As seen in the June 2021 issue of **Nuclear**News

How the NRC modernized infrastructure and where it

its digital I&C goes from here

By Eric J. Benner and Steven A. Arndt

The Nuclear Regulatory Commission[a] first formally developed infrastructure for the review of digital instrumentation and control (I&C) systems in the 1990s. Although the current fleet of nuclear power plants in the United States was originally designed and constructed with analog systems, the U.S. nuclear industry has for more than 30 years been working to upgrade these older systems with modern digital equipment.

Digital systems have many advantages over analog systems, but they also pose different engineering challenges and need to be reviewed by the NRC in a different way. Because of these differences, the NRC started looking at its regulatory infrastructure to see if changes needed to be made to support the expanded use of digital systems in nuclear power plants. Several efforts in the 1990s included a review by the National Academies' National Research Council, a review by the NRC staff of the impact of potential new digital systems resulting from advanced reactor designs, and the NRC staff's update to the I&C section of the Standard Review Plan (SRP).[1]

In the review of the impact of new digital systems arising from the evaluation of potential issues associated with advanced nuclear power plants—the NRC at the time was reviewing the early "advanced" reactors, such as the AP600—several I&C issues were evaluated, but the key issue that came to the forefront was the potential concern with software common cause (then referred to as common mode) failure. Common cause failures had always been evaluated as environmental or manufacturing issues and had been generally excluded from design reviews. With software not having a material presence, however, the "manufacturing" was really in the coding that would be replicated in all the redundant channels of a software-based safety system. At the time, several software professionals were looking at this challenge and had proposed potential solutions, but these potential solutions were not generally accepted for several reasons, including cost and dependence on the underlining requirements specifications.[2]

[a]Hereinafter referred to as the NRC—not to be confused with the National Research Council, which is not abbreviated.

Continued

Portrait of E. Gail de Planque, NRC commissioner 12/16/91–06/30/95, during which the NRC contracted with the National Research Council to investigate how best to regulate the introduction of digital I&C systems into nuclear power plants.

This review led the NRC staff to recommend to the commission[3] that digital system common cause failure be treated as a possible but unlikely event and that the means to cope with it be required. The commission directed the NRC staff to treat digital system common cause failure as a beyond-design-basis event for the purpose of analyzing the adequacy of coping with proposed failures and provided guidance associated with how to develop acceptance criteria.

In parallel with the above review, in 1994, the NRC, at the urging of the Advisory Committee on Reactor Safeguards (ACRS), contracted with the National Research Council to investigate how best to regulate the introduction of digital I&C systems into nuclear power plants. The National Research Council appointed a committee that was charged to define the important safety and reliability issues that arise from the introduction of digital I&C technology in nuclear power plant operations.

The committee, in its 1997 report,[4] identified eight key issues associated with the use of digital I&C systems in existing and advanced nuclear power plants. The eight issues were:

1. Systems aspects of digital I&C technology.
2. Software quality assurance.
3. Common cause software failure potential.
4. Safety and reliability assessment methods.
5. Human factors and human-machine interfaces.
6. Dedication of commercial off-the-shelf hardware and software.
7. Case-by-case licensing processes.
8. Adequacy of the technical infrastructure.

In the area of systems aspects of digital I&C, the committee recommended that the NRC staff reach out to foreign nuclear power regulators and other industries, such as the chemical processing and aerospace industries, to compare their guidance documents with those being developed by the NRC and to develop staff knowledge and experience in digital I&C. In the area of software quality assurance, the committee recommended that the staff develop nuclear-specific software quality assurance guidance and focus on the early phases of the software development life cycle.

In the area of common cause software failure, the committee concluded that the NRC's position as stated in COM-SECY 93-087 was correct. However, it recommended that the NRC continue to revisit its guidance on how to assess whether adequate diversity exists. The committee also recommended that the NRC retain its position that common cause software failures are credible, and

that its basic position regarding the need for diversity in digital I&C systems is appropriate.

In the area of safety and reliability assessment methods, the committee recommended that the influence of software failure in system reliability be included in probabilistic risk assessments (PRAs) for systems that include digital components. Although the ability to accurately model digital system (particularly software) reliability is still quite challenging, the most recent revision of Chapter 19 of the SRP provides guidance on how best to include digital components into PRA models based on research completed by the NRC[5] and others.

The recommendations in the areas of human factors and human-machine interfaces, dedication of commercial off-the-shelf hardware and software, case-by-case licensing process, and the adequacy of the technical infrastructure would also lead to updates to the SRP associated with human factors reviews, the development of guidance on the use of third-party certification for use in licensing commercial off-the-shelf products, guidance on how to amend a nuclear power plant license when upgrading I&C to digital, and new guidance on the use of 10 CRF 50.59 for digital systems.

Also, in parallel with these efforts, the NRC staff updated the SRP chapter associated with the review of I&C systems for both new licenses and amendments for existing licenses to accommodate the use of digital systems. In 1997, Revision 4 of Chapter 7 of the SRP was published and, for the first time, specifically provided for the challenges associated with the regulatory review of digital systems.

Because analog systems' performance can typically be predicted—using well-known engineering models that accurately predict their continuous performance based on physics principles—the review of analog I&C systems is similar to that for other reactor components. The system designers and the NRC staff could establish a reasonable expectation of continuous performance over substantial ranges of input conditions as part of the qualification of the system's design, which allowed reliance on the testing of a finite sample of input conditions and a review of models of the system to demonstrate acceptable performance with a high level of confidence.

The 1997 revision of the SRP acknowledged that digital I&C systems are fundamentally different from analog I&C systems in that minor errors in design and implementation can cause them to exhibit unexpected behavior. Consequently, the performance of digital systems could not generally be established using traditional design reviews and testing. Design reviews, inspections, type testing, and acceptance testing of digital systems and components do not alone accomplish design qualification to adequate confidence levels.

To address this issue, the NRC staff turned to an approach to the review of design systems that was the state-of-the-practice at the time for both military and civilian applications of digital systems. This approach focused to a greater extent on confirming that the applicant or licensee employed a high-quality development process that incorporated disciplined specification and implementation of design requirements. Inspection and testing are still used to verify correct implementation and to validate the desired functionality of the final product, and confidence that discontinuous failures will not occur comes from the discipline of the development process.

To implement this approach, the staff developed several branch technical positions (BTPs) and regulatory guides (RGs) that explained the requirements and endorsed the state-of-the-practice industry standards. This included BTP 7-14 for the development process; RG 1.152, which endorsed IEEE Std. 7-4.3.2-1993, for the general digital system design; and BTP 7-19 to provide staff with review guidance for the commission's position on common cause failures. These and other similar documents made up the NRC's first digital I&C infrastructure.

For the next 10 years, the NRC used this first digital infrastructure to support the licensing of a number of digital systems in the current nuclear fleet. This basic infrastructure was updated as new industry standards were developed and research supported updates. The NRC's digital research program was also established[6] along the lines of the National Research Council report's recommendations.

In January 2007, in response to a November 8, 2006, commission meeting and a staff requirements memorandum dated December 6, 2006 (available through the NRC's ADAMS document retrieval system with accession number ML063400033), the NRC staff initiated

Continued

a project (the Digital I&C Project) to improve the regulatory efficacy and predictability of the licensing of digital I&C systems in new and existing power reactors. During that November 2006 commission meeting, an industry panel expressed concerns about utilities' ability to license digital I&C safety systems and to implement certain NRC policies regarding digital I&C. The Nuclear Energy Institute (NEI) stated that NRC guidance needed improvements to facilitate the nuclear industry's needed retrofits of aging analog systems in operating reactors and orders for new reactor simulators.

The Digital I&C Project, which ran from 2008 until 2011, was managed by a steering committee and organized around seven task working groups to accomplish specific objectives.[7] The industry established a parallel group of industry executives to coordinate industry efforts and interface with the NRC staff. The Digital I&C Steering Committee and the task working groups prepared interim staff guidance (ISG) documents for each of the key issues identified: cybersecurity, common cause failure, review of new-reactor digital I&C PRA, challenges associated with more highly integrated digital system communications, human factors, the licensing process, and fuel cycle facilities. The ISG on cybersecurity was superseded by updated guidance in support of the new rule on cybersecurity.

The ISG that supported the review of digital I&C PRA for new reactor applications was used in the update of Chapter 19 of the SRP and has been used successfully in several Part 52 reviews. The ISG on highly integrated digital system communications remains in effect as part of the digital I&C infrastructure but will be sunsetted when the NRC endorses the most recent version of IEEE 7-4.3.2 in an updated version of RG 1.152. The ISG on human factors was also integrated into an update to the SRP, as was the ISG on digital systems in fuel cycle facilities. (There is a separate SRP for fuel cycle facilities that contains the updated guidance on digital systems.) The ISG on common cause failures was integrated into an update of BTP 7-19.

At the conclusion of the Digital I&C Project, the NRC staff committed to working with the nuclear power industry and other stakeholders to continue to enhance communications on technical issues in this area through a series of periodic public meetings to address issues of common concern. One of the key issues identified during these meetings, and subsequently through inspection findings, was the need to improve guidance on the use of 10 CFR 50.59 for digital systems upgrades. In November 2013, the NRC sent a letter (ML13298A787) to NEI, summarizing the NRC's concerns about NEI 01-01, Revision 1 to EPRI TR-102348, *Guideline on Licensing Digital Upgrades*, the industry guidance on the use of 10 CFR 50.59, "Changes, Tests, and Experiments," for digital safety systems at the time.

Subsequently, in 2014, the NRC held four public meetings to clarify these concerns, including that the technical guidance in NEI 01-01 had become outdated. In parallel with this work, the NRC staff was developing additional updates to the digital I&C infrastructure, but many in the industry stated to the commission that they were hesitant to pursue the deployment of digital I&C through license amendments, new applications, or changes under the 10 CFR 50.59 process unless regulatory efficiency and predictability could be improved. In response, the commission directed the staff to develop an integrated strategy to further modernize the NRC's digital I&C infrastructure.

In 2016, the NRC staff developed an integrated action plan (IAP) (ML17102B296) and submitted it to the commission for approval in SECY-16-0070. Although significant improvements were made to the digital systems licensing infrastructure associated with the previous project, that project's focus was primarily on resolving specific technical issues that were anticipated to be challenges for the licensing of new reactors rather than improvements to the licensing infrastructure.

The NRC's objective for digital I&C has always been to have a clear regulatory structure with reduced regulatory uncertainty that enables the expanded use of digital I&C in commercial nuclear reactors. When developing and implementing the IAP, the NRC staff aimed to address, more broadly, the regulatory challenges for operating reactors, as well as those for new and advanced reactors. The IAP was based on NRC licensing and inspection experience, as well as extensive stakeholder engagement, to reach a common understanding of the regulatory challenges and priorities associated with digital I&C and potential solutions to address them.

This new infrastructure improvement project focused on four areas:

1. Protection against common cause failure.
2. Digital upgrades using the 10 CFR 50.59 "changes, tests, and experiments" rule.
3. Commercial-grade dedication of digital equipment.
4. Additional perceived impediments of the licensing process.[8]

In again looking at the challenge of protection against common cause failure, this new effort focused on developing technical guidance for low risk-significant safety systems and auxiliary and/or support systems that would typically use the 10 CFR 50.59 process.

The NRC staff was able to improve guidance (using qualitative assessment) for evaluating and documenting the proposed use of design attributes, quality measures, operating history, and appropriate coping and bounding analysis to address common cause failure when replacing or modifying lower risk-significant safety systems and auxiliary and/or support digital I&C systems under 10 CFR 50.59. In May 2018, the NRC staff clarified how licensees could perform digital I&C modifications without NRC approval in Regulatory Information Summary (RIS) 2002-22, Supplement 1, *Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems* (ML181430633).

Industry feedback indicates that this guidance has been vital in supporting licensees in addressing real-time equipment obsolescence challenges and improving system and component performance. In addition to providing this new guidance for low safety-significant systems, the NRC staff has also reevaluated the more general position on common cause failure in digital systems. After reviewing both the original position and key issues raised by industry, the NRC staff proposed a strategy for updating BTP 7-19 that would incorporate the five guiding principles in SECY-18-0090 and introduce an approach to grading the level of review based on safety significance. In this way, the NRC staff was able to modernize the common cause failure implementation, including providing more flexibility in the analysis, while at the same time maintaining the commission's policy on common cause failure that has served the NRC well since the inception of the digital I&C infrastructure. The NRC staff actively engaged industry through public meetings throughout 2019 and published a new revision of BTP 7-19 in 2020.

The second major focus of the new improvement effort was to further clarify the use of 10 CFR 50.59 for digital I&C modifications.

Continued

Portrait of NRC commissioner Christopher T. Hanson, sworn in 6/8/2020, designated chairman effective 1/20/21.

The general guidance in this area is NEI 96-07, which is endorsed by an NRC RG. The industry requested this additional information on how to complete the required screening and evaluation of modifications made under 10 CFR 50.59 because of the concerns that the NRC raised with the guidance that was available at the time (NEI 01-01) and the negative experiences that some plants had with the process.

To resolve these concerns, the industry and the NRC staff agreed that the best path to a long-term solution would be to update NEI 96-07 and the RG endorsing it (RG 1.187) to incorporate everything the NRC had learned and to be more consistent with RIS 2002-22, Supplement 1. NEI submitted NEI 96-07, Appendix D, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications*, in November 2018. This document provides insight on the application of the 10 CFR 50.59 guidance contained in NEI 96-07, Revision 1, to activities involving digital I&C modifications. It also provides screening guidance for digital I&C modifications that is not contained in RIS 2002-22, Supplement 1. The NRC staff endorsed Appendix D through a revision to RG 1.187 in July 2020.

Another area that has been a challenge to the digital I&C infrastructure is the use of the commercial-grade dedication process for qualifying digital equipment. Because of the relatively low demand for nuclear-specific digital equipment, it has always been a challenge to get equipment vendors to go through the extensive process of qualifying their equipment specifically for nuclear applications. One way to address this challenge is to use the commercial-grade dedication process.

Although the process of qualifying commercial products varies from country to country,[9] in most cases, this process provides a means by which commercial-grade equipment can be used in nuclear safety systems. The industry requested that the NRC look at relaxing specific requirements in its approval process for these systems by substituting a third-party certification of a commercial product for certain equivalent steps in the U.S. process. In February 2020, NEI submitted NEI 17-06, *Supplemental Guidance for Acceptance of Digital Equipment using 3rd Party Certification*, for NRC endorsement through the issuance of an RG.

Perhaps the most significant area of work in this new update to the infrastructure is the NRC staff's effort to improve efficiency in conducting licensing reviews. In the first infrastructure improvement program, the NRC staff issued ISG-06, *Licensing Process*. This document provided additional guidance to the NRC staff and licensees on what documentation needed to be provided and how to sequence the submission and review of the needed information most effectively for the NRC staff to reach its safety finding. Although this guidance was successfully piloted as part of the Diablo Canyon nuclear plant's reactor protection system (RPS) review, there was a concern that more needed to be done to increase the predictability and efficiency of the review process for major digital upgrades and shift the regulatory decision to earlier in the design process. Unlike most components used in nuclear power plants, the regulatory review of digital I&C systems is done during the design of the system, not after it is complete. In December 2018, the NRC staff issued a revision to ISG-06 (ML18269A259).

The revised ISG contains an alternate review process that would have the NRC start the review at a more mature point in the licensee's design process, would call for only one submittal rather than two, and would allow for the final licensing decision to be made earlier in the design process. This alternate review process is also more performance-based because it leverages vendor and regional inspections for confirmatory checks during the implementation stages if the NRC approves the amendment request. The staff expects this alternate review process to result in faster NRC decisions than the traditional process, which remains available. Although not expected to be an issue, the alternate review process does present the possibility that if the design changes significantly between the time of licensing and completion of the design, it will need to be rereviewed.

Concurrent with these most recent infrastructure modernization activities, the NRC staff has also completed digital I&C licensing activities in an efficient and effective manner. Recent licensing successes include a license amendment for the Purdue University research reactor for a complete digital replacement of the reactor protection and control system, completion of the staff review of the design certification for the APR1400, a license amendment for Hope Creek Generating Station's power range neutron monitoring system, and approvals

of generic topical reports for digital I&C platforms from Lockheed Martin (nuclear protection and control), Mitsubishi Heavy Industries, and Radiy.

The staff also successfully evaluated the highly integrated I&C systems for the NuScale small modular reactor using the approach of a design-specific review standard (DSRS) for digital I&C that is based on adherence to fundamental safety principles, with a focus on risk importance and safety significance. This was the first time an applicant and the NRC staff used a DSRS approach to prepare and evaluate a highly integrated digital I&C design.

While more improvements can always be made, the NRC modernization efforts and the digital I&C licensing infrastructure have enabled the expanded use of digital I&C in commercial nuclear reactors. This is evidenced by the widespread use of RIS 2002-22, Supplement 1, and by licensees planning for more complex digital I&C projects to be submitted as license amendment requests using the alternate review process contained in ISG-06.

Specifically, Entergy submitted a license amendment request in August 2020 for digital equipment modifications regarding the core protection calculator and control element assembly calculator at the Waterford nuclear plant; NextEra is planning to submit a license amendment request for digital replacement of the RPS and the engineered safety features actuation system (ESFAS) in May 2021; and Exelon plans to submit a license amendment request for digital replacement of the RPS, ESFAS, and other safety systems in the third quarter of 2022. At a workshop held by the NRC in February 2021, Dominion and Southern Nuclear Corporation also indicated plans for future license amendment requests using ISG-06. Because of this interest, the NRC staff is now preparing for this licensing work, including undertaking pre-application activities.

The NRC staff also plans to continue upgrading and modernizing the new infrastructure through efforts to expand the use of risk-informed approaches to the regulatory infrastructure, enhanced evaluation of data provided by stakeholders on the likelihood of digital common cause failures, and assessing the use of emergent digital technologies. Examples of this ongoing effort include continuing research on the expanded use of modern hazard analysis and the impact of embedded digital devices. Through proactive research and continued improvements to the infrastructure, the NRC staff will continue to support the expanded use of digital technology in the nuclear industry.

Eric J. Benner (eric.benner@nrc.gov) is director of the Division of Engineering in the NRC's Office of Nuclear Reactor Regulation. Steven A. Arndt (arndtsa@ornl.gov), formerly a senior technical advisor with the NRC, is currently a distinguished scientist at Oak Ridge National Laboratory.

References

1. U.S. Nuclear Regulatory Commission, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*, NUREG-0800, Washington, D.C., 1997.
2. Knight, John C. and Nancy G. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multi-version Programming," *IEEE Transactions on Software Engineering*, vol. SE-12, no. 1, January 1986.
3. SECY-93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs*, U.S. Nuclear Regulatory Commission, April 2, 1993.
4. National Research Council, *Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues*, Washington, D.C., National Academies Press, 1997.
5. Arndt, S.A. and A. Kuritzky, "Lessons Learned from the U.S. Nuclear Regulatory Commission's Digital System Risk Research," *Nuclear Technology*, vol. 173, no. 1, pp. 2–7, 2010.
6. SECY-01-0155, *NRC Research Plan for Digital Instrumentation and Control*, U.S. Nuclear Regulatory Commission, August 15, 2001.
7. Grobe, J.A. and S.A. Arndt, "Regulatory Oversight of the Use of Digital Technology in Nuclear Power Plants," *Nuclear News*, March 2009.
8. Arndt, S.A. and Sushil Birla, "U.S. Nuclear Regulatory Commission's Plan to Modernize Digital Instrumentation and Control Regulatory Infrastructure," *Nuclear News*, June 2017.
9. Guerra, S., S. Arndt, J. Eiler, R. Jarrett, H. Miedl, A. Nack, and P. Picca, "Justification of Commercial Industrial Instrumentation and Controls Equipment for Nuclear Power Plant Applications," *Proceedings of the 11th ANS International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, February 2019.