Frequently Asked Questions about Digital I&C

On this page:

What changes to existing guidance and what new guidance might be expected as a result of ongoing NRC research efforts?

The NRC Office of Nuclear Regulatory Research (RES) is engaged in research that will both augment and enhance the current staff review guidance and will develop information needed to assist in the review of new technologies. RES is not engaged in rulemaking efforts, nor are the results of the research designed to provide new policy. The research is designed to enhance staff acceptance criteria for licensing activities where new technology may render earlier guidance less effective.

TOP

How does the schedule for the preparation of licensing guidance for digital I&C compare with the anticipated need date for that guidance?

DG-1145, "Combined License Applications for Nuclear Power Plants (LWR Edition)," was issued for comment and use in October 2006, and final issuance is anticipated in March 2007. Chapter 7 of the revised Standard Review Plan is expected to be available to the public in April 2007. The first set of combined license applications are expected in September of 2007.

TOP

How are licensees to know what needs to be submitted for NRC consideration in the licensing of digital I&C for nuclear safety applications?

DG-1145, "Combined License Applications for Nuclear Power Plants (LWR Edition)," includes a discussion of what must be submitted by a licensee not referencing an accepted design. This same material would be needed for digital installations in safety service in existing nuclear power plants.

TOP

What is the timeframe for operator actions used to satisfy a diversity requirement?

There is no regulation concerning acceptable timeframes. It is commonly believed that 30 minutes is a reasonable lower limit for operator action, but requirements are assessed on a case-by-case basis. International regulators and a study by the National Research Council generally accept the 30-minute lower limit.

TOP

What are the various research programs within the Research Plan?

The **System Aspects of Digital Technology** program involves research pertaining to internal and external factors that affect the performance of a digital system as a whole.

The **Software Quality Assurance** program involves research pertaining to establishing a quantitative means of assessing the quality of safety system software.

The **Digital System Risk Assessment** research program will establish a program and process to facilitate risk-informing digital system reviews.

The **Emerging Digital Technology** assessment program involves research into new innovations in digital I&C technology that have the potential for deployment in existing, new, or advanced nuclear facility I&C system designs.

The **Digital System Security** program involves research that will address potential security vulnerabilities as part of the system development process and will maintain security of the system after it is installed from threats such as external cyber attacks as well as electromagnetic interference or electromagnetic pulse attacks.

The **Advanced and Future Plant Digital System** program involves research to develop needed regulatory guidance to support the review of future reactor I&C systems and highly integrated digital control rooms.

For more details on these research programs, please refer to the NRC Digital System Research Plan for FY 2005–FY 2009 (ML061150050).

TOP

What has been the operating experience with digital I&C safety systems installed in nuclear power plants?

During the past 20 years, there have been a significant number of safety-related and important-to-safety digital systems or components installed in operating nuclear power plants. The safety-related digital systems were developed in accordance with the requirements in Appendix B to 10 CFR Part 50 and generally have operated safely. However, 38 out of approximately 100 operating plants have reported potential and actual common-mode failures in many of these systems. Some common-mode failures affected a single plant, while others affected several plants using the same digital system.

TOP

What is meant by six diversity attributes?

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," describes a method for analyzing digital safety systems to determine points of design for which credible common-mode failures are compensated for by diversity or defense in depth.

Diversity is complementary to defense in depth and increases the likelihood that defenses at a particular level or depth will be actuated when needed. The types of digital system diversity may be classified into the following six categories:

(1) **Design diversity**—for example, different technologies (analog versus digital), different approaches within a technology, different architectures (arrangement and connection of components)

(2) **Equipment diversity**—for example, different manufacturers of fundamentally different designs, same manufacturer of fundamentally different designs, different manufacturers making the same design, different versions of the same design, different CPU architectures (Intel versus Motorola), different CPU versions (Pentium versus 486), different printed circuit board designs, different bus structures (VME versus Multibus II)

(3) **Functional diversity**—different underlying mechanisms (rod insertion versus boron injection), different purpose or function (normal rod control versus reactor trip rod insertion), different response time scale (secondary system responses late in accident sequence)

(4) **Human diversity**—different design organizations; different engineering management teams within the same company; different designers, engineers, or programmers; different testers, installers, or certification personnel

(5) **Signal diversity**—different reactor or process parameters sensed by different physical effects (high temperature versus high neutron power), different reactor or process parameter sensed by the same physical effect (pressure used for low pressure and low flow), same reactor or process parameter sensed by redundant set of similar sensors (four channels of pressure sensors backed up by four more sensors driving a different design of protective equipment)

(6) **Software diversity**—different algorithms, logic, and program architecture; different timing, order of execution; different operating systems; different computer languages

TOP

What different acceptable strategies may address common-mode failure vulnerabilities in digital safety system designs?

The staff guidance in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," provides a set of recommended criteria for each diversity attribute, ranked in order of relative importance within each attribute. The Diversity and Defense-in-Depth (D3) research project will explore combinations of equipment diversity in microprocessor hardware and software and will assess the strengths and weaknesses of the resulting system D3. This research will provide recommendations for staff guidance in terms of best practices for digital system D3 design strategies.

TOP

What will be the final product in terms of integrating these improved methods for diversity and defense-in-depth analysis into regulatory guidance and acceptance criteria for licensing activities?

The Diversity and Defense-in-Depth (D3) research project will develop combinations of diversity attributes and associated criteria that provide acceptable D3 strategies for addressing common-mode failure vulnerabilities in digital safety system designs. The information obtained from this research project will be used to develop a revision to NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," or a new NUREG that will provide enhanced technical guidance to the staff on appropriate common-mode failure mitigation measures using diversity attributes and criteria. It will also be used to develop regulatory acceptance criteria that will complement existing NRC regulatory processes (i.e., BTP-19, "Guidance on Evaluation of Defense-in-Depth and Diversity (D3) of Digital I&C") for confirming appropriate implementation of common-mode failure mitigation strategies. A regulatory guide could ultimately result from this project.

TOP

How will the new diversity and defense-in-depth review guidance fit into the review schedule for new reactors?

The staff guidance in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," provides a set of recommended criteria for each diversity attribute, ranked in order of relative importance within each attribute. The Diversity and Defense-in-Depth (D3) research project will explore combinations of equipment diversity in microprocessor hardware and software and will assess the strengths and weaknesses of the resulting system D3. This research will provide recommendations for staff guidance in terms of best practices for digital system D3 design strategies. However, licensees can and have used the existing guidance to design digital safety systems that satisfy agency requirements.

TOP

How does the staff envision that the reliability and risk methods developed in its research will be used to supplement the deterministic licensing process?

The staff intends to provide one acceptable method that can be applied to current NRC guidance for using probabilistic risk assessment in risk-informing licensing decisions (Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis").

TOP

What are the digital system modeling methods used in other industries—such as aerospace, defense, and telecommunications—and why does the staff think they may be adapted for use in nuclear power plants?

Other industries have developed methods to model digital systems by using a number of methods, including fault trees, dynamic fault trees (used by the National Aeronautics and Space Administration (NASA)), Markov methods (used by NASA, the transportation industry, and others), dynamic flow graph methodology (used by NASA), and Petri nets. In the case of the space station, for example, the digital system model used is a Markov model that was then partially integrated into the larger station event tree/fault tree model. Although these methods have some limitations (e.g., the space station model does not dynamically link the digital system model to the rest of the probabilistic risk assessment), the staff believes that these modeling methods can be adapted and improved to provide an acceptable method for modeling digital systems in nuclear power plants.

TOP

What is the staff's plan to get information from the vendors on their control room designs that can be used to develop staff guidance in this area?

The NRC Office of Nuclear Regulatory Research will be collaborating with other industries, foreign regulators, other government agencies, and reactor vendors to incorporate lessons learned from the controls industry into agency regulatory programs. Examples of these collaborations include interactions with the following:

- France, Finland, and Areva on EPR I&C
- Germany (TUV and GRS) on generic qualifications of digital platforms
- U.S. Department of Defense to acquire lessons learned associated with the deployment of digital I&C in naval reactors
- Organization for Economic Cooperation and Development (e.g., Halden Reactor Program) and International Atomic Energy Agency in the area of guidance on licensing digital systems
- other reactor vendors to develop appropriate guidance for new designs

TOP

What will be the final product of the NRC research regarding digital system cyber vulnerabilities?

The research end products will augment and supplement the staff's review process described in relevant sections of the updated Standard Review Plan. The results are expected to be in the following form:

- system-specific reports describing any potential cyber vulnerabilities discovered
- review guidance and acceptance criteria
- implementation guidance for the sites with the operational systems

TOP

How is the NRC staff interfacing with the U.S. Department of Homeland Security on cyber security?

The NRC staff has been engaged with the U.S. Department of Homeland Security (DHS) on the National Infrastructure Protection Plan, which allowed the staff to identify areas for potential collaboration on cyber security and on the application of the DHS cyber assessment process, which may be applicable to nuclear power plants.

TOP

What is meant by FPGA? Why is FPGA considered an alternative to a traditional software-driven microprocessor?

Microprocessors are general-purpose state machines that perform operations on programs stored in memory locations. Microprocessors fetch instructions and data from memory locations, decode the instructions, execute the application software instructions using the data, and then write the results to a memory location for subsequent use in the next program step.

A field programmable gate array (FPGA) is a semiconductor device containing programmable logic components and programmable interconnects. The programmable logic components can be programmed to duplicate the functionality of basic logic gates (such as AND, OR, XOR, NOR) or more complex combinational functions (such as decoders or simple mathematical functions). In most FPGAs, these programmable logic components (or logic blocks, in FPGA parlance) also include memory elements, which may be simple flip-flops or more complete blocks of memories.

A hierarchy of programmable interconnects allows the logic blocks of an FPGA to be interconnected as needed by the system designer, somewhat like a one-chip programmable breadboard. These logic blocks and interconnects can be programmed after the manufacturing process by the customer/designer (hence the term "field programmable") so that the FPGA can perform whatever logical function is needed. Once programmed, an FPGA executes only that program repetitively.

TOP

Why may FPGAs be less susceptible than microprocessors to software common-cause failures?

Because field programmable gate arrays (FPGAs) are significantly simpler than microprocessors and link only the functions needed for a given application, the complexity of the resulting application system can be significantly less than that of a microprocessor-based system. Also, FPGAs have burned-in programmed logic that reacts to incoming information and do not rely on application software continuously running to process incoming information.

TOP

How will the new guidance on analytical methods and uncertainty analysis for online monitoring systems be used by the staff?

The safety evaluation report (SER) that approved the generic concept of online monitoring (OLM) also mandated 14 requirements that an OLM system would have to meet if the calibration frequency were to be extended (including the need to conduct a detailed uncertainty analysis). Additionally, the SER did not provide any guidance on the acceptability of any particular analytical method for implementing OLM for calibration frequency extension. The new guidance will provide the staff with detailed technical information that it can use to evaluate licensee responses to the 14 requirements in the SER and with methods for identifying and evaluating the assumptions and limitations associated with the analytical methods that are being applied in OLM systems.

TOP

How has the Federal Aviation Administration contributed to the research associated with licensing digital I&C safety systems at new reactors and as retrofits in current nuclear power plants?

The Federal Aviation Administration (FAA) has developed guidelines (DO-248B and DO-178B) for all software to be installed on aircraft. The FAA has extensive experience with the licensing of flat panels as well as the use of emerging technologies. The NRC has initiated research (e.g., highly integrated control room research and field programmable gate array (FPGA) research) with a number of external agencies and organizations, including FAA, to develop licensing guidance on the basis of experience gained from other types of mission-critical and safety-significant applications.

TOP

Is there a compilation of the full spectrum of possible digital system (hardware and software) failure modes? Isn't this the necessary starting point to determine if each known failure mode has been adequately addressed in the plant design?

To the NRC's knowledge, all possible digital system failure modes have not been compiled. This is one focus area of ongoing NRC research into digital system risk.

Ideally, a list of all digital system failures would be highly desirable; however, in practicality, a well designed, redundant, and diverse digital system should address all system failure modes.

TOP