Research Activities

The NRC Office of Nuclear Regulatory Research (RES) is performing research to update the tools, review procedures, and acceptance criteria that the NRC staff uses to assess the safety and security of digital system applications in the U.S. nuclear industry and to make the regulation of these systems more performance based and risk informed. Toward that end, the NRC Digital System Research Plan for FY 2005–FY 2009 (the Research Plan) defines a coherent set of research programs that support the regulatory needs of the NRC, the Office of Nuclear Material Safety and Safeguards (NMSS), the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), and the Office of Nuclear Security and Incident Response (NSIR). The Research Plan describes the background, technical issues, and ongoing and planned activities to meet the challenges of regulating the implementation of digital I&C technologies in nuclear facilities.

Research Plan Programs

The Research Plan is organized hierarchically into the following six research programs:

(1) System Aspects of Digital Technology
(2) Software Quality Assurance
(3) Risk Assessment of Digital Systems
(4) Security Aspects of Digital Systems
(5) Emerging Digital Technology and Applications
(6) Advanced Reactors

Each research program consists of research projects and associated specific research tasks to support licensing of new reactors and digital I&C upgrades in operating plants.

Current Key Research Projects

The following is a list of the research projects that are under way to support resolution of the NRC's key digital I&C technical issues, including a brief summary of the research projects.

Diversity and Defense in Depth

The objective of this research project is to identify appropriate levels of diversity and defense in depth required for mitigating the effects of common-cause failures (CCFs). The licensee is responsible for determining appropriate diverse systems and defense-in-depth design features for mitigating the effects of CCFs, and the responsibility for independently evaluating the licensee's proposed designs lies with the NRC. Guidance for identifying acceptable nuclear power plant safety system diversity and defense-in-depth design approaches is provided in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems." (ML9501180332) The intention of this regulatory guidance was to provide licensees and the NRC staff a means for assessing whether additional diversity is required in a digital safety system on the basis of the safety system and nuclear power plant design features.

The deterministic approach described in NUREG/CR-6303, while comprehensive, did not provide specific guidance to licensees for assuring (and for enabling the NRC to confirm) that acceptable diversity and defense-in-depth design strategies had been implemented in a digital safety system design. This conclusion arose from industry experience as licensees began evaluating diversity and defense-in-depth design features using the guidance in NUREG/CR-6303 when developing digital safety system upgrades to their existing analog-based safety systems. For example, recent diversity and defense in depth evaluations have placed significant burden for mitigating CCFs on plant operators instead of on diverse mitigating systems.

The objective of this research project is to improve the guidance in NUREG/CR-6303 by identifying specific combinations of diversity attributes and associated diversity attribute criteria that are acceptable to the NRC for reducing the risk and resulting consequences of unmitigated CCFs in digital safety systems.

Draft guidance is scheduled for completion in late 2007, and final guidance should be completed in mid-2008.

Risk Assessment of Digital Systems

The current NRC digital I&C system licensing process is deterministic. In the 1997 National Research Council report on the digital I&C system in nuclear power plants, it was recommended, "The U.S. NRC should strive to develop methods for estimating failure probabilities of digital systems, including COTS [commercial off-the-shelf] software and hardware for use in probabilistic risk assessment." The report also indicated, "These methods should include acceptance criteria, guidelines, and limitations for use and any needed rational and justification." Additionally, the NRC PRA Policy Statement encourages the staff to risk-inform all regulatory reviews to the extent supported by the state of the art.

The NRC and the industry are interested in risk-informing digital safety system licensing reviews. The staff has been working over the past 2 years to develop risk and reliability methods needed to risk-inform digital system reviews. The Electric Power Research Institute (EPRI) has also proposed an approach to risk-inform the diversity and defense-in-depth analysis. More broadly than diversity and defense in depth, the NRC research program is designed to develop methods for modeling reliability and the risk of digital I&C.

One of the major challenges to risk-informing digital system reviews is developing a common method for modeling digital system reliability. The staff examined a number of reliability and risk methods that have been developed in other industries—such as aerospace, defense, and telecommunications—and has determined that some of the digital system risk modeling methods used in these industries can be adapted for use in the nuclear industry. The results of the first phase of the digital system risk research project were published as NUREG/CR-6901, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments." This report reviewed a number of reliability methods that have been used by other industries to model digital systems as well as the research that has been done to support their implementation in practical engineering analysis.

Based on the staff's review of these techniques, together with available failure data, the NRC is evaluating several digital system modeling methods with the intent of establishing best practices for modeling digital systems in nuclear power plants. These methods include Markov modeling, dynamic flow graph methods, and traditional event tree/fault tree methods.

The staff plans to use the digital system reliability and risk analysis methods that are being developed and benchmarked as part of this research as one acceptable method that can be applied to current NRC guidance for using PRA 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"). The staff envisions developing regulatory guidance that will provide specific guidance for risk-informing digital system licensing decisions in a way similar to that of Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications," which provides specific guidance for risk-informing technical specification changes.

Draft regulatory guidance is scheduled for completion in late 2007, and final regulatory guidance should be completed in mid-2008.

Highly Integrated Control Rooms

The primary objective of this research project is to develop a comprehensive process for confirming that an integrated control room design is in conformance with NRC regulations and associated standards for areas such as electrical separation and independence between safety-related displays and controls and nonsafety-related displays and controls, single-failure criteria, equipment qualification of safety-related displays and controls for Class 1E use, and data communication isolation and cyber security.

An 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 and from the lessons learned from operating experience. This research project will survey 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 will compare 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 develop guidance and associated acceptance criteria for use by the staff in confirming that integrated control room designs are in conformance with NRC requirements.

Draft regulatory guidance is scheduled for completion in late 2007, and final regulatory guidance should be completed in mid-2008.

Security Aspects of Digital Systems

The security of digital safety systems involves addressing potential security vulnerabilities as part of the system development process and maintaining the security of the system after it is installed. Since the staff has already reviewed and approved (for generic use) most digital system development platforms that are anticipated for use in the nuclear industry, security assessments of digital systems are being performed on the systems (composed of commercial off-the-shelf digital equipment) that have been developed using these platforms.

Security assessments of cyber vulnerabilities will determine if NRC-approved digital systems have any inherent susceptibility to malicious activity through computing resources. The project is currently focused on the three major NRC-approved digital safety systems, and it involves fault-injection testing (e.g., penetration testing) of the systems to determine failure modes/characteristics. Representative configurations of nuclear power plant installations will be assessed in laboratory settings. Knowledge gained from these laboratory assessments will be utilized in site assessments at various nuclear plants containing the NRC-approved systems. For example, using the knowledge gained from the in-laboratory penetration testing of the NRC-approved systems, an NRC test team will collaborate with a licensee (e.g., pilot plant) on assessing the licensee's specific configuration in the context of NEI-04-04. This assessment will take an inside-out approach that would start at the innermost ring of critical assets and work successively outward to identify potential vulnerabilities of the site's configuration. The data obtained from the laboratory and site assessments will be used by the Network Security project to identify protection and mitigation measures appropriate to nuclear power plant environments. Starting in mid-2007, the Network Security project will evaluate architectures for compliance with NRC regulatory requirements and NEI-04-04 that provide the best chances to survive cyber security attacks (i.e., I&C architectures resilient against cyber attacks). The data obtained from the laboratory and site assessments will also form the bases for regulatory guidance to the NRC staff (for licensing reviews and inspections) as well as licensees and vendors.

In early 2007, the NRC will begin assessment of the electromagnetic (EM) environment at nuclear power plants and its potential impacts on digital safety systems. The project will build upon previous research at Sandia National Laboratory (SNL). The SNL work evaluated a worst-case EM environmental impact on an example nuclear power plant, with generic extensions to other plants. Security assessments of EM environmental impacts will take an

approach similar to that of the earlier study by SNL. First, the worst-case EM model will be updated using recent research results from all available sources, including the classified domain. Second, advances in technology will be considered when developing the model and during subsequent analyses. Consideration of advances in technology may lead the staff to consider a different set of example plants than that previously utilized by SNL in order to obtain an accurate assessment of digital safety system susceptibility to EM effects. In late 2008, the results of this assessment of EM environmental impacts on digital safety systems will be produced in the form of regulatory guidance and updates to the staff review guidance.

Emerging Technology Research

FPGA Design Guidelines

The objective of this research project is to develop a comprehensive process for confirming that using a safety system design based on a field programmable gate array (FPGA) is in conformance with NRC regulations and associated standards.

As a first step, the research will review the regulatory 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 FPGA-based safety systems and will compare the regulatory approaches with the regulatory criteria now used by the NRC. The research also will identify standards regulating the use of FPGAs to determine their suitability for endorsement as regulatory guides.

In addition to using the regulatory experience and associated guidance developed above, FPGA subject-matter experts will be used to develop guidelines for reviewing FPGA-based safety-related applications. These guidelines will follow the hierarchical structure described in NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems," which provides guidance to the NRC for reviewing software programs for safety systems for 10 high-level languages. The FPGA guidance will expand the scope of NUREG/CR-6463 to include software, hardware, and system aspects.

The draft FPGA-based design guidelines will be validated using a safety-related FPGA application in accordance with domestic cooperative research agreements with one or more nuclear power plant licensees.

Draft regulatory guidance is scheduled for completion in late 2007, and final regulatory guidance should be completed in mid-2008.