10th WGDIC Meeting – U.S. Nuclear Regulatory Commission Update on Recent Developments in Digital I&C for New Builds or Plant Upgrades

Outline

- Interim staff guidance (ISG) DI&C ISG 06 (Licensing Process)
- Branch Technical Position (BTP) 7-19 (Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems)
- Design Review Guide (DRG) (Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews)
- Regulatory Guidance Updates
- Boeing 737 Crashes: Lessons Learned Assessment
- Nuclear Energy Institute (NEI) 17-06 (Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications)
- NEI 20-07 (Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems)
- Risk-Informing the Current CCF Policy

Discussion

1. Interim staff guidance (ISG) DI&C-ISG-06 (Licensing Process): The updated ISG DI&C-ISG-06, Revision 2, issued December 2018 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML18269A259), which defines the licensing process used to support the review of license amendment requests associated with safety-related digital I&C equipment modifications in operating plants and in new plants once they become operational. This updated guidance adopted a new streamlined alternate review process to improve the timeliness of licensing reviews and incorporated lessons learned from digital I&C licensing experience. Specifically, the proposed revision reduces the scope of licensee document submittals and provides an alternate review process for earlier approval, which, unlike the current process, would precede factory acceptance testing, for digital designs that are based on approved topical reports. With this revised guidance, the staff has continued to encourage early pre-application interactions for licensees planning major digital upgrades. In August 2021, the U.S. Nuclear Regulatory Commission (NRC) approved a License Amendment Request (LAR) for the digital I&C upgrade of the Waterford Steam Electric Station, Unit 3, core protection calculator system using the alternate review process. The NRC staff is also involved in preapplication meetings with licensees on future digital I&C upgrades before the submittal of their associated LARs.

2. Branch Technical Position (BTP) 7-19 (Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems): On January 25, 2021, the staff published Revision 8 to BTP 7-19 (ADAMS Accession No. ML20339A647). The revision incorporated the five guiding principles outlined in SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls,” dated September 12, 2018 (ADAMS Accession No. ML18179A067) and provided guidance to: (1) Risk-informed graded approach based on safety significance of the digital I&C system; (2) Incorporates lessons-learned from previous operating reactor and new reactor reviews; and, (3) Supports expanded use of defensive measures to address software CCF tailor staff review based on safety significance. The staff will apply this guidance to the ongoing key

licensing actions and intends to update the guidance to incorporate any lessons learned from those reviews.

3. Design Review Guide (DRG) (Instrumentation and Controls for Non-Light-Water Reactor (Non-LWR) Reviews): On February 26, 2021, the NRC published a new technology-inclusive DRG (ADAMS Accession No. ML21011A140). The guidance supports the NRC's non-LWR strategy which involves developing: (1) guidance for flexible regulatory review processes for non-LWRs within the bounds of existing regulations, and (2) a new non-LWR regulatory framework that is risk-informed and performance-based and that features the NRC staff's review efforts commensurate with the demonstrated safety performance of non-LWR technologies. The DRG is technology inclusive because it may also be used in the evaluation of LWR plant designs and other reactor technologies.

4. Regulatory Guidance Updates:
   a. The NRC staff is developing a path forward for RG 1.153, "Criteria for Safety Systems" to best communicate with stakeholders on the use of the Institute of Electrical and Electronics Engineers Standard 603-2018, 'IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
   b. The NRC staff continues the development of an update to RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." RG 1.152 describes an approach that is acceptable to the NRC staff to meet regulatory requirements for promoting high functional reliability, design quality, and a secure development and operational environment for the use of programmable digital devices in the safety-related systems of nuclear power generating stations. The updated RG 1.152, Revision 4, (Draft Guide (DG)-1374) endorses, with exceptions and clarifications, Institute of Electrical and Electronic Engineers (IEEE) Standard (Std) 7-4.3.2-2016, "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations." The IEEE Standard reflects the latest advances in digital technology and techniques for designing and implementing computers into new and operating plants. The updated regulatory guidance is expected to enhance the efficiency and effectiveness of the staff's licensing reviews of upgraded digital I&C systems. The staff anticipates issuing DG 1374 for public comment by December 31, 2022.
   c. The NRC staff continues to assess regulatory options to revise RG 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," to endorse IEEE Std 1012 2016, "System, Software, and Hardware Verification and Validation." The NRC staff is evaluating the use of the graded approach in IEEE Std. 1012 2016, Annex B, for applying software integrity level verification and validation rigor based on the associated safety importance of a DI&C system. Under a holistic theme of "Software Development and Digital Reliability," the NRC staff is also evaluating the feasibility of consolidating RGs 1.168–1.173 into a single RG that endorses individual IEEE computer standards.

5. Boeing 737 Crashes: Lessons Learned Assessment: The NRC staff has completed a summary report, "Boeing 737 Crashes: Lessons Learned for NRC Digital Instrumentation and Controls Evaluation Process," (ADAMS Accession No. ML22241A039). The report documented the staff's evaluation of lessons learned from the Boeing design process and Federal Aviation Administration certification process for the Boeing 737 MAX 8 stabilizer trim control digital modification, including the findings

and recommendations from authoritative investigation reports surrounding the 2018 and 2019 crashes of Boeing 737 MAX 8 aircraft. The NRC staff has determined that no significant gaps exist in the NRC's regulatory infrastructure for digital I&C licensing and inspection as related to the findings and recommendations of the investigative reports. However, the report identifies aspects of the NRC's current digital I&C regulatory program and staff organizational capabilities that should be maintained or could be further enhanced to ensure the continued safe use of evolving digital I&C technologies in regulated nuclear facilities. The NRC staff intends to implement report's recommendations and to continue to evaluate these lessons as part of the normal infrastructure development processes.

6. NEI 17-06 (Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications):
On February 23, 2021, the Nuclear Energy Institute (NEI) submitted NEI 17-06, Revision 0 (ADAMS Accession No. ML21337A380) to the NRC for review. NEI 17-06 clarifies how licensees can use safety integrity level (SIL) certification in their commercial-grade dedication programs, which would provide increased access for digital equipment from international vendors. SIL certification confirms that a given piece of commercial digital equipment meets the stated SIL provisions in International Electrotechnical Commission Standard 61508-2010, "Functional safety of electrical/electronic/programmable electronic safety-related systems." The NRC staff plans to complete the RG development process (i.e., DG-1402, ADAMS Accession No. ML22003A180) for endorsing NEI 17-06 in calendar year 2022. [Update: The RG development process was completed in October 2022 with the issuance of RG 1.250, "Dedication of Commercial-Grade Digital I&C Items for Use in Nuclear power Plants," available via ADAMS Accession No. ML22153A408.]

7. NEI 20-07 (Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems): On August 31, 2020, NEI submitted NEI 20-07, Draft B, "Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems" (ADAMS Accession No. ML20245E561), to support preapplication interactions. As a result of the staff's feedback, during a public meeting on July 1, 2021, the NEI discussed its intent to significantly revise its approach for NEI 20-07 (ADAMS Accession No. ML21229A160). The new approach, submitted on September 30, 2021 (ADAMS Accession No. ML21278A472) to support preapplication interactions, incorporates risk information and the use of probabilistic risk assessment models to form the technical basis to justify that common cause failure is adequately addressed. This approach may be inconsistent with the existing Commission policy in Item II.Q of SRM-SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993 (ADAMS Accession No. ML003708056), so the staff will continue to provide the Commission with information and recommendations, as appropriate, related to any emerging policy issues associated with NEI's proposal.

8. Risk-Informing the Current CCF Policy: The current policy for addressing digital I&C CCFs is from 1993: SRM-SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." The policy has been effectively used to license digital I&C systems in nuclear power plants,

but it requires a diverse means of actuation if a CCF could disable a safety function. The NRC staff has issued guidance on risk-informed, graded approaches to address digital I&C CCFs for low safety-significant systems. The NRC staff recognizes that there is an opportunity to risk-inform the current policy to address digital I&C CCFs for high safety-significant systems. The NRC staff has developed a SECY paper that will provide a recommended expanded policy which will encompass the current positions in SRM-SECY-93-087 and the use of risk-informed approaches to determine the appropriate level of defense-in-depth and diversity to address digital I&C CCFs. Specifically, SECY-2022-76, "Expansion of current policy on potential common-cause failures in digital instrumentation and control systems," was issued on August 10, 2022, and the staff is awaiting Commission feedback. The expanded policy will encompass the current points of SRM-SECY-93-087 (with clarifications) and expand the use of risk-informed approaches. Any use of risk-informed approaches will be expected to be consistent with the NRC's application of risk-informed decision making in other technical disciplines. The current digital I&C CCF policy will continue to remain a valid option for licensees and applicants.

Bibliography

1. SECY-20-0100, "ANNUAL UPDATE ON THE INTEGRATED STRATEGY TO MODERNIZE THE U.S. NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROL REGULATORY INFRASTRUCTURE," October 23, 2020, https://www.nrc.gov/docs/ML2026/ML20269A466.pdf.

2. SECY-21-0091, "ANNUAL UPDATE ON ACTIVITIES TO MODERNIZE THE U.S. NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROLS REGULATORY INFRASTRUCTURE," October 25, 2021, https://www.nrc.gov/docs/ML2125/ML21253A212.pdf.

3. SECY-22-0095, "ANNUAL UPDATE ON ACTIVITIES TO MODERNIZE THE U.S. NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROLS REGULATORY INFRASTRUCTURE AND LICENSE AMENDMENT REQUESTS," October 25, 2022, https://www.nrc.gov/docs/ML2222/ML22222A148.pdf.

4. Public Meeting on "Expansion of Current Policy Regarding Potential Common-Cause Failures in Digital Instrumentation and Control Systems," June 8, 2022, https://www.nrc.gov/pmns/mtg?do=details&Code=20220429.