatory Commission, “Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” RG 1.168, Revision 1, July 2013.

9. U.S. Nuclear Regulatory Commission, “Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” RG 1.170, Revision 1, July 2013.

10. U.S. Nuclear Regulatory Commission, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” RG 1.171, Revision 1, July 2013.

11. U.S. Nuclear Regulatory Commission, “Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants,” RG 1.172, Revision 1, July 2013.

12. U.S. Nuclear Regulatory Commission, “Developing Software life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” RG 1.173, Revision 1, July 2013.

13. U.S. Nuclear Regulatory Commission, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” BTP 7-19, Revision 7.

14. U.S. Nuclear Regulatory Commission, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” Regulatory Issue Summary 2002-22, Supplement 1, May 2018.

15. U.S. Nuclear Regulatory Commission, “Digital Instrumentation and Controls Licensing Process,” DI&C-ISG-06, Revision 2, December 2018.

16. U.S. Nuclear Regulatory Commission, “Design Specific Review Standard for NuScale,” Chapter 7.

17. International Electrotechnical Commission, IEC 61513, “Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems,” Edition 2. Geneva, Switzerland.

18. U.S. Nuclear Regulatory Commission, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” NUREG-0800, SRP, BTP 7-14.

19. International Electrotechnical Commission, IEC 61226, “Nuclear Power Plants – Instrumentation and Control Important to Safety -Classification of Instrumentation and control Functions,” Edition 3. Geneva, Switzerland.