Regulatory oversight of nuclear power plant digital technology use

By Steven A. Arndt

The NRC has improved its regulatory guidance by addressing a number of technical issues associated with safety-related applications of digital I&C technology.

Nuclear power plant operators rely on instrumentation and control systems to monitor and control plant equipment and ensure plant and public safety. These systems, in conjunction with the associated human-system interfaces (HSI), are essential for the safe and efficient operation of the current fleet of nuclear power plants in the United States, all of which were designed and built using pre-1980s analog I&C technology, with minimal application of digital technology. Since the last U.S. operating nuclear plant was built, significant advances have been made in computer-based I&C systems and HSI.

U.S. nuclear plant operators have upgraded many non-safety-related analog I&C systems with digital technology. As the maintenance of safety-related analog I&C systems has become more challenging—primarily due to the obsolescence of equipment—and the reliability and efficiency of digital I&C systems have continued to improve, U.S. nuclear plant operators have initiated design changes to replace safety-related analog I&C systems.

The Nuclear Regulatory Commission has received multiple applications for new nuclear power reactors in the United States in the past few years. Designers of new nuclear power plants use digital I&C systems and video display units in highly integrated control rooms to provide modern control systems. Properly implemented, these new systems have the potential to increase the safety and reliability of nuclear power plants. To support these changes, the NRC is continuing to update its regulatory infrastructure and processes and is developing plans for further collaboration with the industry on additional research into digital I&C system performance and characteristics to keep pace with the changes in technology.

Steven A. Arndt (<steven.arndt@nrc.gov>) is the Senior Level Technical Advisor for Digital Instrumentation and Control in the Nuclear Regulatory Commission's Office of Nuclear Reactor Regulation.

Digital I&C project and beyond

In January 2007, in response to an NRC meeting held on November 8, 2006, and the Staff Requirements Memorandum (SRM) dated December 6, 2006 (ADAMS Accession No. ML0634000331), the NRC staff initiated a project to improve the regulatory efficiency and predictability of licensing digital I&C systems in new and existing power reactors. During that November 2006 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 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. In response to the SRM, the staff established the Digital I&C (DI&C) Steering Committee (ML063390606), which is composed of key NRC executives responsible for ensuring the safety and security of operating reactors, new reactors, and fuel cycle facilities and for implementing the NRC's regulatory research program.

The steering committee was created to provide management focus across NRC organizational boundaries to develop a more predictable, consistent, and efficient regulatory process, to interface with the industry, and to facilitate the resolution of strategic and regulatory challenges. The committee directed six task working groups (TWG) to accomplish these objectives. Subsequently, the staff formed a seventh TWG to resolve similar issues for fuel cycle facilities. The industry established a parallel group of executives to coordinate industry efforts and interface with NRC staff.

The steering committee determined that Interim Staff Guidance (ISG) documents would be issued to address the problem statements and meet the need for additional guidance specified in the digital I&C project plan. The ISGs would subsequently be incorporated into the NRC's regulatory infrastructure in the form of regulations, revisions to the Standard Review Plan, Branch Technical Positions (BTP), regulatory guidance, regulatory reports, or industry consensus standards, as appropriate. The NRC staff has used the ISGs for reviews of facility and vendor applications for the use of digital technology. The NRC staff and industry provided generally positive feedback on the use of the ISGs and their effectiveness, including improved predictability and consistency. The NRC staff is continuing to refine the guidance based on experience.

The DI&C Steering Committee and the TWGs prepared ISGs for all of the technical issues identified in the digital I&C project plan. The ISG documents were developed with significant input from external stakeholders through public comments and a series of public meetings. The TWGs addressed the technical issues of cybersecurity (TWG-1); diversity and defense-in-depth (TWG-2); the review of new reactor digital I&C probabilistic risk assessments (PRA) (TWG-3); highly integrated control room communications (TWG-4); highly integrated control room human factors (TWG-

5); the licensing process (TWG-6); and fuel cycle facilities (TWG-7). (TWG-6 provided additional guidance on the scope and conduct of the review of digital retrofits to operating plant safety systems, and TWG-7 addressed many of the same technical and licensing questions as the other TWGs, but with special consideration of the significant differences in licensing requirements for fuel cycle facilities and the consequences of digital system failures.)

TWG-1 provided clarification on acceptable methods to meet NRC requirements for cybersecurity. NRC Regulatory Guide (RG) 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* Revision 2, and draft NEI 04-04, Revision 2 (ML073461212), describe an acceptable cybersecurity program for protecting safety-related digital systems from internal and external cyber attacks. TWG-1 issued DI&C-ISG-01 (ML072980159) in December 2007, clarifying one acceptable method for meeting NRC cybersecurity requirements, including draft NEI 04-04, Revision 2, and a cross-correlation table (ML072980164) between the guidance in RG 1.152, Revision 2, and draft NEI 04-04, Revision 2. Subsequent to the issuance of DI&C-ISG-01, the staff issued 10 CFR 73.54, *Protection of Digital Computer and Communications Systems and Networks,* and RG 5.71, *Cyber Security Programs for Nuclear Facilities.* This guidance, based in part on the work of TWG-1, defined the process for the review of cybersecurity in nuclear facilities. To bring regulatory reviews of digital systems for new reactors or upgrades to existing reactors in line with the 10 CFR 73.54 requirements, RG 1.152, Revision 3, was issued in July 2011 and reflects the updated approach. All short- and long-term actions associated with TWG-1 are complete.

As part of the review of the license amendment request (LAR) for the Oconee nuclear station to perform a digital upgrade of its protection systems, the NRC staff performed not only the safety review, but also a cyber-oriented review, in accordance with Revision 2 of RG 1.152. The LAR was approved in January 2010. Subsequently, the licensee completed the physical modifications, and the new digital systems have been working reliably in all three units. During the period in which the LAR review was conducted, the NRC shifted the responsibility for cyber protection and oversight to the Office of Nuclear Security and Incident Response, which included having licensees develop cybersecurity plans and implementation schedules.

TWG-2 provided clarification of staff guidance in BTP 7-19 regarding diversity and defense-in-depth. In 2007, TWG-2 developed DI&C-ISG-02 (ML072540118), which addressed system characteristics that comprise adequate diversity and sufficient defense-in-depth, criteria for crediting the use of operator manual actions as a defensive measure, system-level or component-level actuation of equipment when manual actuation is used as a defensive measure, the effects and applicability of common-cause failures, echelons of defense, and whether common-cause failures are classified as single failures in design basis evaluations. The ISG provided several alternatives for designers to meet the diversity and defense-in-depth guidance. The NRC staff reviewed domestic and international operating experience to ensure that the guidance would provide an adequate level of safety. DI&C-ISG-02 was updated in 2009 (ML09159 0268). The guidance of ISG-02 was incorporated into the latest version of BTP 7-19, Revision 6, and ISG-02 has been retired.

Pursuant to 10 CFR 52, new nuclear power reactors are required to include a description of the design-specific PRA and its results in the design certification or combined construction and operating license (COL) application. TWG-3 developed an ISG (ML080570048) describing the characteristics of a PRA for safety-related digital I&C systems, which NRC staff will evaluate during the review of the application. The plan is for DI&C-ISG-03 to be integrated into Chapter 19 of the Standard Review Plan during its next revision to support the re-

view of digital systems in required PRAs for new reactors.

TWG-4 identified that NRC guidance for highly integrated digital control rooms needed refinement on adequate communications independence. Specifically, the guidance needed to better address communications independence between individual digital systems, between safety divisions within a digital system, between a digital system and a nonsafety I&C system, and between a safety division within a digital system and a nonsafety I&C system. Additional areas for improving the guidance included command prioritization between safety and nonsafety commands, the design of multidivisional control and display stations, and digital system network configuration to ensure safety. In 2007, TWG-4 developed DI&C-ISG-04 (ML072540138), which provided an acceptable method to address these communication issues. Revision 1 of DI&C-ISG-04 (ML083310185) was issued on March 6, 2009. The criteria of ISG-04 has been incorporated into the latest version of IEEE Std 7-4.3.2, but the NRC has not yet revised RG 1.152 to endorse the new IEEE standard. Therefore, DI&C-ISG-04 remains in effect.

TWG-5 addressed human factors issues within highly integrated digital control rooms. The HSI concerns include the minimum inventory of alarms, controls, and displays needed to implement emergency operating procedures, the use of computerized procedures and soft controls, the implementation of the safety parameter display system pursuant to 10 CFR 50.34(f)(iv), a graded approach to human factors issues, and criteria for evaluating operator manual actions as a defensive measure in lieu of a diverse automatic actuation system. TWG-5 developed an ISG (ML082740440) to provide enhanced guidance on one acceptable method of addressing these HSI issues. The primary impact of this ISG has been on the human factors review guidance for manual actions associated with diversity and defense-in-depth reviews. The criteria of DI&C-ISG-05 have been incorporated into the Standard Review Plan's Chapter 18A, which was issued in April 2014.

For the licensing process, TWG-6 developed DI&C-ISG-06 (ML110140103) to provide the level of detail needed in a licensing application and to describe the process for NRC review of digital modifications to safety systems in operating plants. In developing DI&C-ISG-06, the NRC staff incorporated the lessons learned from the reviews of digital safety system applications for the Oconee and Wolf Creek facilities. Revision 1 of DI&C-ISG-06 was issued on January 19, 2011 (ML110140103). The ISG process is being piloted with the Diablo Canyon digital process protection system license amendment (see article on page 42).

Licensees are now able to use this ISG when planning an LAR. The guidance identifies documentation needs and methods for making documents available to the NRC staff, and also presents a timeline for various phases of an NRC staff review in parallel with system development. This is intended to reduce regulatory uncertainty and improve efficiency in the application preparation and review processes. From the NRC's perspective, the ISG has provided the staff with a useful means of conveying its technical evaluation needs to the licensee. The topical areas covered by ISG-06 provide a framework to facilitate the interactions necessary for the NRC staff to complete its safety evaluation activities.

The NRC has identified some shortcomings with the ISG-06 process, including incorrect assumptions as to how digital systems are developed, the impact of system scope on the safety evaluation schedule, and the impact of simple design or process changes on the overall project schedules. The NRC was to meet with the public in February 2015 to discuss the status of this pilot project, to identify areas for improving the digital I&C licensing process, and to determine where this guidance should be incorporated in a more permanent way.

TWG-7 addressed many of the same technical and licensing questions as the other TWGs, but with special consideration of

the differences in licensing requirements for fuel cycle facilities and the consequences of digital system failures. TWG-7 issued DI&C-ISG-07 in 2009 (ML091550599) and revised it in December 2010 (ML10190 0316). DI&C-ISG-07 will be incorporated into a future revision of NUREG-1520, *Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility.* In addition to the work of the TWGs, the NRC staff has continued to improve regulatory guidance and the NRC staff review process by actively working with international regulatory counterparts and key stakeholders to address high-priority issues in a timely manner.

The DI&C Steering Committee successfully supported the completion of the digital I&C project plan, advised line organizations, ensured the completion of the actions directed in the SRM mentioned earlier, and provided an effective interface with all external stakeholders on these issues. At the final commission briefing on this subject on February 1, 2011, the staff informed the commissioners that all of the tasks associated with the SRM had been or would shortly be completed and that the DI&C Steering Committee would be completing its work and transitioning to a new approach for interfacing with external stakeholders. This approach involves holding public meetings with external stakeholders to address issues of concern, including the need to develop a better process for updating digital system topical reports and the need to update industry and NRC guidance on implementing digital system upgrades using 10 CFR 50.59.

Other improvement efforts

Although the NRC staff has been able to improve regulatory guidance in a number of areas, additional opportunities to improve regulatory guidance and develop new infrastructure are also being addressed through the digital I&C project. The NRC staff has started working on a number of initiatives, including the development of improved guidance on hazard analysis and more effective guidance for the review of small modular reactors (SMR). The NRC staff is also working with industry to improve guidance on the use of 10 CFR 50.59 for digital systems.

In November 2013, the NRC sent a letter (ML13298A787) to NEI summarizing the NRC's concerns with NEI 01-01, *Guidelines on Licensing Digital Upgrades,* the industry guidance on the use of 10 CFR 50.59 for digital safety systems. Subsequently, in 2014, the NRC held four public meetings to clarify these concerns, including the fact that the technical guidance in NEI 01-01 has become outdated. For example, it does not address field programmable gate arrays, and it does not address lessons learned from recent violations issued for inadequate interpretations of NEI 01-01 criteria. Industry representatives expressed concern that it was not clear from the guidance how the installation of a digital modification to a safety system should address the creation of the possibility for a malfunction of a structure, system, or component that is important to safety with a result different from any that has been previously evaluated in the final safety analysis report (as updated), when the malfunction is associated with software common-cause failures. To address industry's concern, the Electric Power Research Institute (EPRI) has committed to drafting a report on how to address this issue, and NEI will subsequently revise the licensing guidance.

In anticipation of SMR applications, the NRC developed a design-specific review standard (DSRS), since the designs could be significantly different from those of large light-water reactors. In developing Chapter 7 of the DSRS for mPower and NuScale SMRs, the NRC staff incorporated lessons-learned from recent new large light-water reactor reviews. For instance, while the current Standard Review Plan serves the NRC staff well in conducting new reactor reviews, it is organized based on individual I&C systems. In new reactor and SMR reviews, I&C designs are heavily integrated. In addition, because of their greater reliance on passive designs, SMR I&C systems may not have the same importance as those in large LWRs. The NRC staff found that it was more efficient to organize the review according to design principles, such as independence, and so the DSRS is design-principle focused versus system focused. The NRC staff also saw an opportunity to better integrate portions of the review with other review areas. For example, I&C quality assurance contains components, such as configuration management and organizational structure, that are part of the greater quality assurance program. For new reactor designs, a key goal is the establishment of an adequate licensing basis (for example, the final safety analysis report). The DSRS provides a sharper distinction between the level of design information that should be included within the licensing basis and the design information that would be addressed under the inspections, tests, analyses and acceptance criteria (ITAAC) inspections.

Trends in digital I&C systems are driving a need to evaluate emerging analysis methods, techniques, and tools. The NRC's Office of Nuclear Regulatory Research (RES), under a memorandum of understanding with EPRI, is addressing this need through its study of the state-of-the-art in hazard analysis. RES prepared Research Information Letter (RIL) 1101 (ML14237A359) in response to a request to develop the technical basis for the regulatory review of an applicant's hazard analysis of digital I&C safety systems. The technical basis provided in RIL-1101 focuses on challenges that the NRC staff has encountered during its licensing reviews. Most of these challenges stem from hazards that are rooted in systemic causes, such as inadequacies in engineering. Based on RIL-1101, the NRC derived its regulatory review guidance for hazard analysis in the DSRS. The NRC requested reviews of evolving drafts of RIL-1101 by EPRI researchers and other external stakeholders. This approach can apply to an early-stage functional concept, with iterations of it applied to successive work products as development progresses. Early identification of avoidable contributory hazards and constraints, and the development of ways to eliminate them, drives downstream engineering to prevent later problems. Plans are under way to evolve the technical basis established in RIL-1101, including intermediate illustrative example applications and learning cycles.

Going forward

Throughout these efforts, the NRC staff has worked closely with the industry and the public and has refined its regulatory guidance by addressing a number of technical issues associated with safety-related applications of digital I&C technology. This has resulted in a more predictable and efficient regulatory review of applications for digital I&C system modifications at operating reactors and new reactor design certifications and COL applications. The staff will continue to work collaboratively with the industry and the public to resolve digital technology–related issues at operating and new nuclear power plants and will meet periodically with industry to ensure effective communications.

As part of its efforts to continue to improve NRC regulatory guidance and the staff review process, the NRC staff is also actively working with international regulatory counterparts and key stakeholders to address high-priority issues. The NRC staff has been participating in the Multinational Design Evaluation Program (MDEP) new reactor design-specific working groups and chairs the MDEP's digital I&C working group. One issue involves the MDEP's digital I&C initiative to develop innovative approaches and to leverage the resources, experience, and knowledge of other regulatory authorities. The NRC staff is also active with other international organizations, including the International Atomic Energy Agency and the International Electrotechnical Commission, in supporting the development of international I&C standards, which are used by vendors of nuclear safety I&C systems in the development of digital systems. The NRC staff also coordinates with its international regulatory colleagues, as well as these standards bodies, to ensure that NRC regulations and standards are informed by the most up-to-date information and methods. NN