DRAFT
Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure

Preliminary Draft

NUCLEAR REGULATORY COMMISSION

Contents

Integrated Action Plan to Modernize
Digital Instrumentation and Controls
Regulatory Infrastructure

NOTE: *Public availability of this draft document is intended to inform stakeholders of the NRC staff's development of an integrated action plan to modernize the NRC's digital instrumentation and controls regulatory infrastructure as directed in the SRM-SECY-15-0106 (ML16058A614). The NRC staff is making this information public prior to an NRC public meeting to allow stakeholders to review the material in advance, facilitate discussion during the meeting, and to submit written comments to the NRC. The opportunity to submit written comments on this document is set forth in the Federal Register notice announcing the availability of this document.*

This draft document has not been subject to all levels of NRC management review. Accordingly, it may be incomplete or in error in one or more respects and may be subject to further revision before the staff presents an action plan regarding an integrated strategy to modernize the NRC's digital instrumentation and controls regulatory infrastructure to the Commission in a SECY paper (currently scheduled to be provided to the Commission in May 2016).

Introduction

This document describes the NRC staff's draft integrated action plan for modernizing the digital instrumentation and controls (DI&C) regulatory infrastructure in response to Staff Requirements Memorandum (SRM) -SECY-15-0106 (Agencywide Document Access and Management System (ADAMS) Accession No. ML16058A614) to enable the industry's deployment of DI&C technology in nuclear power plants in a safe and efficient manner. This integrated action plan will also ensure that the modernized regulatory infrastructure will improve the predictability and consistency of the agency's regulatory process for licensing and oversight for the industry stakeholders.

Background

In the operating nuclear power plant fleet, instrumentation and control (I&C) equipment obsolescence is becoming significantly burdensome to licensees, and if not resolved, has the potential to impact the safety of operations. The implementation of current digital technology in safety systems can be useful for resolving obsolescence issues, reducing uncertainties in the maintenance of plant safety, reducing opportunities for human error, and reducing maintenance costs. New nuclear facility designs being submitted for NRC licensing action incorporate modern, highly-integrated I&C design approaches. Such approaches and technology promise benefits to nuclear facility safety and operation, including increased reliability and diagnostics and improved human-machine interfaces. Many industry stakeholders (i.e., licensees, applicants, and vendors) desire to take advantage of these safety and reliability improvements.

The NRC maintains a robust regulatory program for ensuring the safety and security of nuclear facilities protected and operated with analog and digital I&C systems.[1] Using its current regulatory infrastructure, the NRC staff continues to review and approve license amendments for specific DI&C systems, and evaluate new reactor applications that fully incorporate highly integrated digital technologies. To prepare for the review of applications for small modular reactor (SMR) design certifications and combined licenses, the NRC staff has developed a design-specific review standard (DSRS) Chapter 7, which is an innovative initiative specifically for the NuScale SMR design. This DSRS chapter reflects a number of important lessons the staff learned when using the Standard Review Plan (SRP) NUREG-0800 Chapter 7 to review new large light water reactor designs. One of the lessons learned incorporated into this guidance emphasizes fundamental I&C design principles such as independence, redundancy, determinism, and diversity and defense-in-depth, as derived through design and analysis, such as hazard analysis, to prevent loss or impairment of a safety function. This guidance addresses significant aspects of the I&C design in a unified manner.

The NRC provides effective oversight on the construction, implementation, use and maintenance of digital I&C technologies, and maintains an operational experience evaluation program to uncover any systemic issues with DI&C systems. The NRC staff routinely updates its infrastructure (e.g. regulatory guides and SRPs) to address new types of digital technologies and emergent regulatory issues in specific areas. This includes participation in IEEE, ISA, and IEC consensus standards development activities. For example, the NRC is currently working to update Regulatory Guide 1.180 endorsing revised and new industry consensus standards addressing electromagnetic and radiofrequency interference qualification processes. The NRC staff also conducts research to support development of the technical bases for future regulatory infrastructure improvements and emergent licensing challenges. For example, the NRC is currently performing key research activities in the area of digital system hazard analysis to inform future regulatory guidance for evaluating digital safety systems. Such continued update and maintenance of the DI&C infrastructure has helped the continued safe operation of reactors and materials facilities.

Some industry stakeholders have expressed concern that the current DI&C licensing and oversight process for power reactors is cumbersome and inefficient, and/or unpredictable. Some have stated they are hesitant to pursue the deployment of DI&C through license amendments, new applications, or changes under the 10 CFR 50.59 process, unless regulatory efficiency and predictability can be improved. As a result, the NRC staff interacted significantly with industry to discuss its concerns regarding these regulatory challenges. In response to these interactions, the NRC staff developed an action plan to define specific regulatory challenges to be addressed and propose paths for resolving them. In January 2016, the NRC released its working version of this draft action plan (ML16014A085) in an effort to solicit initial feedback from stakeholders. The draft action plan described the staff's interpretation of several challenges to be addressed in response to stakeholder comments regarding their licensing and oversight experience in implementing DI&C. The draft action plan also considered staff experience in evaluating digital safety system designs submitted over the past seven years as part of license applications or amendments, while implementing the interim staff guidance developed as a result of the 2007-2011 Digital I&C Project. The draft action plan identified key regulatory challenges and opportunities for improvement, including potential enhancements to policies, rules, guidance, practices, and processes in the licensing and oversight process.

[1] This program was significantly improved in 2007 - 2011 when staff working groups and industry developed interim staff guidance to address DI&C regulatory challenges at that time.

On February 25, 2016, the Commission issued a Staff Requirements Memorandum (SRM) regarding SECY-15-0106, which disapproved the staff's recommendation to publish for comment in the *Federal Register* a proposed rule which would incorporate by reference (IBR) the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." This proposed rule had included, along with the incorporation by reference of IEEE Standard 603-2009, additional conditions for addressing digital hazards analysis, independence, and digital communications. In the SRM, the Commission directed the NRC staff to develop an integrated strategy, with proposed implementation milestones, to modernize the NRC's DI&C regulatory infrastructure. In developing an integrated action plan, the Commission directed the staff to consider the broader context of DI&C regulatory challenges and include all related activities being pursued by the staff including incorporation of IEEE Std. 603-2009 into 10 CFR 50.55a, updates to the policy on common-cause failure in SRM-SECY-93-087**,** and development of guidance for 10 CFR 50.59 evaluations of DI&C upgrades.

The Commission also directed the staff to engage in public workshops and meetings with the relevant IEEE standards setting committee, licensees, vendors, and other external stakeholders to reach a common understanding of the DI&C regulatory challenges, priorities, and potential solutions to address them. In developing the plan, the Commission also directed the development of the plan to be guided by the following principles:

- The staff's plan should include the establishment of a senior management steering committee to oversee resolution of DI&C regulatory challenges.

- Any new or revised requirements addressed in the action plan should be performance-based rather than prescriptive.

- DI&C safety requirements should be technology neutral, however, guidance should be tailored if necessary. In addition, the same requirements should apply to operating and new reactors.

- Guidance should focus on acceptable approaches to complying with requirements and may include specific technology-focused provisions. If only one approach is acceptable to the staff to ensure safety based on current understanding, and this approach is appropriately technology neutral and performance-based, then it should be included in a requirement rather than in guidance.

- NRC requirements and guidance should not pose an unnecessary impediment to advancement in nuclear applications of digital technology.

Integrated Action Plan

This document provides the integrated action plan as directed in the SRM. It builds upon ongoing regulatory activities, stakeholder feedback concerning the previous draft action plan, and specific Commission direction in SRM-SECY-15-0106 to modernize the DI&C regulatory infrastructure. This plan describes broad topical issues that represent potential regulatory challenges and focuses on potential solutions to areas address them. Based on additional feedback from stakeholders on industry priorities, and on further staff assessment, this integrated plan identifies twelve topical issues and detailed working group action plans that

appear to have the most impact in addressing near-term regulatory challenges and needs of industry.

To put this plan into effect, the staff established individual working groups and developed detailed working group action plans with milestones for addressing five near-term priorities or regulatory challenges with near-term action items. The staff recognizes that the other seven topical areas are important for improving the regulatory infrastructure, but they generally represent longer-term activities, or actions to implement them are dependent on the outcome of the near-term priorities. The staff will periodically update the working group action plans for individual topical areas, as well as develop detailed working group plans when appropriate for the other areas after work progresses on the near-term priorities.[2]

Development and Updating Processes for this Integrated Action Plan

As directed by SRM-SECY-15-0106, the staff has established a senior management steering committee (SC) to oversee resolution of DI&C regulatory challenges. The SC is comprised of five division directors from the following divisions: Director of the Division of Engineering in the Offices of Nuclear Regulatory Research (RES) and Nuclear Reactor Regulation (NRR); the Director of the Division of Engineering, Infrastructure and Advanced Reactors in the Office of New Reactors (NRO); Director of the Cyber Security Directorate in the Office of Nuclear Security and Incident Response (NSIR), and the Division of Fuel Cycle Safety, Safeguards and Environmental Review in the Office of Nuclear Material Safety and Safeguards (NMSS).

The SC will periodically assess the status and effectiveness of this integrated action plan in light of the directives of the Commission SRM, and evaluate the progress of meeting the overall objectives of the modernization of the NRC's DI&C regulatory infrastructure. The SC will be supported by managers and staff in the offices with expertise and shared responsibility in the field of DI&C. This integrated action plan will be maintained by the respective NRC line organizations under the supervision of the SC. The staff members will coordinate with the SC to update and modify individual working group action plans, as well as obtaining SC approval to establish new working groups as progress is made on the near-term activities. Ownership of each working group action plan will be assigned to appropriate NRC office leads. This integrated action plan will be updated semi-annually to indicate progress made within each activity, so that the document can also be used as a reporting/briefing tool. Changes to the working group action plans that are identified during these periodic reviews shall be agreed upon by the SC.

DI&C Regulatory Challenges, Priorities, and Potential Solutions

A summary of key regulatory challenges, priorities, and potential solutions are described below. These topics were identified through significant engagement with stakeholders and staff analysis of the regulatory infrastructure. The first five topics have been identified as near-term priorities and have associated working group action plans later in this document. The remaining topics have been identified as important activities needed to be addressed to complete the DI&C infrastructure modernization effort, but for which the specific actions are either dependent on the outcome of near-term actions, or are being deferred while the staff's resources are being used to address the first five activities.

[2] As discussed in the Background Section, the staff continue to perform routine updates of regulatory guides under normal processes, and performs various research activities to support emergent and long-term regulatory activities. These individual activities are not tracked in this integrated action plan.

1. Assess Commission Policy on Potential Common Cause Failures.

NRC staff and industry stakeholders generally agree that the Commission policy on potential common cause failure (CCF) should be addressed as a near-term regulatory challenge. Industry has suggested that the current NRC policy and guidance to address software CCF to perform analog-to-digital or digital-to-digital modifications have insufficient details or are overly conservative for simpler or lower risk-significant digital applications. The NRC staff has identified several activities necessary to evaluate the current NRC policy and staff guidance necessary in response to the industry suggestions. For modern DI&C systems, these activities will address common-cause or common-mode failures, which could lead to safety-significant common-mode failures and represent plant vulnerabilities incompatible with the protection of public health, safety, security and the environment. The desired outcome of this effort is to clarify NRC staff position regarding how the potential for CCF of DI&C systems should be addressed for acceptability and ensure that there will be appropriate, clear guidance for implementing this policy. An updated policy and revised guidance should serve to improve the ability of licensees, vendors, or applicants to evaluate a proposed design of or modification to digital safety systems (including their components) through an NRC license application or change under 10 CFR 50.59. This is a near-term priority with a detailed working group action plan.

2. Improve Guidance for Using DI&C in Existing Nuclear Power Plants Using 10 CFR 50.59 Process.

NRC staff and industry stakeholders generally agree that updating the current guidance for implementing DI&C upgrades under the change authority of 10 CFR 50.59 is a near-term regulatory challenge. There is a need for clarity of mutual industry and NRC staff understanding that NRC guidance is being properly used during industry actions for performing 10 CFR 50.59 evaluations of DI&C plant modifications. The desired outcome of this effort is to reach a common understanding of the DI&C challenges, priorities, and potential solutions to develop guidance for 10 CFR 50.59 evaluations of DI&C upgrades. This includes improving the clarity for assessing common cause failure and associated criteria in 10 CFR 50.59 analysis. This is a near-term priority with a detailed working group action plan, and will be closely coordinate with CCF.

3. Incorporation by Reference of IEEE Standard 603 into 10 CFR 50.55a.

NRC staff believe that updating the design criteria for instrumentation and control (analog and digital) (by incorporating by reference IEEE 603 into 10 CFR 50.55a) is a near-term regulatory challenge. Some stakeholders have agreed that IEEE 603 should be IBR. However, these stakeholders have opposed the inclusion of additional technical conditions beyond the standard, such as those that were proposed in the proposed rulemaking in SECY-15-0106. The staff does not intend to further pursue incorporation of IEEE 603-2009 into the regulation. In this integrated action plan, the NRC staff is developing an approach to IBR a future revision of the IEEE Standard 603 into 10 CFR 50.55(a) ideally without additional conditions. This effort will seek feedback from the standards development organization (SDO), IEEE Nuclear Power Engineering Committee (NPEC), and industry stakeholders, regarding future NPEC efforts to update the standard and the NRC plans to codify IEEE Standard 603 criteria. The desired outcome of this effort is to solicit feedback from the SDO on the next standard update (IEEE 603-2018) and develop a rulemaking

approach for updating 10 CFR 50.55a to reflect modern IEEE design standards for DI&C. This is a near-term priority with a detailed working group action plan.

4. IEEE Standard 7-4.3.2 Regulatory Guidance Plan

NRC staff believe that considering the new IEEE 7-4.3.2-2016 standard and updating Regulatory Guide 1.152 to endorse this standard is a near-term regulatory challenge. In SECY-15-0106, the NRC staff recently proposed several conditions for the use of IEEE 603-2009 regarding system independence and data communication. The proposed IBR of IEEE 603 rulemaking was disapproved by the Commission at this time. Although not approved by the Commission, some of the proposed, digital-specific conditions in SECY-15-0106 would technically align closer with the scope and purpose of IEEE 7-4.3.2, instead of the broader criteria of IEEE 603. The objective of this effort is to (1) determine objectives for modifying the guidance presently included in Regulatory Guide 1.152, in consideration of IEEE 7-4.3.2-2016 and (2) seek feedback from the IEEE on the additional conditions for communication and independence that were proposed in SECY-15-0106. This is a near-term priority with a detailed working group action plan. This item will be closely coordinated with the IEEE 603 working group efforts.

5. Evaluate Regulatory Action Concerning Review of Cyber Security Design Aspects

Operating reactor licensees and Combined License (COL) applicants are currently required to submit a cyber security plan to be reviewed by the NRC in accordance with 10 CFR 73.54. However, they are not required by regulation to submit design information to address cyber security requirements as part of the NRC licensing review. The objective of this effort is to provide NRC staff with sufficient guidance to support the review of voluntarily-submitted cyber security design information within current regulations to determine its potential impact on a licensee's/applicant's cyber security program and to support the review of DI&C design elements for evaluation of potential security impact, and to revise the appropriate regulatory documents to facilitate cyber security reviews. This is a near-term priority with a detailed working group action plan.

6. Embedded Digital Devices[3]

Equipment vendors have increasingly introduced embedded digital devices (EDDs) into nuclear plant equipment (e.g., emergency diesel generators, motor control centers, pumps, and relays) used by licensees and applicants for systems considered important to safety. There have been instances where the introduction of these devices by equipment vendors as sub-components within active plant equipment, such as valve actuators and motor control centers, was discovered after the equipment was installed and operating. Information Notice (IN) 2016-01, "Recent Issues Related to the Commercial Grade Dedication of Allen Bradley 700-RTC Relays," also highlighted the unrecognized introduction of an EDD into important I&C applications and noted deficiencies in commercial grade item dedication processes. It is important that licensees have appropriate guidance enabling them to ensure these devices are properly identified, installed, and operated safely

[3] The staff seeks specific feedback on this particular item to determine if it should be a near-term regulatory priority with a detailed working group plan.

such that potential hazards and impact on required safety functions are appropriately addressed.

A public webinar is planned for April, 2016 to enable the staff to outline how it has addressed stakeholder comments received during the development of Regulatory Issue Summary (RIS) 2015-12, "Embedded Digital Devices in Safety-Related System." The purpose of this RIS is to alert the applicable stakeholders of the issue and clarify the current regulatory requirements and guidance on the subject. In the near term, following the issuance of the RIS, the NRC staff plans to seek input from stakeholders regarding any near-term issues identified following issuance of the RIS, to increase the staff's understanding of the degree to which licensees have identified all EDDs installed in their plants and are evaluating the safety of such applications before their introduction into plant applications. In the longer term, the information gained from the near-term action will be evaluated in light of the outcome of activities pertaining to the re-evaluation of the criteria for CCF due to software error, improved guidance on 50.59 evaluations, and the staff's ongoing evaluation of operating experience events and review of inspection findings in this area. Finally, the staff may consider possible next steps in addressing EDD issues, with the overall objective of modernizing the DI&C regulatory infrastructure. This plan will be closely coordinated with other action plans and working groups for addressing common mode failures due to software error, 10 CFR 50.59 guidance, and others as needed.

7. Regulatory Document Infrastructure Improvements

Stakeholders have commented that the overall regulatory document infrastructure (regulatory guides, standard review plan, branch technical positions, ISGs, etc.) makes it difficult to achieve efficient, effective and consistent staff evaluation of licensing submittals. The Standard Review Plan (SRP) content and organization, and the multiple I&C-related regulatory guidance documents will be assessed. NRC staff will assess possible methods for consolidating and organizing this guidance to enhance the ability of technical reviewers to address the review criteria will be identified. This topic will be addressed as the results of the near-term topics are documented in order to establish a consolidated set of review guidance to enable more efficient technical reviews.

8. Guidance for Evaluation of Proposed Alternatives to Regulatory Guides and Endorsed Standards

NRC technical reviewers would benefit from additional guidance to evaluate licensee-submitted proposed alternatives to the criteria in regulatory guidance and endorsed codes and standards, applicable to the licensing of DI&C systems and components. Gaps in guidance create a challenge for technical reviewers seeking to make consistent engineering judgments on the safety assurance of proposed alternative solutions for meeting applicable acceptance criteria presented in regulatory guides and the SRP. The outcome of this effort will be the implementation of an alternative review process to enable a more efficient evaluation of proposed alternatives to the current NRC staff review criteria.

9. DI&C Licensing Process

Staff and industry agree that specific guidance in the standard review plan for license reviews can be improved. The level of technical detail submitted in license applications,

license amendments, and licensing topical reports, as well as the timing and sequence of the technical information expected to be submitted for NRC evaluation during the review cycle should be reassessed and improved. Revised guidance will incorporate lessons learned from recent licensing actions and identify and bridge gaps between the 10 CFR Part 50 and Part 52 processes in an effort to minimize the need for requests for additional information (RAIs) and to clearly define for the license applicants, design certification vendors and licensees, what types of information is needed at each stage of the application evaluation process. The outcome of this effort would be to update the SRP with current guidance and lessons learned from the use of ISG-06 and design specific review guides. This is a longer term activity that would not begin until progress is made on addressing items 1, 3, and 4 of this plan.

10. Improved Guidance for Evaluation of Highly-Integrated Digital Technologies

Proposed new reactor I&C designs, with their advanced and more fully-integrated digital technologies, are challenging for both the staff and industry to evaluate for safety assurance, in part because the existing review guidance does not fully address the accompanying hazards impacting safety that could result from highly-integrated I&C systems. Current assessment approaches and associated review guidance do not effectively address the challenges and potential hazards (e.g. data communication independence and potential for spurious actuation of safety and non-safety control systems). Further, the continually evolving nature of digital technology appears to increase the impact of these challenges and hazards. In general, the current assessment approach does not credit the safety benefits offered by new design approaches and technology and adequately identify methods to apply for evaluating whether the hazards have been minimized. The outcome of this effort will be improved regulatory guidance for licensees and applicants that will enable a more efficient and effective hazards analysis and safety evaluation.

11. Improvement in Regulatory Consistency from Licensing to Inspection

Industry stakeholders have expressed concerns that regulatory positions are not always consistent between the NRC Headquarters staff, which performs licensing actions, and the Regional Offices, which perform inspections. Stakeholders indicate there has been inconsistency in interpretation of current regulatory guidance. There is currently room for greater interaction on generic DI&C technical matters between licensing staff and the regional office inspection staff. Typically, these staffs do not interact regularly, unless there is a problem found during a region inspection that cannot be resolved by the region personnel. The outcome of this effort will be improved regulatory consistency and will be influenced by the results of the revised guidance of the 10 CFR 50.59 near-term efforts. This is a longer term activity that would take into account the results of progress made on addressing items 1 through 4 of this integrated action plan.

12. DI&C Topical Report Evaluation and Update Process

The expenditure of NRC staff resources for the review of DI&C platform topical reports has not gained the efficiencies in performing licensing evaluations as was originally envisioned. A process is needed to effectively and efficiently address updates to topical reports, and to address design changes made to platforms following issuance of the original

topical report safety evaluation. Staff will engage with vendor and licensee stakeholders to identify the challenges in keeping the topical reports current and to establish a process for them to maintain vendor I&C platform topical reports current. The desired outcome of this effort will be a reduction in staff review time and scope when licensing reviews reference a topical report. This is a longer term effort to be worked in conjunction with the resolution of item 9 of this integrated action plan.

Working Group Action Plans

The following working group action plans have been developed to resolve near-term regulatory challenges or potential policy issues identified by NRC and/or industry. Several of these items are inter-related and the working group action plans ensure integration and coordination on common issues.

1. Assess Commission Policy on Potential Common Mode Failures (CCF)

2. Improve Guidance for Using DI&C in Existing Nuclear Power Plants using the 10 CFR 50.59 Process

3. IEEE 603 Working Group Action Plan

4. IEEE Standard 7-4.3.2 Regulatory Guidance Plan

5. Evaluate Regulatory Action Concerning Review of Cyber Security Design Aspects

1. Assess Commission Policy on Potential Common Mode Failures

Introduction

The NRC staff has identified several activities necessary to evaluate current NRC policy and branch positions necessary to modernize the regulatory framework, as well as to improve the efficiency in licensing or subsequent inspection processes. For modern digital I&C systems, these activities will address common-cause or common-mode failures, which lead to safety-significant common-mode failures and represent plant vulnerabilities incompatible with the protection of public health, safety, security and the environment.

Background

This working group action plan is based on action plan item # 2 in the NRC document "Draft Digital Instrumentation and Control Path Forward Action Plan" (ADAMS Accession No. ML16014A085).

Industry has suggested the historical guidance provided by the NRC staff, which has been used by licensees to perform analog-to-digital or digital-to-digital modifications, has insufficient details regarding: a) how to address the potential for common cause failure (e.g., potential plant vulnerabilities from having identical redundant digital I&C divisions, or mistakes made or errors introduced by processes for implementing configuration changes); and b) how to evaluate malfunctions with the possibility of a new result. Specifically, industry stakeholders are looking for clearer NRC staff guidance on methods for analysis of the potential for common cause failures of modern digital I&C systems. For example, analysis methods or acceptance criteria might adopt a graded approach based on the safety consequence of a potential CCF. Stakeholders would like to have improved regulatory guidance and criteria for performing common cause failure evaluations.

The SRM to SECY 93-087 does not include any criteria for eliminating consideration of software CCF in a diversity and defense-in-depth analysis. However, BTP 7-19 includes two criteria for eliminating the consideration of CCF. It is anticipated that industry may propose criteria to qualitatively "eliminate" consideration of CCF within a digital design guidance document, which NEI is expecting to receive from EPRI later 2016.

The current regulatory treatment and acceptance criteria dealing with the potential for common cause failure in the analysis of digital I&C systems has been problematic for licensees. The proper application of the screening criteria for "simple systems" in BTP 7-19 regarding 100% testability, and the lack of a graded approach based on safety significance, places a high burden for demonstrating adequate digital I&C system development processes have been employed—especially for systems containing localized embedded digital I&C components.

Objectives

The objective of this effort is to perform an evaluation of the current NRC position in an effort to recommend to the Commission that it either modify or affirm the NRC's current digital system CCF position as discussed in Item II.Q of the SRM to SECY 93-087, and Branch Technical Position (BTP) 7-19. Although the current position focuses on common cause failure due to software error in digital systems, the evaluation will look at whether the position should continue to focus on software.

The desired outcome of this effort is to clarify the NRC staff position regarding how the potential for CCF of digital I&C systems should be addressed for systems and components. This clarification should serve to improve the ability of licensees to evaluate a proposed design of or modification to digital safety systems (including their components) through an NRC license application or change under 10 CFR 50.59. The scope of systems to be included in the NRC position on CCF of digital I&C systems will also be reviewed.

Proposed Actions

This plan is part of the Digital I&C Action Plan, and defines the specific activities to be performed to evaluate the current NRC position on CCF of digital I&C systems. The actions proposed are:
define and prioritize key activities, hold internal and public meetings with external stakeholders (e.g., NEI, Owners Groups, EPRI, etc.) and the ACRS, and develop a SECY paper outlining the technical basis for recommending either modifying or re-affirming the existing CCF position as described in the SRM to SECY 93-087 and in BTP 7-19. Consequently, the following specific activities will be performed.

Activity	**Schedule**
1. Complete evaluation of existing position and regulations related to common mode failures	March 30, 2016
2. Engage industry and public stakeholders in workshops and targeted meetings to gather insights on key technical and policy issues	March 21, 2016 April 2016 May 2016
3. Prepare a technical basis document to summarize the evaluation of current NRC position and regulations	July 15, 2016
4. Present Technical Basis to the ACRS	July 2016
5. Request independent peer review of technical basis	August 15, 2016
6. Request general comments from the public	August 15, 2016
7. Receive comments from independent reviewers	August 31, 2016
8. SECY paper to the Commission identifying proposed action to modify or affirm existing position	TBD
9. Implement resolution identified in SECY paper	TBD

Status
(as of March 22, 2016)

The working group is finalizing the schedule for activities to be performed.

A meeting with external stakeholder was completed on March 21, 2016.

The working group is currently writing the technical basis that will summarize the evaluation on the current NRC position.

Potential Regulatory Challenges and Policy Issues

The proposed NEI approach to eliminate consideration of CCF through qualitative likelihood factors may result in a delay in the resolution of this topic due to the NRC review and resolution of the proposed NEI methodology.

Any change or affirmation of the current CCF position is a potential policy issue that would be coordinated with the Commission.

Interactions with other Action Plan Items

CCF of digital I&C systems is an important aspect supporting the working group responsible for improving licensee guidance for incorporating DI&C using the 10CFR 50.59 Process.

CCF of digital I&C systems was not considered in the SRM-SECY-15-0106. Therefore, results from the staff's evaluation will be considered in the action plan for IEEE 603 Rulemaking and Associated Guidance.

2. Improve Guidance for Using DI&C in Existing Nuclear Power Plants Using the 10 CFR 50.59 Process

Introduction

This action plan describes the activities and schedule for improving guidance for incorporating DI&C using the 10 CFR 50.59 process. These activities will address the need for clarity of mutual industry and NRC staff understanding that NRC guidance is being properly translated into industry actions for performing 10 CFR 50.59 evaluations of DI&C plant modifications. An industry task force is nearing completion of its improved guidance and has stated that it is now ready to coordinate with the staff to obtain feedback from a regulatory and technical perspective.

Background

Inadequate guidance for the 10 CFR 50.59 screening and evaluation of DI&C systems has resulted in several licensees having improperly performed 10 CFR 50.59 analyses for modifications of I&C systems using digital technologies. The NRC staff has held several public meeting and discussions with industry representatives on this subject, and indicated where the industry guidance should be improved.

RIS 2002-22, "Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,' " provides the NRC staff's endorsement for the use of NEI 01-01. However, experience with implementing DI&C upgrades under 10 CFR 50.59 at nuclear power plants have revealed several shortfalls in the screening of modifications, addressing the appropriate design criteria, and evaluating the impact of proposed DI&C on established licensing basis. A key issue in recent oversight experience has been licensee assessment of potential CCF and any potential new malfunctions, with respect to the change authority criteria in 10 CFR 50.59(c)(2)

In a November 2013 letter to NEI (ML13298A787), the NRC staff summarized its concerns regarding licensee implementation of the current guidance in NEI 01-01 (ML020860169). In response, NEI formed a working group to update its guidance for implementing DI&C modifications under 10 CFR 50.59. The NEI working group found that additional guidance was needed to support three specific aspects of evaluating the impact of such modifications on plant safety. The NEI working group identified that additional guidance is needed for assessing whether the impact of the new digital equipment will: (a) result in more than a minimal increase the likelihood of occurrence of a malfunction of a system or component important to safety previously analyzed; (b) create the possibility for an accident of a different type than previously evaluated; and (c) create the possibility for a malfunction of a system or component important to safety with a different result than previously analyzed.

Regulatory Guide 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments," provides the NRC staff's endorsement of industry guidance for evaluating the impact on plant safety analyses for plant modifications performed under 10 CFR 50.59. The objectives of 10 CFR 50.59 are to ensure that licensees: (1) evaluate proposed changes to their facilities for their effects on the licensing basis of the plant, as described in the FSAR, and (2)

obtain prior NRC approval for changes that meet specified criteria as having a potential impact upon the plant license basis.

Objectives

The goal is to ensure there is adequate NRC guidance for 10 CFR 50.59 evaluations of DI&C upgrades. The activities to achieve the objective include:

- Review Appendix D to NEI 96-07 for potential endorsement in RG 1.187
    - Identify and determine whether NRC policy or guidance may need to be modified, and identify and determine impact on NRC policy or guidance and develop remedies, where appropriate.
    - Engage NRC Headquarters and Region Staff in the review of Appendix D of NEI 96-07 and in the development of the NRC position for endorsement for Appendix D of NEI 96-07.
    - Identify any areas where the proposed draft of Appendix D of NEI 96-07 may deviate from current NRC policy or guidance.

Proposed Actions

Activity	**Schedule**
1. Staff received NEI guidance document, Appendix D 96-07, Guidelines for 10 CFR 50.59 Evaluations	April 1, 2016
2. Staff completed initial review and comment on NEI guidance	April 2016
3. Public Engagement; public meeting at NRC headquarters and via Go-To-Meeting. Purpose - NEI to present the guidance in the Appendix and discuss with the NRC.	April 2016
4. Staff completes its review comments on Appendix D.	June 6, 2016
5. Public Engagement; public meeting at NRC headquarters and via Go-To-Meeting. Purpose – NEI to provide feedback on NRC staff review comments.	June 23, 2016
6. NRC staff makes decision on acceptable method(s) for addressing CCF in 50.59 guidance (as applicable).	July 2016
7. Staff receives revised Appendix D from NEI.	August 2016
8. Staff issues safety evaluation on Appendix D.	Fall 2016
9. ACRS / External stake holder interaction	Summer/Fall 2016
10. Begin update of RG 1.187	Fall 2016

Status
(as of March 22, 2016)

NEI indicated they will provide a draft of Appendix D to NEI 96-07 by the end of March, 2016, and would like a meeting during the second week of April 2016.

Potential Regulatory Challenges and Policy Issues

- The NRC Staff expects NEI's proposed industry approach to eliminate evaluation of some types of potential software CCF through qualitative likelihood.

- No potential policy issues identified

Interactions with Other Action Plan Items

It will be necessary to coordinate with working group on CCF to ensure alignment on regulatory guidance positions and NRC policy for addressing software CCF.

3. IEEE 603 Working Group Action Plan

Introduction

The purpose of this plan is to establish the structure, scope, and expectations for the Nuclear Regulatory Commission's (NRC) IEEE Standard 603 Working Group for its portion of implementation of the Integrated Digital Instrumentation and Control (I&C) Action Plan. This item in the integrated action plan is to potentially streamline the rulemaking process to incorporate by reference (IBR) the current or future revision of the IEEE Standard 603 into 10 CFR 50.55(a). This effort will also facilitate interactions with standard's developer, IEEE Nuclear Power Engineering Committee (NPEC), and industry stakeholders regarding the NRC's plans to codify IEEE Standard 603 criteria.

Background

Currently IEEE Std. 603-1991 is IBR into 10 CFR 50.55a along with IEEE Std. 279-1971 depending on the date of the construction permit or operating license of the facility as the paragraph stipulates. The NRC staff has determined that there is no safety issue involved with facilities using the previous, 1991, version, IEEE Std. 279 or previous criteria identified by the agency depending on the licensing basis of the facility.

In publishing the current version, IEEE Std 603-2009, the IEEE has advanced the standard to include characteristics related to the use of advanced technologies (while maintaining the technological neutrality of the standard) such as electromagnetic compatibility, independence, isolation and updating the use of the latest referenced standards including the more extensive use of the digital standard if that technology is selected for implementing the requirements.

In SECY-15-0106, the NRC staff proposed to the Commission to IBR IEEE Std. 603-2009 with certain licensing and technical conditions into 10 CFR 50.55a. SECY-15-106 also included Draft Regulatory Guide (DG) 1251 as a proposed revision to Regulatory Guide (RG) 1.153 which provides the underlying basis of the 10 CFR 50.55a(h) regulation when implementing or modifying safety systems in nuclear power plants. The Commission did not approve publishing the proposed rule. In SRM-SECY-15-0106, the Commission directed the staff to consider broader regulatory challenges and stated that DI&C safety requirements should be technology neutral, however, guidance should be tailored if necessary. In addition, the Commission directed that the same requirements should apply to operating and new reactors. Although not approved by the Commission, some of the proposed, digital-specific conditions in SECY-15-0106 would align with the scope and purpose of IEEE 7-4.3.2 guidance, instead of the broader criteria of IEEE 603

The NRC staff participates in development of IEEE Std. 603. These high level principals directed by the Commission are inherent to the development of the standard by the IEEE working group. Collaboration with the industry and with the consensus standard development organization (IEEE NPEC) on the technical content of the requirements is a primary focus of the NRC Staff to complete the objective.

Objectives

The objective of the NRC IEEE 603 working group's effort is to modernize the requirements into 10 CFR 50.55a that would reference current design standards for DI&C. The preferred method would be incorporating by reference the work-in-progress 2018 version of the IEEE 603 standard which has included several of the technical requirement conditions in SECY-15-0106 but the scope of revision has been set. Addressing the following requirements proposed by the NRC staff in SECY-15-0106 will likely be included in the 2018 version of the IEEE-603 standard:

- 50.55a(h)(7) – Maintenance Bypass – Only exception to 2009 standard by retaining 1991 standard for bypass with a "shall" statement.
- 50.55a(h)(4) - System Integrity - Safety functions shall be predictable and repeatable
- 50.55a(h)(6) - Maintenance Bypass - Corrects Reference between this and operating bypass clause.
- 50.55a(h)(1) - Definitions - Related to the added requirements noted above and further enhancement of the standard.

The alternative objective would be the IBR of the next revision (202X) of the IEEE 603 standard where the NRC staff could collaborate with IEEE NPEC on possible requirements beyond those noted above.

Proposed Actions

This plan is part of the Integrated DI&C Action Plan, and defines the specific activities to be performed to evaluate the any new or revised regulatory requirements that are currently in or should be added to the scope of IEEE Std. 603.

Activity	Schedule
1. Request feedback from IEEE on the consideration of proposed conditions in SECY-15-0106 for the next update to IEEE 603 and the potential timing of the next update.	March 2016
2. Evaluate if additional changes can be added to IEEE 603-2018 that would not affect the scope and publication release date of the revision. Include evaluation of each specific condition proposed in SECY-15-0106 and specific Commission direction in SRM-SECY-15-0106 in coordination with the NRC IEEE &-4.3.2 working group	September 2016
4. Continue participation on IEEE 603 WG to support the balloting process and final publication of IEEE 603-2018	July 2016 January 2017 July 2017 January 2018
5. Coordinate with the CCF and IEEE 7-4.3.2 working groups to ensure alignment on regulatory guidance, positions, and policies.	On-going as appropriate
6. Engage stakeholders on our planned approach to update 10 CFR 50.55(a)	November 2016

Activity	Schedule
7. Make Decision on whether to begin a streamlined rulemaking for incorporation by reference of IEEE 603-2018 into 10 CFR 50.55a or wait for the next update.	December 2017
8. Provide recommendations if RG 1.153 draft needs to be revised..	December 2017
9. Continue participation on IEEE 603 WG to support development of the PAR for next update of IEEE 603-202x.	July 2018

Status
(as of March 4, 2016)

The IEEE NPEC has identified the scope and intent of the revisions to be included in the next revision of IEEE Std. 603 which should be the 2018 version. The timeline for publishing the standard is set by the IEEE 10 year lifetime policy for a version of a standard before the standard automatically goes inactive. (In this case, the 2009 version must be revised by 2019 or the standard will go inactive.)

The draft language for most of the changes (including the NRC proposed new and revised requirements listed in the Objectives section.) has been developed and the draft version of IEEE Std. 603-2018 is being created.

Potential Regulatory Challenges and Policy Issues

- Industry does not currently support incorporation by reference of IEEE 603 into the regulations and considers the activity a low priority

- Standard development should consider these differences and be consistent with the requirements in SRM-SECY-15-0106 as listed previously:

    1) Technology neutral
    2) Performance based
    3) Same requirements apply to new and operating reactors
    4) Requirements should not pose an unnecessary impediment to advancement in nuclear applications of digital technology

- It is not clear that IEEE will further consider the proposed conditions in SECY-15-0106 into the 603 standard.

- Proposed rulemaking to incorporate by reference an updated IEEE 603 standard into 10 CFR 50.55a may be provided to the Commission as a policy decision

Interactions with other Action Plan Items

The NRC staff is involved with the IEEE 603 working group. As details of the IEEE 603 rulemaking have been publically released, the NRC staff involved in the working group has updated and provided details of the proposed changes and conditions to members of the IEEE working group. Many of the conditions have been accepted by the working group, however the topics listed below have not been and will be addressed as noted.

- The next update to IEEE 603-2018 will include generic language regarding the treatment of common cause failure. The IEEE 603 NRC working groups members will coordinate with the software CCF as appropriate

- IEEE 603-2018 generically references IEEE 7-4.3.2 as additional standards for DI&C. The IEEE 603 NRC working group have and will closely coordinate with the IEEE 7-4.3.2 NRC working group

- The regulatory infrastructure review group may determine the need for additional requirements affecting 10 CFR 50.55(a) or IEEE 603, or may establish a need for additional task working groups. The IEEE 603 task working group will interact as appropriate with the infrastructure review group and with any new task working groups that may be created.

4. IEEE Standard 7-4.3.2 Regulatory Guidance Plan

Introduction

The purpose of this plan is to establish the structure, scope, and expectations for the Nuclear Regulatory Commission's (NRC) IEEE Standard 7-4.3.2 Task Working Group for its role in implementation of regulatory guidance relating to the proposed conditions of SECY-15-0106. This effort will include interactions with industry and external stakeholders regarding the next update to IEEE 7-4.3.2 and development of regulatory guidance for the use of IEEE 7-4.3.2 criteria.

Background

The NRC recently proposed several regulatory requirements regarding system independence and data communication for the proposed rule to incorporate by reference IEEE 603-2009 into 10 CFR 50.55a (SECY-15-0106). Some of these conditions were applicable only to new or operating reactors. The Commission did not approve publishing the proposed rule. In SRM-SECY-15-0106, the Commission directed the staff to consider broader regulatory challenges and stated that DI&C safety requirements should be technology neutral, however, guidance should be tailored if necessary. In addition, the Commission directed that the same requirements should apply to operating and new reactors. Although not approved by the Commission, some of the proposed, digital-specific conditions in SECY-15-0106 would align with the scope and purpose of IEEE 7-4.3.2 guidance, instead of the broader criteria of IEEE 603. The NRC staff intends to interact with IEEE on future development of IEEE 7-4.3.2 and determine whether such conditions should be pursued in the industry consensus standard.

The NRC considers conformance with the requirements within the 2003 version of IEEE Standard. 7-4.3.2,"Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as conditioned in revision 3 of regulatory guide 1.152, to be an acceptable method for satisfying regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. The NRC staff participates in working group 6.4 of subcommittee 6 for the standards development of IEEE 7-4.3.2. IEEE 7-4.3.2-2016 is an approved draft standard and adds guidance for several topical areas to address changes which have occurred in DI&C technology. The newer versions of the standard also address criteria derived from NRC interim staff guides DI&C-ISG-04, "Highly-Integrated Control Rooms- Communications Issues" and DI&C-ISG-02, "Diversity and Defense-in-depth Issues"

The IEEE is also developing a new standard P-1891 to address the use of intelligent digital devices such as Smart Transmitters for use in nuclear power plant applications. When this guidance becomes available, the NRC will evaluate its criteria to establish a regulatory position and guidance on the application development activities associated with these devices. NRC staff may choose to develop guidance on this topic in Regulatory Guide 1.152, in concert with its review of IEEE 7-4.3.2, or staff may recommend creation of a new regulatory guide or other means of addressing the provisions of the standard.

Objectives

The objective of this effort is to (1) interact with IEEE to determine if proposed conditions from SECY-15-0106 can be added to IEEE Std. 7-4.3.2, and (2) identify the scope and objectives for modification of regulatory guide 1.152, in consideration of IEEE-7-4.3.2-2016.

The following are conditions proposed in SECY-15-0106 to be considered as part of the objectives discussed above.

- 50.55a(h)(5)(i) - Hazard analysis between redundant safety systems
- 50.55a(h)(5)(ii) - Hazard analysis between safety and other Systems
- 50.55a(h)(5)(ii) - Signal processing
- 50.55a(h)(5)(iii)(B) - Detection and mitigation of signal faults
- 50.55a(h)(5)(iii)(C) - Outside communication signals must have safety benefit
- 50.55a(h)(5)(iii)(D)(*1*) - Data communication one-way only from safety to non-safety
- 50.55a(h)(5)(iii)(D)(*2*) - Data between safety systems shared only if safety benefit
- 50.55a(h)(5)(iii)(D)(*3*) - Safety systems can only receive data from outside if it provides diversity and anticipatory trip benefits. Such outside communication must be hardwired.
- 50.55a(h)(5)(iii)(D)(*4*) - All pathways must be identified if alternative is requested to (D)(1) thru (3)
- 50.55a(h)(1) - Definitions associated with new independence requirements

Proposed Actions

This plan is part of the Integrated DI&C Action Plan, and defines the specific activities to be performed in connection with IEEE Standard 7-4.3.2.

Activity	**Schedule**
1. Request feedback from IEEE on the consideration of proposed conditions in SECY-15-0106 for the next update to IEEE 7-4.3.2 and potential timing of next update.	March 2016
2. Request technical feedback from IEEE NPEC working group 6.4 on proposed conditional requirements in SECY-15-0106.	July 2016
3. Coordinate with working groups on CCF and IEEE 603 to ensure alignment on regulatory guidance, positions, and policies.	On-going as appropriate
4. Engage NEI/Stakeholders on our planned approach to IEEE 7-4.3.2 2016, RG1.152, and the standard Review Plan.	November 2016
5. Determine scope for the next update to Regulatory Guide 1.152 and to the Standard Review Plan to address the current IEEE 7-4.3.2-2016 and P-1891 standards.	December 2016
6. Continue participation on IEEE 7-4.3.2 working group to support identified changes to next update to IEEE 7-4.3.2	On-going, per IEEE schedule

Status
(as of March 7, 2016)

The working group is reviewing the criteria of IEEE 7-4.3.2-2016 for regulatory consideration.

Potential Regulatory Challenges and Policy Issues

The IEEE Standards Committee may not be willing or able to incorporate proposed SECY-15-0106 provisions into the standard, or to incorporate them in a sufficiently timely manner.

Incorporation of the SECY-15-0106 provisions into guidance may not be sufficient to address the issues that have been identified, and the staff may need to consider other avenues to resolve them.

Interactions with other Action Plan Items

It will be necessary to coordinate with working group on CCF to ensure alignment on regulatory guidance positions and NRC policy for addressing software CCF.

It will also be necessary to coordinate activities with the Cyber Security working group in order to adopt review guidance relating to SDO and cyber security into RG 1.152 Revision 4 as necessary.

The IEEE 603 standard generically references IEEE 7-4.3.2 as additional guidance for DI&C. The IEEE 7-4.3.2 NRC working group will closely coordinate with the IEEE 603 NRC working group on future updates.

The regulatory infrastructure review group may determine the need for additional provisions affecting Regulatory Guide (RG) 1.152 or IEEE 7-4.3.2, or may establish a need for additional task working groups. The 7432 Task Working Group will interact as appropriate with the infrastructure review group and with any new task working groups that may be created.

5. Evaluate Regulatory Action Concerning Review of Cyber Security Design Aspects

Introduction

The purpose of this plan is to determine how reviews of cyber-related design information should be evaluated as part of the licensing process.

Background

Operating reactor licensees and Combined License (COL) applicants are currently required to submit a cyber security plan to be reviewed by the NRC in accordance with 10 CFR 73.54. However, they are not required by regulation to submit design information to address cyber security requirements as part of the NRC licensing review. Thus, for new reactors, the first opportunity for the NRC to inspect the implementation of the cyber security program is after the COL is issued. This inspection typically occurs after the design certification applicants have completed the design of systems that support safety, security, and emergency preparedness (SSEP) functions, particularly systems that perform safety and important-to-safety functions. For operating reactors, design information becomes available for inspection when a system is entered into the operating reactor licensee's cyber security program. This increases the regulatory uncertainty for COL holders and operating reactor licensees, who are ultimately responsible for ensuring their systems comply with the NRC's cyber security regulations (e.g., 10 CFR 73.54), and may have to address vulnerabilities in system's design after the design has been completed. The NRC received feedback from some design certification applicants that staff review of cyber security design features should be performed during design certification application reviews.

The Advisory Committee on Reactor Safeguards (ACRS) has also raised concerns associated with the control of access to plant equipment and networks. Specifically, the ACRS stated that control of access to critical plant systems should be reviewed as part of design certifications and COL application reviews. ACRS made the same recommendation relative to licensing reviews of operating plant digital instrumentation and controls (DI&C) upgrades. ACRS has indicated that such a review should consist of evaluating the design of the communication flow enforcement device between cyber security defensive architecture Level 4 and Level 3, and between Level 3 and Level 2, to verify this device maintains unidirectional flow from higher security levels to lower security levels. To address this ACRS concern, the EDO has committed to develop a SECY paper seeking Commission direction on the particular issue of evaluating design features to address cyber security during licensing and design certification application reviews (ML14071A121).

NRC staff understands that 10 CFR 73.54 does not require licensees or applicants to submit cyber security design information to the NRC. However, staff further understands that the NRC has the regulatory authority to review voluntarily submitted cyber security design information and provide insight on its potential impact on a licensee's/applicant's required cyber security program. The NRC also has the appropriate regulations and regulatory authority to ask the licensee/applicant questions related to the potential security impact of DI&C design elements. However, the SRP does not currently include sufficient guidance to enable staff to conduct these reviews.

Objectives

The objective of this effort is to determine whether NRC should evaluate cyber security design information and their potential security impact as part of the licensing process.

The final determination will be summarized in an Informational SECY paper to be submitted to the Commission. This Informational SECY paper will be provided to the ACRS prior to its submission to the Commission.

The desired outcome is the development of a new subsection to the Standard Review Plan (SRP), and any other related regulatory documents, to provide review guidance for performing cyber security design reviews.

Proposed Actions

Activity	**Schedule**
1. Complete an evaluation of the current regulatory scope regarding cyber security design	March 01, 2016
2. Public engagement & external stake holder interaction	April 09, 2015 August 18, 2015 May 2016 June 2016 TBD (throughout SRP Development)
3. Complete draft Informational SECY	May 2016
4. ACRS	May 2016 (Submit draft SECY) June 2016 (Meeting)
5. Information SECY to the Commission	October 2016
6. Finalize SRP updates	TBD

Status

(as of March 4, 2016)

The Working Group, which consists of representatives from NSIR, NRR, NRO, and RES, is in the process of drafting the Informational SECY paper and development milestones for the SRP update effort.

Potential Regulatory Challenges and Policy Issues

The proposed approach for addressing cyber security design is not consistent with the ACRS' initial recommendations that cyber security be addressed through a regulatory requirement. Final submission of the Informational SECY paper may be delayed due to ACRS' concerns.

Interactions with other Action Plan Items

Because part of the intended process for cyber security design reviews will likely be performed concurrently with DI&C safety reviews, the content of the draft SRP may be affected by the IEEE 7-4.3.2 Guidance Development effort.