Key Issues

Key issues related to digital instrumentation and controls (I&C) include those discussed below.

On this page:

- Diversity and Defense in Depth
- Highly Integrated Control Rooms—Digital Communication Systems
- Highly Integrated Control Rooms—Human Factors
- Cyber Security
- Risk-Informed Digital I&C

Diversity and Defense in Depth

NRC regulations establish the requirement that each safety system must operate regardless of failures from within or outside the safety system. The regulatory basis for this requirement is found in Title 10, Part 50, "Domestic Licensing of Production and Utilization Facilities," of the *Code of Federal Regulations* (10 CFR Part 50). In particular, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that "…(1) no single failure results in the loss of the protection system…." In addition, GDC 22, "Protection System Independence," requires, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

These GDCs mandate diverse design features to minimize the possibility of a common-cause failure (CCF) that could result in the loss of a protection function. Nuclear power plant safety system designs rely on three design principles to compensate for failures that could degrade safety system reliability, specifically (1) functional defense in depth, (2) functional diversity, and (3) system diversity.

Industry experience with digital I&C systems has shown that reliance upon quality assurance processes alone has not been adequately effective at preventing CCFs even in high-integrity digital systems. The possibility of unanticipated CCFs in digital systems is higher than that in analog systems, so the importance of functional defense-in-depth, functional diversity, and system diversity features is correspondingly enhanced by the application of digital technology. Additionally, it is necessary to confirm that CCF vulnerabilities are not introduced when a system is modified.

TOP

Highly Integrated Control Rooms—Digital Communication Systems

With digital I&C technology, judicious communication between redundant safety channels and between safety and nonsafety systems may offer enhancements to reliability and safety that were not attainable when existing operating nuclear power plants were designed with the analog technology of the time. Proposed designs include varying degrees of communication between redundant safety channels and between safety and nonsafety systems to validate signals and ensure high reliability. It should be demonstrated that the provisions for the implementation of such communications and the communication processes and messages themselves do not impair the proper execution of the associated safety functions through

unintended behaviors or inadequately managed failure modes or by any other means or influence. The NRC is developing a set of consolidated guidelines to support staff reviews of proposed communication protocols and systems. Issues such as two-way communication, data density, and communication traffic levels appropriate for safety-related applications need to be addressed in the documentation of the proposed designs.

In Appendix A to 10 CFR Part 50, General Design Criterion (GDC 24), "Separation of Protection and Control Systems," states the following requirement:

> The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

GDC 24 provisions regarding interconnection of the protection and control systems limit two-way communication between safety and nonsafety systems. Consensus standards indicate that such communication pathways are acceptable as long as failure of the communication system does not impair the safety function, and the safety function does not rely on nonsafety system inputs to operate. The NRC has approved digital safety systems that use limited two-way communications between safety and nonsafety components to allow safety system reconfigurations while in operating modes specifically designed to accept changes (e.g., Test mode for testing a channel and Inop mode for changing setpoints and performing channel maintenance).

Some of the new control room designs may apply strategies for integrating safety- and nonsafety-related controls within the same controller or display device. The proposed controls and displays could include extensive two-way communications among safety channels and between safety and nonsafety channels. Applicants should demonstrate that proposed mixed-channel displays and controls and operation of safety devices by means of nonsafety controls or of controls in other channels maintain the required independence and isolation of redundant safety systems.

The NRC is developing failure analysis techniques for use in the evaluation of complex digital communication systems proposed for use within and among redundant safety channels and between safety and nonsafety channels. As part of this development, the NRC will use case studies of current technologies to identify scenarios that could challenge a safety system and to identify mitigation measures to address those challenges. The primary objective of this effort is to develop a comprehensive process for confirming that an integrated control room design is in conformance with 10 CFR Part 50.55a(h), "Protection and Safety Systems" requirements and the requirements in associated standards and regulatory criteria for areas such as electrical separation and independence between safety- and nonsafety-related displays and controls; single failure criteria; equipment qualification of Class 1E safety-related displays and controls; and data communication isolation pursuant to Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses with exceptions IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

TOP

Highly Integrated Control Rooms—Human Factors

Proposed new nuclear power plant designs are taking advantage of advances in digital technology to change the control room from a collection of discrete controls and analog displays to a highly integrated glass cockpit-style control room design which may include

touch screen video display devices, semi-autonomous controls, and other advanced operator interfaces and technologies.

Applicants should be able to show that the physical and virtual locations of displays and controls, the distribution of functions among display panels and backup devices, the use of color and other graphical display attributes, provisions for navigation among display screens, provision of backup devices and the conditions and procedures under which they are used, and other factors relating to the use of the control and protection systems by plant operators have been suitably addressed, support understanding of current plant conditions and unexpected events by the operator, and provide for prompt and effective operator responses.

The NRC will supplement review guidelines and acceptance criteria to support reviews of proposed designs and also to benefit applicants preparing those designs. One important source of acceptance criteria is the experience that regulatory agencies in other countries and the United States have gained in their reviews of highly integrated control rooms. Another source is lessons learned from operating experience. The Highly Integrated Control Rooms research project is surveying the approaches used by other countries (e.g., France, Finland, Japan, and Korea) and other U.S. agencies (e.g., the National Aeronautics and Space Administration, the Federal Aviation Administration, and the Department of Defense) for licensing or certifying highly integrated glass cockpit-style control rooms and is comparing the results of the survey with the regulatory criteria now used by the NRC. The research will use the information gained from the survey to supplement guidance and associated acceptance criteria for use by the staff in confirming that integrated control room designs are in conformance with NRC requirements.

TOP

Cyber Security

The purpose of cyber security assessments is to detect and then eliminate or mitigate vulnerabilities in the digital system that could be exploited either from outside or inside of the digital system protected area. The process of defending against this class of failures is made more challenging by the rapidly evolving "industry" that continues developing new attack methods. In addition to developers of viruses, worms, and associated computer programs, there are individuals and undocumented organizations that concentrate on developing methods for gaining access to protected data and systems with the intent to disrupt system operations or illegally obtain information from the systems.

Two security-related NRC orders issued in the wake of the terrorist attacks on September 11, 2001, mandated in part that nuclear power plant licensees take certain actions to enhance the cyber security of their digital systems. In response, through a contract with the Pacific Northwest National Laboratory and in cooperation with the Nuclear Energy Institute (NEI) Cyber Security Task Force, the NRC developed and issued a NUREG on method for performing a cyber security self-assessment at U.S. nuclear power plants. That report provides guidance that licensees can use to systematically identify cyber vulnerabilities at their facilities, assess their relative (security) risk-significance, and institute cost-effective mitigating measures. Using this NUREG as a foundation, the NEI task force developed comprehensive guidance that nuclear power plant licensees can use to develop and manage an effective cyber security program. In December 2005, the NRC staff endorsed this NEI guidance as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants.

In parallel with the development of the NUREG and NEI guidance, staff revised existing regulatory guidance on use of computers in nuclear digital safety systems. Regulatory Guide 1.152, Rev. 2 "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," in parts, states that digital safety system development processes should address potential security vulnerabilities in each phase of digital safety system development lifecycle. Use of

the deterministic guidance contained in Regulatory Guide 1.152, in conjunction with NEI guidance, for digital safety system designs would assure security against cyber vulnerabilities.

As part of the agency's ongoing effort to respond to the two security-related NRC orders issued, the Commission will codify the mandated cyber security enhancement requirements in new regulations in 10 CFR Part 73, "Physical Protection of Plants and Materials." Additionally, the staff will develop regulatory guidance that relies heavily on the NUREG, which the industry used in its NEI program management guideline. In doing so, the staff anticipates that research will likely be required to establish inspection review procedures, criteria, and assistance needed to prepare regulatory guidance documents associated with the implementation of NUREG and NEI guidance.

The NRC is engaging other Federal agencies, most notably the U.S. Department of Homeland Security and the Federal Energy Regulatory Commission, as well as the North American Electric Reliability Corporation in an effort to leverage related cyber security work that these agencies have completed or are conducting. The NRC also is participating in a project sponsored by the intergovernmental Technical Support Working Group to develop a software-based tool that will facilitate the implementation of NUREG and NEI guidance and to develop a device that will provide secure communications for digital safety systems. The tool is expected to use a question-and-answer format to guide security audits of installed networks and digital systems through the NUREG and NEI guidance topic areas. The product of this research may be integrated into the NRC's cyber security review processes.

TOP

Risk-Informed Digital I&C

As discussed in the NRC's policy statement on probabilistic risk assessment (PRA), the agency supports the use of PRA in regulatory matters to the extent supported by state-of-the-art PRA methods and data. Since digital systems will play an increasingly important role in nuclear power plant control and safety systems, the need for risk assessment methods for digital systems is evident. An accident sequence precursor (ASP) events database study has demonstrated the prevalence of embedded (digital) I&C components and their impact on plant safety. This study identified several ASP events that involved failure of digital controls that were embedded in larger plant systems (e.g., circuit breakers, transformers, and diesel generators). Because of the prevalence of digital I&C systems and their potential impact on plant safety, future risk-informed regulatory decisions are likely to require risk assessment of both freestanding and embedded digital systems.

The NRC is actively working to develop tools and methods to perform quantitative risk assessments of nuclear power plant digital systems. This information will assist the staff in evaluating proposed digital system applications to ensure that they do not result in an unacceptable increase in the frequency of occurrence of an accident or in the likelihood of occurrence of a malfunction of a structure, system, or component important to safety.

The objectives of risk assessment are to (1) identify failures that can occur, (2) determine the impact of those failures, and (3) quantify their frequency. The NRC is investigating the use of methods, tools, and criteria to meet these three digital risk assessment objectives. This entails assessing the types and causes of failures that can occur in digital systems, characterizing the risk-importance of I&C systems (impact of digital failures on safety), developing digital reliability assessment methods (frequency of failures), and collecting and analyzing the data needed to support this work. The staff recognizes the potential difficulty in integrating digital systems into PRAs and in the practicality of using a PRA to assess digital systems.

TOP