Regulatory oversight of the use of digital technology in nuclear power plant safety

BY JOHN A. GROBE AND STEVEN A. ARNDT

To support the changes to digital I&C that are occurring at operating plants and in new plant designs, the NRC is updating its regulatory infrastructure and processes and is working with the industry to effect a smooth transition.

NUCLEAR POWER PLANT operators rely on instrumentation and control (I&C) systems to monitor and control plant equipment. These systems, in conjunction with the associated human-system interfaces (HSI), are essential to ensuring the safe and efficient operation of the plant. All of the 104 operating nuclear power plants in the United States were designed and built using pre-1980s analog I&C technology, with minimal application of digital technology. Since the last of these plants were built, significant advances have been made in computer-based I&C systems and HSIs.

In recent years, U.S. nuclear plant operators have upgraded many nonsafety 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 with digital technology, and they are currently in the process of seeking approval from the Nuclear Regulatory Commission to upgrade these systems. In addition, the NRC has received 17 applications for combined construction and operating licenses (COL) for 26 new nuclear power reactors in the past couple of years. Designers of new plants are using 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 updating 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 advances in the technology.

Continued

John A. Grobe (jack.grobe@nrc.gov) is Associate Director for Engineering and Safety Systems in the NRC's Office of Nuclear Reactor Regulation and Chairman of the NRC's Digital Instrumentation and Controls Steering Committee. Steven A. Arndt (steven.arndt@nrc.gov) is the Senior Level Technical Advisor for Digital Instrumentation and Control in the NRC's Office of Nuclear Reactor Regulation.

The regulatory perspective on digital systems

BY PETER B. LYONS

As digital systems become more and more ubiquitous, replacing aging analog systems, they will play an ever-increasing role in the protection and control systems of both existing and future nuclear power plant designs. I have no doubt that current and future digital technology will have multiple applications—improving, for example, the effectiveness of human-machine interfaces, the precision by which plants can monitor and control reactor parameters to maintain safety, and the ability to diagnose and predict plant equipment failures. As a nuclear regulator, the Nuclear Regulatory Commission must make judgments on the suitability of individual applications of this technology. We must also strive to promulgate the basis for our judgments, as well as provide information addressing the challenges that have been encountered by the NRC and others, so that lessons learned the hard way need not be repeated, especially at the cost of safety.

As demonstrated in the consumer electronics arena, advancements in digital technology are happening almost continuously. The protection and control systems in nuclear power plants, however, cannot tolerate the uncertainties caused by these rapid advances. Reactor designers in general, and digital safety and I&C system designers in particular, must begin with the end goal of safety, which recognizes that fundamental regulatory principles must be satisfied. These include adequate defense-in-depth based, in part, on independent means to satisfy each safety function. The goal to keep the "safe" in digital safety system design is absolute and must be met. To achieve this, we must find appropriate ways to apply the concepts of redundancy, diversity, and independence with digital system designs.

In order for any advancement in digital technology to be a success, designers, researchers, and regulators need to be systematic, methodical, and thorough in identifying and cataloging all of the ways that digital systems can fail. Security must also be considered, so that systems cannot be inappropriately accessed or modified. To be able to fully realize the potential benefits of this technology while maintaining safety, protection, and control, systems must be designed as an integral part of the overall plant design.

The nuclear community needs to share these insights broadly, deriving them from design work as well as from our collective operating experience. As a regulator, the NRC will continue to improve the clarity and usefulness of regulatory requirements and standards for digital technology and will find better ways to evaluate these new designs, which will surely continue to evolve.

Peter B. Lyons is a Commissioner on the U.S. Nuclear Regulatory Commission.

Early actions

In November 2006, the NRC staff, along with representatives from the nuclear industry, briefed the NRC commissioners on the status of efforts to incorporate digital I&C technology and modern HSI into operating and future nuclear power plants. Following this briefing, the commissioners concluded that there was a need to improve the NRC's regulatory guidance and procedures to facilitate a more predictable and efficient design and licensing process. This would meet the nuclear industry's need to retrofit aging analog systems at operating nuclear power facilities as well as design new nuclear power plants and fuel cycle facilities using safety-related digital I&C systems.

In January 2007, the NRC established the Digital Instrumentation and Controls Steering Committee, made up 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 committee was created to provide management focus across NRC organizational boundaries, develop a more predictable and efficient regulatory process, interface with the industry, and facilitate the resolution of strategic, regulatory, and technical challenges. The industry established a parallel group of executives to coordinate its efforts and to interface with NRC staff.

Challenges and the path forward

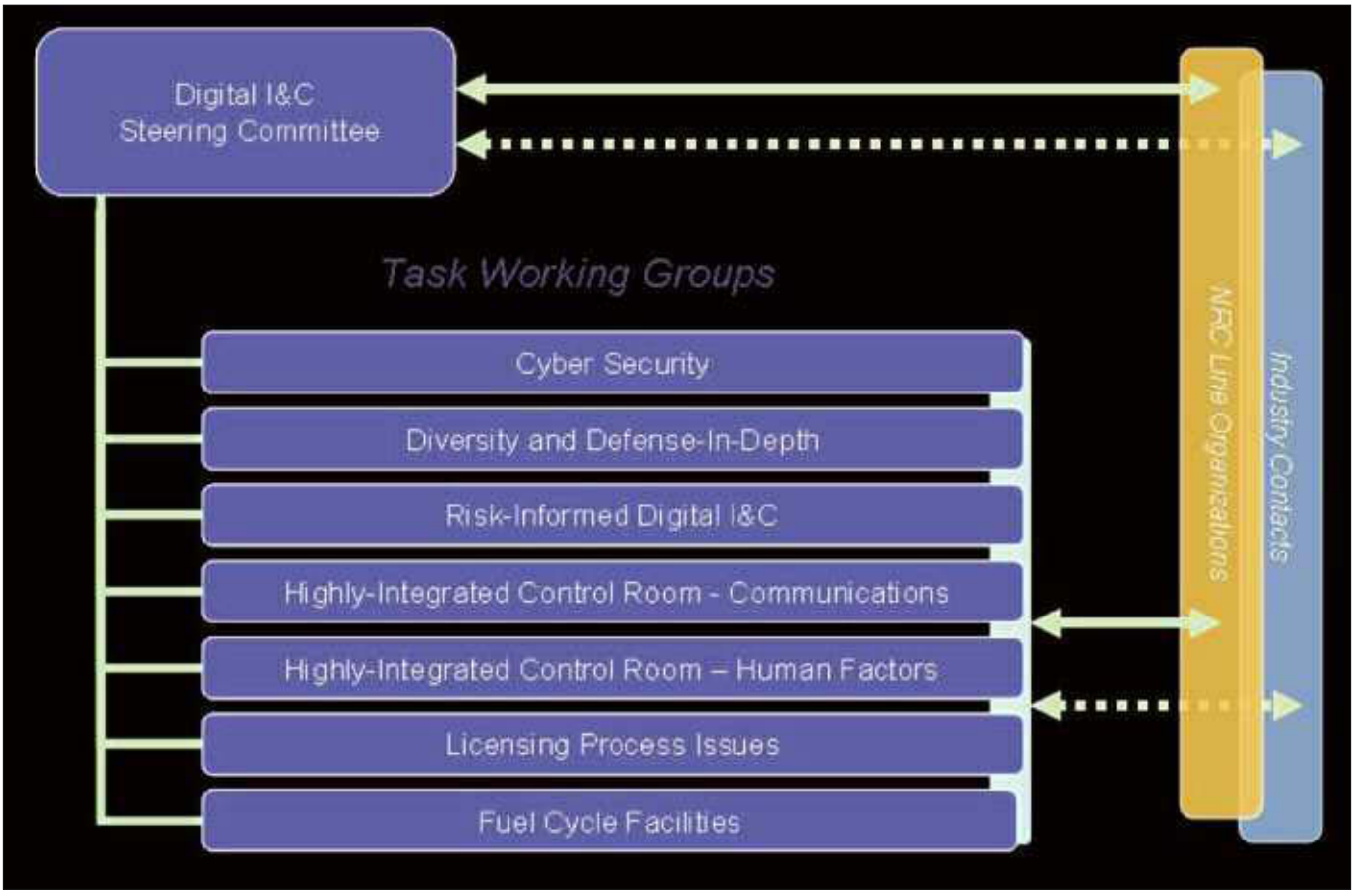
While the NRC's current regulatory infrastructure, including regulations, regulatory guidance, and licensing procedures, has been successfully used for the review and approval of digital I&C systems, the NRC staff, with input from the industry, identified seven key areas where improvement in regulatory guidance and processes could result in improved clarity and predictability. To address these areas, the steering committee formed the following Task Working Groups (TWG):

- TWG 1–Cyber Security.
- TWG 2–Diversity and Defense-in-Depth.
- TWG 3–Risk-Informed Digital I&C.
- TWG 4–Highly Integrated Control Room–Communications.
- TWG 5–Highly Integrated Control Room–Human Factors.
- TWG 6–Licensing Process.
- TWG 7–Fuel Cycle Facilities.

The TWGs are composed of NRC staff members from the relevant NRC offices to address issues in each area. Each TWG was responsible for defining areas needing improvement and developing solutions to address them. The TWGs interacted with the public and the industry to identify specific problem statements in each key area. In total, 25 problem statements were incorporated into an integrated NRC Digital Instrumentation and Control Project Plan, Revision 2 of which was issued on December 9, 2008 (available through the NRC's ADAMS database using accession number ML083440345). In each area, the plan contains background information, detailed problem statements, near-term and long-term milestones, and assignments to address the problem statements in each key area.

The steering committee developed a process to provide timely guidance to address each problem statement. Each step in the process includes substantial interaction with industry and the public through public meetings to discuss technical issues and proposed resolutions to the problem statements. More than 100 public meetings have been conducted by the steering committee and the TWGs over the past two years.

The steering committee determined that Interim Staff Guidance (ISG) documents would be issued to address the problem statements, and would subsequently be incorporated into the NRC's regulatory infrastructure, which includes regulations, the Standard Review Plan, Branch Technical Positions, Regulatory Guides, reports, and industry consensus standards. Each ISG describes one acceptable approach for each specific problem area and represents the "fast lane" for NRC review. Acceptable alternatives may also exist, and the NRC would consider proposed alternative approaches that are adequately supported by a complete technical basis.



Digital I&C Project/Steering Committee structure

A conventional analog control room in a nuclear power plant (Photo: NRC)

The ISGs are being provided in draft form for industry and public comment and are then being issued as final following appropriate TWG consideration of the comments. The development and issuance of the formal regulatory infrastructure documents will follow well-defined and -understood formal public processes. Although TWG 7 was to address technical and process issues for using digital technology at fuel cycle facilities, the remainder of this article will focus on the work of TWGs 1 through 6 in addressing those same issues at operating and new nuclear power reactor facilities.

Technical issues

Following significant NRC staff and industry effort over the past two years, TWGs 1 through 5 have developed and issued ISGs addressing all of the technical problem statements associated with power reactors. These ISGs are being used in ongoing NRC staff reviews of facility and vendor applications for the use of digital technology and have improved the predictability and consistency of the reviews.

TWG 1 provided clarification on acceptable methods for meeting NRC cyber security requirements. An acceptable cyber security program to protect safety-related digital systems from internal and external cyber attack is described in NRC Regulatory Guide 1.152, Revision 2, and in draft Revision 2 of NEI 04-04. TWG 1 issued an ISG (ADAMS ML072980159) that clarifies one acceptable method for meeting NRC cyber security requirements, including draft NEI 04-04, Revision 2 (ADAMS ML073461212), and a cross-correlation table between the guidance in Regulatory Guide 1.152, Revision 2, and draft NEI 04-04, Revision 2 (ADAMS ML072980164).

TWG 2 provided clarification of staff guidance in NRC Branch Technical Position 7-19 regarding diversity and defense-in-depth. TWG 2 developed an ISG (ADAMS ML072540118) that addresses 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- 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 provides several alternatives for designers to use to meet the diversity and defense-in-depth guidance. Various domestic and international operating experiences were reviewed to ensure that the guidance would provide an adequate level of safety.

Pursuant to 10CFR52, new nuclear power reactors are required to include a description of the design-specific probabilistic risk assessment (PRA) and its results in the design certification or COL application. TWG 3 developed an ISG (ADAMS 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.

TWG 4 determined that refinements were needed in NRC guidance for highly integrated digital control rooms regarding adequate communications independence between digital systems. Additional guidance was needed on communications between safety divisions, and between safety and nonsafety I&C; command prioritization between safety and nonsafety commands; design of multidivisional control and display stations; and digital system network configuration. TWG 4 developed an ISG (ADAMS ML072540138) that provides one acceptable method for addressing these communication issues.

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; 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 (ADAMS ML082740440) that provides enhanced guidance on one acceptable method to address these HSI issues.

Continued

A control room of the future, with digital I&C (Photo: Westinghouse Electric Company)

The NRC staff is using the ISGs to address the technical issues in ongoing reviews, and the feedback from licensees and staff who have worked with the ISGs has been positive. The NRC staff will continue to refine the guidance based on experience and will incorporate the guidance into formal regulatory documents.

Refining the licensing process

TWG 6 is working to provide a clear description of the NRC licensing review process for digital modifications to safety systems in operating plants and of the level of detail needed in a license application. Licensees will be able to use this ISG when planning a license amendment request. The guidance will identify the documentation needs and methods, as well as the timing of various aspects of the NRC staff's review, thereby reducing regulatory uncertainty and improving efficiency in preparing the application and in the review process. The staff is taking advantage of the lessons being learned from the digital I&C reactor protection system and/or engineered safety features actuation systems retrofit applications currently under review for the Oconee and Wolf Creek facilities. The NRC staff is engaged in frequent public meetings to solicit licensee and public comments in order to complete this guidance. The current goal is to complete the draft licensing process ISG in May.

Moving forward

Although the NRC staff has been able to improve regulatory guidance in a number of areas, additional work is being undertaken in several other areas.

Further progress can be made in defining adequate diversity attributes, such as fault tolerance, to address common-cause failure susceptibilities. Also, further understanding of digital system failure modes and development of PRA methodologies can facilitate risk-informed licensing decisions. The NRC's Office of Nuclear Regulatory Research is developing a memorandum of understanding with the Electric Power Research Institute to collaborate on additional research activities and develop the technical basis for further refinement of regulatory guidance in these areas.

To support continued improvement in the NRC's regulatory guidance and staff review process, the commission is actively working with international regulatory counterparts and key stakeholders to address high-priority issues in a timely manner. One example is digital aspects of the Multi-national Design Evaluation Program (MDEP), an initiative to develop innovative approaches and to leverage the resources and knowledge of other regulatory authorities with experience in specific new reactor designs and technical areas. The NRC staff has been participating in the MDEP new reactor design-specific working groups, and an NRC manager chairs the MDEP digital I&C working group.

In addition, the Office of Nuclear Reactor Regulation has determined that clarifications may be necessary regarding the application of regulations involving control of the licensing basis (10CFR50.59) and implementation of the maintenance rule (10CFR50.65) once digital I&C modifications have been implemented at operating reactors. It may also be necessary to refine the NRC baseline inspection program and the significance determination process to address digital modifications. The Office of New Reactors has also noted that additional guidance is needed on the appropriate level of detail to be provided in design acceptance criteria for digital systems in design certifications for new reactors.

The NRC staff, working closely with the industry and the public, has refined its regulatory guidance to address 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 certification and COL applications. The NRC continues to collaborate with the industry and the public to resolve further issues associated with the application of digital technology at operating and new nuclear power plants. NN