U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agency-wide Digital Instrumentation and Controls Action Plan to Improve Regulatory Processes

Draft DI&C Path Forward Action Plan

Draft for Public Release

NRC staff tour an all-digital control room at the Taiwan Electric Company Lungmen Nuclear Plant in 2010

Agency-wide Digital Instrumentation and Controls Action Plan to Improve Regulatory Processes

Draft DI&C Path Forward Action Plan

ADAMS Accession No.: ML16014A085

OFFICE	NRR/DE/EICB	NRO/DE/ICE	RES/DE/ICEEB
NAME	DRahn	JZhao	BDittman
DATE	01/ /2016	01/ /2016	01/ /2016
OFFICE	BC: NRR/DE/EICB	BC: NRO/DE/ICE	BC: RES/DE/ICEEB
NAME	MWaters	TJackson	TBD
DATE	01/ /2016	01/ /2016	01/ /2016
OFFICE	DD: NRR/DE	DD: NRO/DE/	DD: RES/DE
NAME	JLubinski	MMayfield	BThomas
DATE	01/ /2016	01/ /2016	01/ /2016

OFFICIAL RECORD COPY

Executive Summary

The USNRC has successfully completed safety evaluations of the instrumentation and controls aspects of power reactor designs for many years. To do so, the NRC staff uses tools, such as Chapter 7 of the Standard Review Plan, NUREG-0800, along with recently-developed interim staff guidance (DI&C-ISGs) pertaining to the use of digital technology in safety applications to assure the quality and uniformity of safety reviews. These tools describe the technical acceptance criteria the Digital Instrumentation and Control (DI&C) reactor technical reviewers apply when evaluating license amendment requests and license applications. The staff uses these tools in conjunction with a formal license submittal and evaluation process to ensure that proposed digital instrumentation and control designs are consistent with the regulations, codes, and standards, commensurate with the importance of the safety functions to be performed.

From 2007 through 2011, the NRC staff worked with stakeholder counterparts, under the charter of a Digital I&C Steering Committee, to enhance the review tools available to the staff to include additional review guidance specific to the implementation of digital technology. Many of the seven new interim staff guidance documents (ISGs) that were developed under the Steering Committee have helped to provide clarity in the application of the staff's review guidance when applied to the implementation of various aspects of digital technology. While the use of these new tools and enhanced evaluation process has enabled the staff to successfully conduct its evaluations, now that they have been in use for some time it has been observed that further improvements can be made in the quality of these tools, and in the interfaces that should take place between the staff and license applicants, to enable smoother and more efficient licensing evaluation processes.

This document describes the NRC staff's action plan for improving the Digital Instrumentation and Control (DI&C) licensing evaluation process to make it easier for the staff to conduct its technical reviews of licensee and applicant submittals, thus enabling the licensing process to be more reliable and predictable for industry stakeholders. The staff identified aspects of the current licensing process (including updating the policies, application material submittal practices, review procedures, and review tools) for which efforts expended to make improvements could result in an overall improvement in the efficiency in licensing or subsequent inspection processes. Each improvement area is described within this document, along with a Path Forward Action Plan for carrying out the process improvement.

This initial Revision 0 version is a Draft Working Document for discussion and approval. Once this version has been approved by a NRC steering committee, future versions will contain an update of each topic to track the progress being made on each of the individual action plans. This draft outlines the specific issues that were identified to enable planning for the review guidance enhancement.

Introduction

The proper implementation of DI&C at operating plants is one of the most important technical challenges currently facing the US nuclear industry. Industry stakeholders desire to take advantage of the many safety and reliability benefits that can be gained through the implementation of digital I&C safety systems, but some are hesitant to pursue licensing actions unless regulatory uncertainty can be reduced. Some industry stakeholders (licensees, applicants, and vendors) have expressed concern that the current digital instrumentation and controls (DI&C) licensing process for power reactors is cumbersome and inefficient, and/or unpredictable. While the current staff review guidance for digital safety controls are considered adequate, staff has also identified areas in which policy or guidance could be improved. The NRC management encouraged the staff to evaluate its current processes and identify any issues, policies, requirements, and practices that should be considered as candidates for possible regulatory process improvement. The staff focused on enhancing licensing to achieve a more reliable, efficient, and effective regulatory process for evaluating new DI&C technologies that will be proposed by licensees and applicants for the operating and new reactor fleets.

The NRC staff performed an assessment of its experience in evaluating digital safety system designs submitted over the past seven years as part of license applications or amendments, and identified specific policies, guidance, practices, processes, and tools used in the licensing and oversight process that could be considered as candidates for improvement. This DI&C Path Forward Action Plan presents the specific topical challenges to be addressed, along with a proposed plan for resolving each topic. Some of these issues were identified as “Near-term,” while others were considered “mid-term” or “long-term” items to be addressed. Each plan identifies the expected outcome of each issue resolution. Once agreed upon, further efforts will be expended to identify the resources needed to accomplish them, key milestones to be achieved, and specific deliverables to be produced. The overall goal of the DI&C Path Forward Action Plan is to modify the DI&C licensing process in a manner that maintains a high degree of safety and that increases efficiency, supports a more risk-informed/consequence-based approach where appropriate, and improves regulatory effectiveness and predictability.

Background

In the operating nuclear fleet, I&C equipment obsolescence management is becoming significantly burdensome to licensees, and if not resolved, has the potential to impact the safety of operations. The INPO scram data for 2013 indicates that for operating reactors, the rate of scrams due to safety system equipment failures is increasing. NRC operating experience data also indicates that spurious ESF Actuations due to equipment failure or human error during safety system surveillance or maintenance is also increasing. The implementation of digital technology in safety control systems is desirable to resolve obsolescence issues, increase safety control system reliability, reduce opportunities for human error during surveillances, and reduce maintenance costs.

Industry stakeholders have stated the process for DI&C safety system licensing is not flexible or "scalable," based on risk information, and lacks efficiency. These stakeholders voiced a need for a "graded approach" to licensing based on safety significance, and a need for additional guidance for implementing a commercial grade dedication process that does not rely upon the Branch Technical Position (BTP) 7-14 software quality processes or the "100% testability" clause to address the potential for common cause software failure. Industry stakeholders also expressed the need for NRC staff to re-examine what should be an appropriate process for the regulatory treatment of potential common cause failures. For example, some stakeholders expressed they do not believe sufficient guidance is available to define "simple systems" capable of 100% testing to address the potential for common cause failure due to software error, and they believe strict adherence to the Institute of Electrical and Electronics Engineers (IEEE) software quality standards is unnecessarily burdensome. Industry representatives state the overall cost of developing a safety related digital control system is high and the efficiency of the current process needs improvement. Finally, where feasible, industry stakeholders wish to perform some types of digital safety system upgrades, changes, or modifications via the 10 CFR 50.59 safety evaluation process rather than the LAR process.

New reactor designs reviewed by the NRC are fully utilizing modern I&C design approaches and technology. Such approaches and technology offer many benefits to nuclear power plant operation, including increased reliability and diagnostics and improved human-machine interfaces. However, use of such approaches and technology has challenged the safety review by introducing potential hazards to the design as a result of the highly-integrated I&C systems. For example, the staff spent a significant level of effort during recent licensing reviews to evaluate data communication independence, the potential for spurious actuation of safety and non-safety control systems, and the control of safety-related equipment from non-safety-related controls. Current assessment approaches and review guidance do not efficiently address the continually evolving nature of digital technology, and they do not optimize the benefits offered by new design approaches and technology while, at the same time, addressing potential hazards that may be introduced. Experience with new reactor I&C designs has shown that, in several cases, applicants proposed new and unique technology or design approaches that were not sufficiently justified from a safety perspective, and required additional staff efforts to achieve resolution.

Intended Maintenance and Use of this Plan

This plan is to be maintained by an assigned DI&C Regulatory Process Improvement Working Group (DI&C WG) under the supervision of a Steering Committee (SC), composed of the three Division Directors of the Division of Engineering within the offices of RES, NRR, and NRO. The DI&C WG will be responsible for formulating the specific Actions identified under each problem statement described herein. Ownership of each Action Plan will be assigned to appropriate NRC Office leads. This plan will then 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 these plans that are identified during these periodic reviews shall be agreed upon by the three Engineering Division Directors within NRR, NRO, and RES.

Table of Contents

Reference Information

1. Content and Schedule of DI&C Application Submittals (Near-term)

Challenge:

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.

Supplemental Information

In a previous effort (2007 – 2011 time frame) to improve the quality of license amendment requests for proposed digital upgrades of safety related control systems, the staff prepared Interim Staff Guidance (ISG) document DI&C-ISG-06, "Licensing Process." In addition to describing in detail the evaluation criteria that is used by the staff to review such licensing submittals, this document contains an enclosure describing the various phases of the staff's licensing process, specific information the staff needs for its evaluation of such license amendment requests during each phase, and provides the staff's desired schedule for the submittal of the various types of licensing information. Lessons learned through a pilot use of this ISG have indicated that the descriptions of which documents need to be submitted on the docket could be further enhanced, and the type of information contained within each document type could be better explained. Also, the staff found that it does not need all the information that was identified in the type of documents listed in the Enclosure to ISG-06, but only a portion of it. Information that is currently in ISG-06 should be updated to reflect these lessons learned, and the information should be placed into permanent guidance.

As described in 10 CFR Part 52, applicants for new reactors are required to submit a level of design information sufficient to enable the NRC staff to evaluate the applicant's proposed means of assuring the construction will conform to the design, and to be able to reach a final conclusion on all safety questions associated with the design. The level of DI&C design information provided to the staff constitutes the licensing basis as described in the proposed final safety analysis report (FSAR), which should be available at the time the application is submitted to the NRC. Typically, applicants can demonstrate they meet NRC requirements at the DI&C architectural level, and thus, the level of design information and analysis would be commensurate with the architectural level. However, the staff's experience in previous new reactor reviews revealed that applicants may choose to address NRC requirements at a lower level in the DI&C design (e.g. hardware and software). In such situations, the staff found the applicants did not have the requisite level of design information and analysis at that level of the design. As a result, applicants either modified their design to meet NRC requirements at a higher level of the design or the review became significantly protracted to gain the necessary level of design information. Guidance for reviews performed for 10 CFR Part 52 licensing submittals should be updated to ensure that an applicant's design approach is adequately described and the level of design detail submitted is commensurate with the approach the licensee has taken to meet NRC requirements.

Proposed Actions

- Identify and define lessons learned from the use of Enclosure B to ISG-06, and refine the matrix of information to be submitted for each tier and phase of the licensing review process. Prepare a revised document submittal schedule for license amendment requests.

- Summarize recommendations arising out of Diablo Canyon pilot plant effort. Prepare Lessons Learned Report outlining findings. Identify whether FAT Report findings are required to make licensing decision, or whether a periodic staff "safety findings status letter" can provide safety decision status. Meet with stakeholders to discuss arguments for and against the use of a periodic "safety findings status letter".

- Propose modifications to industry/staff guidance for Part 52 submittals to highlight the need to provide new reactor design information and analysis at a level that is commensurate with the design level where NRC requirements are fulfilled.

- Identify differences and gaps between Part 50 and Part 52 processes, and potential improvements that can be made to existing licensing processes based on licensing experience to date.

- Update Chapter 7 of the Standard Review Plan—NUREG-0800 (SRP), either through text changes, subchapter additions, or new branch technical positions, to contain the information submittal schedules for each type of DI&C system to be evaluated.

Desired Outcome

Licensing Evaluation Efficiency Improvement

The purpose of these actions is two-fold: a) to provide the information needed by the NRC staff technical reviewer at the appropriate stage of the evaluation, to facilitate an efficient review and minimize the need for RAIs requesting additional information; and b) to clearly define for potential license applicants, design certification vendors, and licensees contemplating digital safety system upgrades what types of information are needed at each stage of the evaluation, so that their licensing submittal package can be prepared sufficiently in advance of the staff's needs.

2. Evaluation of NRC Policy on Potential CCF due to Software Error (Near-term)

Challenge:

The current regulatory treatment and acceptance criteria dealing with the potential for common cause failure due to software error 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 software and hardware development processes have been employed—especially for systems containing localized embedded digital I&C components.

Supplemental Information

Historical guidance provided by the NRC staff, which has been used by licensees for performing 10 CFR 50.59 evaluations of analog-to-digital or digital-to-digital modifications, has insufficient details regarding a) how to address the potential for common cause failure (e.g., vulnerabilities within identical software in redundant channels, effects of EMI/RFI on redundant channels, faults within identical revisions to software on multiple redundant channels, or errors made within processes for implementing configuration changes), and b) how to evaluate the possibility of a malfunction with a new result. Specifically, industry stakeholders are looking for clearer NRC staff guidance on methods for analysis of the potential for common cause failure due to software error. For example, for 10 CFR 50.59 evaluations, licensees need better guidance for responding to the question in paragraph 50.59(c)(2)(vi) regarding whether a LAR would be required because the potential for common cause failure due to software error was not adequately addressed, and the change could create a malfunction with a result different than explicitly described in the UFSAR. Stakeholders would like to have improved regulatory guidance for performing common cause failure evaluations and criteria for evaluating the safety of FPGAs, CPLD's, and similar programmable logic devices included within proposed designs.

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 (i.e., diversity & testability – See BTP 7-19 Section 1.9, "Design Attributes to Eliminate Consideration of CCF"). These two BTP 7-19 criteria are different from criteria used in NEI 01-01 (high-quality software development process). It is expected that industry will propose additional criteria within a digital design guidance document they are expecting to receive from EPRI later this year (2015) to "eliminate" consideration of CCF.

The Commission's SRM associated with Item II.Q of SECY 93-087 states:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have adequately been addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of safety grade displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

Proposed Actions

- Perform an evaluation of current NRC policy in an effort to either modify or affirm the NRC's current digital system CCF policy as discussed in Item II.Q of the SRM to SECY 93-087, and Branch Technical Position (BTP) 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems." This policy is restated in Chapter 7, "Instrumentation and Controls," of NUREG-0800. Determine whether significant technological or systems development process changes have occurred in the intervening years between 1993 and the present that would influence or validate a decision to modifiy the existing policy. Determine whether there is adequate evidence and/or a sufficient regulatory basis to support the initiation of rulemaking to require the performance of a Defense-in-Depth and Diversity (D3) analysis to accompany the safety analyses and evaluation packages for new digital I&C system implementation or upgrades.

- In parallel with this effort, maintain appropriate interfaces with industry stakeholders (e.g., NEI, Owners Groups, EPRI, etc.). Identify what activities, if any, these groups are performing which have the potential to contribute to either the technical basis for modifying the SECY 93-087 policy, or to the development of a future regulatory guide and staff review guidance. Such guidance should address appropriate acceptance criteria for preparing D3 analyses for evaluating digital I&C safety system upgrades and new digital I&C safety system designs.

- Prepare a technical basis document and a SECY paper outlining the technical basis for either modifying the existing CCF policy as described in the SRM to SECY 93-087 and in BTP 7-19 of the Standard Review Plan (NUREG-0800), or, for establishing a new rule regarding the appropriate application of D3 for use in developing and applying digital I&C safety systems. The technical basis paper should include a discussion of the evaluation of the potential for CCF in available documentation on

D3 methods and experience from nuclear power and non-nuclear industries, capture of expert knowledge and lessons learned, determination of best practices, and assessment of the nature of common-cause failures (CCFs) and current and past assumptions regarding the likelihood of software based common-caused failures and their consequences. The investigation leading to the development of the technical basis paper should include an evaluation of the impact of the evolution of technology in digital systems used in safety applications in the nuclear industry in the past few years, including the use of field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs). The investigation should provide insights on the consequences of the use of different technologies, different approaches within the same technology, and different architectures within the same technology.

- As appropriate, prepare a proposed modification to the existing SRM to SECY 93-087 policy statement. Through a corresponding SECY paper, initiate a rulemaking, if appropriate, to implement the findings outlined in the technical basis paper developed in Action Item 2 above. Carry out this process to include stakeholder input at appropriate milestones, commensurate with the findings in the technical basis paper.

- As appropriate, prepare draft regulatory guidance and accompanying review guidance addressing appropriate acceptance criteria for preparing D3 analyses for evaluating digital I&C safety system upgrades and new digital I&C safety system designs. Incorporate lessons learned from recent safety evaluations of proposed digital upgrades at operating plants and installation of new digital safety systems for proposed new reactor plants. For example, consider including methods for identifying the appropriate plant anticipated operational occurrences (AOOs) and design basis events (DBEs) to be evaluated. Provide criteria for design of enhancements that may be needed for initiatiating safety functions at the system level. Identify appropriate criteria enabling licensees and staff reviewers to establish whether the minimum level of diversity is being provided in a digital I&C safety system under evaluation.

- Review for possible endorsement IEEE Standard 7-4.3.2-2015, which contains guidance for conducting defense-in-depth and diversity analyses for software-based digital upgrades. If appropriate, revise Regulatory Guides 1.152 and 1.153 to reflect the 2015 or later versions of IEEE 7-4.3.2, and provide references to new guidance or rules arising from this effort.

Desired Outcome

Clarity of NRC policy and NRC staff position regarding how software CCF is to be addressed for systems and components. This clarity should serve as an improvement in licensee efforts to evaluate the proposed implementation of digital safety systems and components, and enable licensees and applicants to focus efforts to address such CCFs, which should result in efficiency in the licensing process.

3. NRC Assistance in Updating Industry Guidance for DI&C 10 CFR 50.59 Modifications (Near-term)

Challenge:

Guidance for the 50.59 screening and evaluation of digital I&C systems is ambiguous and weak in some areas, contributing to several licensees improperly performing 50.59 analyses for modifications of I&C systems using digital technology. Greater clarity in the implementing guidance is needed.

Supplemental Information

NRC inspections of 10 CFR 50.59 plant digital modifications revealed that inadequate industry guidance for performing DI&C modifications resulted in several plant modifications being performed that could have required a license amendment request. The NRC staff has held several public meeting discussions with industry representatives on this subject and provided NEI with a letter detailing eleven areas where the industry guidance should be improved. An industry task force is working to improve the implementing guidance.

Proposed Actions

- Maintain close contact with the cognizant NEI project leads for the 50.59 Working Group and the DI&C Working Group to identify opportunities to evaluate and comment on planned changes in guidance for performing 50.59-related upgrades using digital technology. Also, maintain contact with the NEI Digital I&C Working Group to identify opportunities for evaluating digital I&C design guidance pertaining to design features for minimizing or eliminating CCF vulnerabilities. At present, the staff's understanding is that NEI plans to develop a new Appendix D for NEI 96-07 that would contain guidance for addressing in detail three of the eight safety evaluation questions in 10 CFR 50.59 that are particularly applicable to the introduction of new digital technology. Concurrently, EPRI is developing licensee guidance for designing new digital systems or upgrades to existing systems, which will contain criteria for evaluating proposed digital system designs to either eliminate the potential for CCF vulnerabilities or mitigate the effects of failures of digital systems due to the potential for CCFs.

- When the new Appendix D for the new NEI 96-07 revision is available in draft form for NRC review, perform a review in light of current NRC staff understanding of the applicable regulatory criteria and guidance. Provide timely feedback of the staff's comments on this draft to stakeholders. Identify any areas where the proposed draft may deviate from current NRC policy or guidance. Determine whether NRC policy or guidance may need to be modified, as a result.

- Identify impact on NRC policy or guidance documents and develop remedies, where appropriate.

Desired Outcome

Clarity of mutual industry/NRC staff understanding that NRC staff guidance is being properly translated into industry guidance for performing 10 CFR 50.59 evaluations of Digital I&C plant modifications.

4. Development of IBR Rulemaking for IEEE Std 603-2009 into 10 CFR 50.55a (Near-term)

Challenge:

The industry consensus standard currently incorporated by reference (IBR) in 10 CFR 50.55a, IEEE Std 603-1991, does not address certain design concepts that the introduction of newer technologies makes possible. IEEE Std 603-1991 does not include criteria for design concepts such as data communications, integration of systems via shared resources, consolidation of functions, and systems self-diagnostics. In addition, some applicants and licensees have expressed interest in licensing systems to newer standards.

Supplemental Information

The staff developed a proposed rule to incorporate the new version of IEEE Std 603 (2009) into regulation by reference. The proposed rule addresses design concepts that digital technology makes possible. In part, the rulemaking proposed to enhance some of the provisions within the standard by incorporating different criteria for new and operating reactors regarding the assurance of division/channel independence. As described below, staff review experiences under Part 52 (NRO) and Part 50 (NRR) have generated different lessons-learned. The different criteria for independence within the proposed rulemaking reflects these unique experiences.

New reactors licensed under the 10 CFR Part 52 process are not required to provide design implementation details at the time of design certification. As stated in § 52.47, the application must contain a level of design information sufficient to enable the Commission to reach a final conclusion on all safety questions associated with the design before the certification is granted. The requirements proposed by this rule would allow new reactors to demonstrate communications independence with a level of design information at the hardware architecture level without the need to provide detailed design implementation information, which is consistent with the requirements of § 52.47. If a new reactor applicant chooses to implement software-based solutions to enforce communications independence, additional design details and implementation information (e.g., software code, testing data, Factory Acceptance Test (FAT) results, etc.) may be needed in the licensing basis to demonstrate the software-based solutions to enforce communications independence are safe. Based on experience of new reactor I&C systems reviews conducted prior to the development of this proposed regulation, many applications did not have this level of information available at the time of design certification or licensing due to the state of maturity of their designs.

It is preferable from a safety and licensing point of view to design systems to promote elimination of failure modes as opposed to incorporating strategies to mitigate the results of failures. New reactor designs are able to more readily accommodate the rule as these designs do not have a current licensing basis for an existing system that may impact the particular design. However, for current reactors, this requirement does not appear to be justified from a safety standpoint. Therefore, certain clauses proposed in the rule do not apply to currently

operating nuclear power plant licenses or operating licenses whose construction permits were issued before the effective date of the rule.

At various public meetings, including DI&C Working Group meetings, NRC staff briefed stakeholders about the pending rulemaking. The staff also held a public meeting on the proposed rulemaking prior to providing its recommendation to the Commission.

During public interactions, industry stakeholders expressed concerns regarding different independence requirements for new and operating plants. One industry stakeholder also suggested, if the different criteria resulted from the absence of details under Part 52, then the proposed rule should enable applicants to have the option of providing those details under Part 52, in order to allow for the continuation of a common technical basis between new and operating plants. Further, in an October 30, 2015 letter from NEI to NRC Chairman Burns, NEI President Anthony Pietrangelo expressed concern that the "proposed rule could negatively impact the path to regulatory stability in licensing digital upgrades offered in current regulatory guidance (e.g. DI&C-ISG-04) by adding conditions on the use of IEEE 603-2009. These conditions include treating new plants and operating plants differently and expanding the scope of applicability to all safety systems rather than just reactor protection systems. Implementation of these changes would unnecessarily increase the cost of digital upgrades without a corresponding safety benefit."

Proposed Actions

- Provide the proposed rule and draft regulatory guidance for Commission review (complete)

- Conduct public workshops for proposed rule (if approved for publication by the Commission)

- Address public comments on the proposed rule and draft regulatory guidance and provide the final rule to the Commission for consideration.

Desired Outcome

An IBR of IEEE Std 603-2009 into 10 CFR 50.55a and accompanying regulatory guidance in order to streamline approval of applications and amendments implementing new digital technology.

5. Guidance for Evaluation of Highly-Integrated Digital Technologies (Mid-term)

Challenge:

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 can result from highly-integrated I&C systems.

Supplemental Information

New reactor designs reviewed by the NRC are fully utilizing modern I&C design approaches and technology. Such approaches and technology offer many benefits to nuclear power plant operation, including increased reliability and diagnostics and improved human-machine interfaces. However, use of such approaches and technology can also challenge the safety review by increasing the potential for design faults because of the highly-integrated nature of the I&C system design. Challenges include 1) obtaining a clear understanding of the potential for adverse interactions between individual components and systems, including interactions between externally-connected systems and components to the DI&C safety system when in a faulted condition; 2) understanding the limitations of fault tree analysis (FTA) methods and Failure Modes and Effects Analyses (FMEA) to identify systemic defects in highly- integrated/ interconnected systems; and, 3) finding the means to appropriately characterize highly-integrated/interconnected system behavior, so it is properly addressed in and bounded by Chapter 15 safety analysis.

During reviews of highly-integrated I&C systems of new reactor designs, the staff spends significant time and resources addressing, for example, data communication independence, potential for spurious actuation of safety and non-safety control systems, and control of safety-related equipment from non-safety-related controls, in part, due to the challenges. Current assessment approaches and associated review guidance do not effectively address these challenges, and the continually evolving nature of digital technology appears to increase the impact of the challenges. 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.

Proposed Actions

- The DI&C WG shall meet to designate a team to assess current guidance and identify candidate methods to develop additional guidance to enhance the ability of technical reviewers to address the criteria in the SRP Chapters 7.0 through 7.9 for highly-integrated control systems. The team will then identify whether outside contractor support would be needed to develop the guidance, and determine a realistic schedule for completion of this guidance. Candidate areas for improvement and assessment could include, but are not limited to:

- Guidance for addressing the potential for multiple spurious actuation of plant equipment connected on common network architecure
- Use of hazard analysis techniques to address highly-integrated, DI&C systems
- Use of DI&C system modeling tools to better analyze for potential design faults
- Guidance for addressing the unique characteristics of embedded digital devices
- Evaluation of regulatory processes and criteria applied by other industries requiring safety-critical use of digital technology and how such processes and criteria may be applied to the nuclear industry
- Application of a safety case approach as a means to provide DI&C design information in a structured manner

- Implement the recommendations of the DI&C Working Group.

- The recommendations for each item may take the following general form:

  - Establish a Technical Basis (if it does not yet exist)
  - Formally document the Technical Basis
  - Engage stakeholders to identify an appropriate number and scope of related regulatory guides (or other regulatory infrastructure documents)
  - Develop regulatory guides and/or other regulatory infrastructure documents (e.g., NUREGs), as identified
  - Update SRP and/or create alternative regulatory infrastructure document to appropriately reference the new guidance.

Desired Outcome

Improved regulatory guidance for licensee/applicants submittals (e.g., hazard analysis-focused, structured safety argument) that enables an efficient and effective staff safety evaluation of highly-integrated I&C systems, when proposed. Improved review guidance for staff that enables more efficient and effective safety evaluations of highly-integrated control systems.

6. Regulatory Infrastructure Improvements (Long-term)

Challenge:

The regulatory infrastructure (regulatory guides, standard review plan, branch technical positions, etc.) makes it difficult to achieve efficient, effective and consistent staff implementation, for a number of reasons. The infrastructure: a) is considered cumbersome, b) is not well organized and is somewhat redundant, c) does not allow for graded approaches based on safety significance, d) is not updated frequently enough to address advancements in technology, and e) could be better integrated with other areas/disciplines of regulatory evaluation.

Supplemental Information

The regulatory infrastructure supporting the evaluation of DI&C safety systems is very large. The standard review plan in Chapter 7 of NUREG-0800 is challenging to use, in the following ways:

- Review guidance for newer technologies (e.g., FPGAs, CPLDs), is not provided, so technical reviewers must make case-by-case judgments for safety reviews.
- Review guidance is not updated frequently enough to keep up with changes to NRC policy evolving from steering committee processes, or new revisions to applicable industry codes and standards.
- Review guidance is not provided for evaluating and crediting operating history or for evaluating the safety assurance of proposed designs that are based on alternatives to the NRC regulatory guidance, such as the use of international standards. Review guidance is needed regarding methods for evaluating alternatives to the underlying regulatory guidance referenced in the review plan.
- The SRP does not distinguish among minimum design criteria required to be applied for safety systems with high safety significance versus safety systems with low safety significance. Example: Post-accident monitoring systems are reviewed at the same level and manner as RPS/ESF protection systems.
- The SRP provides minimal guidance for reviewers to evaluate the potential impact of highly-integrated digital safety (and non-safety) system failures on the adequacy and completeness of Chapter 15 event analyses to ensure the design basis for safety systems is and remains bounded by the analysis.
- The format of Chapter 7 is function-based, rather than safety design criteria-based. The appropriate safety review acceptance criteria are repeated from function to function, and are unnecessarily repetitive for reviews of highly-integrated DI&C designs. A streamlined version (e.g., DSRS format) is needed to provide efficiencies in review processes.
- More guidance is needed for reviewers to evaluate the impact of digital I&C systems on the application review aspects of other NUREG 0800 chapters (e.g., Chapter 15—safety analyses, Chapter 16—technical specifications, Chapter 17—QA, Chapter 18—Human Factors, and Chapter 19—PRA).

- Neither Chapter 7 or 17 provides sufficiently detailed acceptance criteria or review guidance regarding an appropriate commercial grade dedication process to be used for the application of high-quality commercially-developed digital system designs in safety related applications.

Proposed Actions

- The DI&C WG shall meet to designate a team to assess current content of the SRP and regulatory guidance and identify potential methods for consolidating or organizing this guidance to enhance the ability of technical reviewers to address the review criteria. Consideration shall be made as to whether the approach taken in the Design-Specific Review Plans (DSRPs) for the review of small modular reactor design certification applications could be utilized in the SRP. The team will then identify whether outside contractor support would be needed to facilitate the development of the guidance, and determine a realistic schedule for completion of this guidance.

- The recommendations of the DI&C WG will be implemented.

- The recommendations may take the following general form:
  - Engage stakeholders to obtain input regarding options for improving the SRP that would benefit I&C system designers, as well as licensing engineers, and NRC staff license reviewers. Incorporate lessons learned from licensing reviews of recently-completed license applications/amendments and the NuScale DSRS.
  - Identify the types/scopes of review standards that would best support the goals, and then prioritize and select a pilot project effort.
  - Develop a pilot review standard method development project that considers the safety-significance of the kind of system within scope.
  - Determine corresponding regulatory infrastructure (or licensing update) required to appropriately reference applicable sections of the review standard.
  - Repeat process above for each proposed review standard of sufficient priority.

Desired Outcome

A streamlined set of review guidance should enable all technical reviews to be completed more efficiently.

7. Guidance for Evaluation of Proposed Alternatives to Regulatory Guides and Endorsed Standards (Mid-term)

Challenge:

More guidance is needed for NRC technical reviewers to evaluate licensee-submitted proposed alternatives to the criteria in regulatory guidance and endorsed codes and standards, applicable to the licensing of digital I&C systems and components. These gaps in guidance create a challenge for technical reviewers seeking to make appropriate and consistent engineering judgments on the safety assurance of proposed alternative solutions for meeting applicable acceptance criteria presented in regulatory guides and the SRP.

Supplemental Information

Licensees are reluctant to propose alternatives to codes and standards endorsed in NRC guidance or incorporated by reference in the regulations. For example, certain IEC standards may address a design criterion in a different manner than US standards, but are still considered effective by European regulators. The acceptance criteria in Regulatory Guides used by licensees to design safety system upgrades could be evaluated and adopted more frequently so that licensees and applicants could take advantage of developments in new technologies, testing and qualification methods, or inspection and maintenance practices identified in the updated or alternative codes and industry standards. More guidance is needed for technical reviewers of applications to evaluate the acceptability of proposed alternative design criteria.

Proposed Actions

- The DI&C WG shall meet to designate a team to survey and assess review processes and practices employed by nuclear power plant regulators in other countries and by regulators of public safety design requirements in industry sectors other than the nuclear power sector. The team will identify whether outside contractor support would be needed to identify the methodologies used to implement safety reviews for those sectors. (Simultaneously, the team could also consider ways to harmonize review methods with those of other nuclear regulators.) Then the WG will formulate a plan to incorporate the best practices of those other sectors.

- The recommendations of the DI&C WG will be implemented.

- The recommendations may take the following general form:
  - Engage stakeholders to scope a generic method for the evaluation of alternatives as an acceptable means to satisfy §50.34 (h).
  - Develop the generic process for the evaluation of alternatives into a draft review standard, including FRN and public comment cycle.
  - Determine how to reference the new review standard (SRP or licensing process).

- Pilot use of the draft review standard using a broad-based licensee interest in the potential use of an alternative, as follows:
  - Obtain a topical report that addresses the draft review standard
  - Evaluate the alternative using the draft review standard
  - Identify and document lesson-learned and incorporate into a revision of the draft review standard.
- Repeat the steps above for additional broad-based licensee requests to use an alternative.

Desired Outcome

Implementation of alternative review processes could serve to enable a more efficient evaluation of proposed alternatives to the NRC staff's review criteria.

8. Improvement in Regulatory Consistency from Licensing to Inspection (Mid-term)

Challenge:

Representatives of the US nuclear industry 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. For example, feedback from industry representatives indicates NRC staff interpretation/application of 10 CFR 50.59 criteria has changed or is inconsistent between regional inspectors and headquarters staff.

Supplemental Information

It is not clear the inconsistency expressed by the stakeholders is technically significant. However, there is currently room for greater interaction on generic digital I&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.

Proposed Actions

- The DI&C WG will first meet to identify, on a topic for topic basis, whether there is significant technical inconsistency between licensing and inspection staff.
- If it appears that actual technical inconsistencies exist, the reasons for this will be explored by the WG, and if necessary, the WG will identify a sub-group to develop specific problem statements outlining the areas of inconsistency that are found, and develop action plans for resolving them.
- The recommendations of the DI&C WG will be implemented.
- Licensing staff and headquarters inspection staff will organize periodic meetings (e.g., bi-monthly) with regional digital I&C inspection experts to discuss specific I&C topics of mutual interest. The purpose of these teleconferences would be to improve understanding and reach alignment on the technical basis for specific DI&C-related regulatory findings.

Desired Outcome

Technical consistency among licensing and inspection staff.

9. Early-Development Stage Evaluation of Cyber Security Aspects of Proposed DI&C Designs (Near-term)

Challenge:

The consideration of cyber security early in the design process can help licensees and applicants to avoid unsecurable designs and reduce regulatory uncertainty. However, the NRC cyber security rule is programmatic and does not provide a process for NRC to review cyber security design information during licensing reviews. Absent a timely evaluation against cyber security criteria during the development phase, concerns remain that cyber vulnerabilities potentially introduced during the development process could adversely impact safety.

Supplemental Information

Current NRC policy and regulations separate a design's safety evaluation from its programmatic security evaluations. Programmatic security evaluations occur later than control of access safety evaluations. Designs that do not readily accommodate meeting cyber security criteria may require modifications. Modifications could cause a design's safety evaluation to be revisited. As such, late modifications increase the likelihood that application-specific review expertise will go unleveraged, which would exacerbate inefficiencies. An early limited and targeted security-related evaluation can prevent increased inefficiencies from occurring late or in the critical path of applicant/licensee efforts. This would eliminate delays and also mitigate the potential of late schedule pressure adversely impacting the continued validity of prior safety conclusions, without such an impact being recognized.

Currently, operating reactor licensees and COL applicants are required to submit a cyber security plan to be reviewed by the NRC. However, they are not required to submit design information used to address cyber security requirements for NRC licensing review. 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 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 who will have to address vulnerabilities in system's design after the design has been completed. Due to this regulatory uncertainty, the NRC received feedback from design certification applicants that staff review of cyber security design features should be performed during design certification application reviews.

Further, the Advisory Committee on Reactor Safeguards (ACRS) 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. The ACRS made the same recommendation relative to licensing reviews of operating plant digital instrumentation and controls (I&C) upgrades. Such a review would 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. During the review of Chapter 7, Instrumentation and Controls, for the mPower Design-Specific Review Standard, the ACRS raised a similar concern (i.e., control of access) in a letter dated March 19, 2013 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13084A057). In a letter dated August 5, 2014 (ML14196A137), the ACRS made similar recommendations for the proposed 10 CFR 50.55a rulemaking to incorporate by reference IEEE Std. 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear power Generating Stations." In the staff's response letter dated April 3, 2014 (ADAMS Accession No. ML14071A121), NRC staff 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.

Proposed Actions

- Evaluate options for considering cyber security early in the design and development process and for developing a process to allow staff to review cyber security design information as a part of licensing reviews. The purpose of such early review would be to address and/or eliminate cyber vulnerabilities that could be inadvertently introduced at the early stages of development of proposed digital safety systems.

- Work with the NRC Office of General Counsel (OGC) on the legal basis for reviewing voluntary submissions of digital I&C cyber security design-related information.

- Implement the resulting process for addressing cyber security early in the development of DI&C safety related systems.

Desired Outcome

Additional regulatory certainty for licensees and applicants. Greater efficiency and effectiveness by performing evaluations of I&C against cyber security criteria early and in parallel with the I&C systems development and its safety reviews.

10. DI&C Topical Report Evaluation and Update Process (Mid-term)

Challenge:

The expenditure of NRC staff resources for the review of digital I&C platform topical reports has not gained the efficiencies in performing licensing evaluations as was originally envisioned. A means or process to (1) effectively and efficiently address updates to topical reports, and (2) address design changes made to platforms following issuance of the original topical report safety evaluation, has not been established.

Supplemental Information

The NRC staff expends several FTE annually evaluating new DI&C-related safety system topical reports. The variety of proposed new DI&C safety system designs ranges from individual PC boards containing digital components, to complete platforms which may be configured as a RPS or ESFAS system. Yet all of these topical reports yield many areas for which a safety conclusion cannot be made because they are dependent on application-specific implementation issues. Also, there are many topical reports under evaluation for which there has been no interest shown by the US nuclear industry for use in a US nuclear plant. The NRC staff needs to examine whether resources should continue to be expended in evaluating topical reports for which (a) there is no US industry interest; (b) there is minimal benefit from such reviews because either there remains many plant specific application issue to be resolved; (c) the topical report has not been kept current with vendor platform upgrades; or (d) the topical report has not been kept current with NRC regulatory changes. The industry stated it would like to make it easy for vendors to keep topical reports current using a NRC-approved change management process that identifies whether the change impacts any safety conclusions reached by the staff. If it is determined that evaluation of vendor topical reports is to be continued, there is a need to ensure that efficiencies are gained in the processing of future licensing actions that reference the approved topical report.

Proposed Actions

- Engage vendor and licensee stakeholders to outine the challenges in keeping approved vendor I&C platform topical reports current and identify and prioritize the key areas to be addressed.
- Investigate how nuclear regulators in other countries and regulators of other public safety related sectors address this issue.
- Appoint a Working Group to develop a guidance document for nuclear vendors to use for identifying when update to NRC-approved topical reports are needed, and what threshold is to be reached for triggering a required update to be submitted for NRC evaluation.
- Develop the technical basis for the regulatory guidance, and produce a guidance document.

Desired Outcome

As originally envisioned when licensing reviews reference a topical report, a staff evaluation of any digital I&C platform topical report (and its timely updates) should yield a commensurate reduction in staff review time and scope (i.e., a return on the investment). A means or process to effectively and efficiently address updates to previously reviewed and approved digital I&C platform topical reports.